THREATDOWN™

Business Compliance Framework Report

A practical overview of Global, North American and EMEA regulatory standards

Contents

What Business Leaders Need to Know About Compliance Frameworks

Organizations today face cyber threats alongside an expanding set of regulatory requirements that vary by region and industry. Understanding these frameworks is critical to protecting sensitive data, avoiding penalties, and maintaining customer trust.

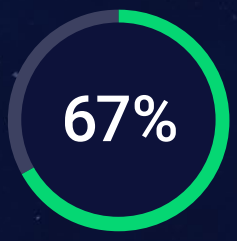
This guide gives you a clear overview of the most widely recognized compliance frameworks in North America, EMEA, and across global markets. By understanding which frameworks apply to your operations, you can make informed decisions about risk management, security investments, and operational priorities.

Why Compliance Matters Now

The impact of regulations extends well beyond legal teams. They shape how organizations design security programs, choose vendors, and maintain customer trust. These requirements exist to safeguard against threats, protect sensitive data, and preserve confidence in the marketplace.

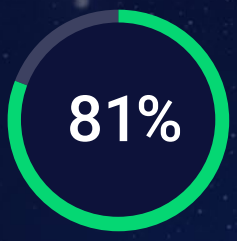
Whether it's a global standard or a local privacy law, the goal is the same: ensure organizations handle information responsibly and operate with integrity. Failing to meet these obligations can bring costly fines, operational disruption, and lasting damage to reputation.

Fast facts to know about compliance



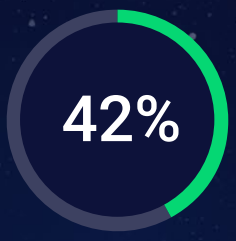
of SMBs say regulatory compliance is now a top driver for cybersecurity investment.[1]

[1] ISACA State of Cybersecurity 2025



of data breaches involve records protected under at least one compliance regulation.[2]

[2] Verizon 2025 DBIR



of medium size companies spend $100K on audits each year.[3]

[3] A-LIGN 2025 Compliance Benchmark Report

As compliance expectations grow, knowing which frameworks apply to your organization is the first step toward meeting them. The following sections outline key standards by region and industry, along with what they typically require, so you can focus resources where they matter most.

Global Compliance Frameworks in Detail

	SOC 2	PCI-DSS	ISO/IEC 27001
What it covers	Controls for data security, availability, processing integrity, confidentiality, and privacy.	Security standards for handling credit card and payment data.	International standard for information security management systems (ISMS).
Why it matters to your business	Many organizations require a current SOC 2 report before working with a security vendor, making it a common prerequisite for market access and customer trust.	Required by payment brands and acquirers; failure to comply can result in fines, higher transaction fees, or loss of payment processing privileges.	Certification demonstrates a mature, structured approach to information security and is often required in global contracts and RFPs.
Regions it applies to	North America/Global	Global	Global
Industries it applies to	All service-based industries	Retail, eCommerce, Finance	All industries
What's typically required	Security policies, monitoring, incident response, access controls	Firewall configuration, secure storage, encryption, access restriction	ISMS policies, risk assessments, internal audits, continuous improvement
Example in practice	A SaaS company completes its first SOC 2 Type II, tightening access controls and documenting policies. The final report gives sales a clear "security compliance" win during procurement reviews.	An online retailer segments payment systems, encrypts all card data, and passes quarterly scans. Annual PCI audits keep transactions secure and payment partners confident.	A manufacturer certifies its ISMS, covering factories and cloud systems. The ISO 27001 certificate helps secure new contracts with international partners.

North America Compliance Frameworks

	HIPAA	NIST 800-53	CMMC 2.0
Why it matters to your business	HIPAA compliance is mandatory for any organization that stores or processes protected health information. Noncompliance can lead to significant fines, loss of patient trust, and increased scrutiny from regulators.	NIST 800-53 is important because it provides businesses with a proven framework to secure data, reduce risk, demonstrate compliance, and build lasting confidence with partners and customers.	Required for U.S. Dept of Defense (DoD) contractors to handle controlled unclassified information (CUI). Establishes a required cybersecurity baseline for defense.
What it covers	Regulates the use and disclosure of protected health information (PHI) in the U.S.	U.S. federal cybersecurity framework for securing systems and data.	Cybersecurity standards required for defense contractors and subcontractors to safeguard Controlled Unclassified Information (CUI).
Regions it applies to	North America	North America	United States
Industries it applies to	Healthcare	Government, Finance, Healthcare	Defense Industrial Base (DIB)
Examples in practice	A regional clinic encrypts medical records, restricts access to authorized staff, and runs annual HIPAA risk assessments. These measures protect patient data and maintain eligibility for insurance network partnerships.	A federal contractor implements strict access controls, continuous monitoring, incident response to meet NIST 800-53 requirements to keep existing contracts and qualify for new bids.	A defense supplier achieves Level 2 CMMC certification, documenting security plans and undergoing a third-party assessment to retail eligibility for military procurement.
What's typically required	Access control, data encryption, audit logging, risk assessments	Security controls, risk management, continuous monitoring	Access controls, system security plans, continuous monitoring, multi-factor authentication, incident response, security awareness training

North America Compliance Frameworks (continued)

	CCPA/CPRA	PIPEDA
Why it matters to your business	Gives California residents rights over their personal data, including access, deletion, and opt-out of sale. Noncompliance can lead to state fines and lawsuits.	Sets rules for how Canadian organizations collect, use, and disclose personal information in commercial activities.
What it covers	California privacy laws granting consumers rights over personal data, including access, deletion, and opt-out of sale.	Canadian federal law regulating the collection, use, and disclosure of personal information in commercial activities.
Regions it applies to	California, United States (with influence on other U.S. privacy laws)	Canada
Industries it applies to	All businesses handling California resident data	All industries engaged in commercial activities
Examples in practice	A retail chain maps where customer data is stored, updates privacy policies, and implements a process to honor opt-out requests.	A Canadian financial services firm encrypts sensitive records, applies access controls, and trains staff on privacy obligations.
What's typically required	Data mapping, consent management, data access requests, breach notification protocols, opt-out mechanisms	Data protection policies, breach reporting, consent mechanisms, security safeguards, accountability measures

EMEA Compliance Frameworks

	GDPR	DORA
Why it matters to your business	Applies to any organization. handling EU residents' personal data, regardless of location. Violations can result in substantial fines and loss of EU market access.	Requires financial institutions in the EU to demonstrate operational resilience against ICT-related disruptions. Noncompliance can jeopardize regulatory approval to operate.
What it covers	Protects privacy and personal data of EU citizens.	Ensures ICT risk resilience in financial institutions in the EU.
Regions it applies to	EMEA	EU/EMEA
Industries it applies to	All industries handling EU personal data	Financial Services
Examples in practice	An online retailer updates consent forms, builds an automated process for deletion requests, and encrypts customer data to meet GDPR requirements.	A European bank develops and tests incident playbooks, conducts resilience assessments, and reports results to regulators in line with DORA.
What's typically required	User consent, breach reporting, data access and deletion rights, data protection officer	ICT risk management, incident reporting, digital operational resilience testing

EMEA Compliance Frameworks (continued)

	UK Cyber Essentials	NIS2
Why it matters to your business	A basic cybersecurity certification backed by the UK government. Often required for public sector contracts and valued in the private sector as proof of foundational controls.	Applies to essential and important entities in the EU, requiring stronger risk management, incident reporting, and supply chain security. Noncompliance can lead to large fines and regulatory enforcement.
What it covers	UK government-backed certification for basic cybersecurity controls.	EU directive aimed at enhancing cybersecurity across essential and digital services providers.
Regions it applies to	UK	EU/EMEA
Industries it applies to	All industries	Critical infrastructure, Energy, Transport, Health, Digital services
Examples in practice	A manufacturing company gains Cyber Essentials certification by implementing MFA, securing devices, and passing an external vulnerability scan.	An EU-based organization implements 24/7 monitoring, performs quarterly continuity tests, and documents supply chain risk assessments to meet NIS2 obligations.
What's typically required	Firewalls, secure configuration, access control, malware protection	Risk management, incident reporting, business continuity, supply chain security, governance policies

Conclusion: Supporting Your Compliance Journey

Three actions to take now:

1. **Know what you need to comply with**
   Identify which regulations apply to your business model, industry, and geographic footprint. This creates a focused plan and helps you align compliance requirements with the right security solutions to support growth.

2. **Audit your security and reporting practices**
   Evaluate whether your technical controls, policies, and reporting meet the requirements of your applicable frameworks. Address gaps now to avoid audit failures or contract delays.

3. **Make compliance a leadership topic**
   Incorporate compliance status into regular leadership meetings and board updates. This ensures visibility, sustained investment, and accountability across the business.

Building and maintaining compliance readiness is about having safeguards in place to protect data, reduce risk, and satisfy regulatory requirements. That takes security capabilities that can address both framework obligations and real-world threats.

ThreatDown delivers cybersecurity solutions built with compliance in mind. Our technologies map to the control areas most often called for in frameworks like SOC 2, ISO 27001, PCI DSS, HIPAA, and GDPR — from endpoint and email protection to vulnerability management and threat detection. While no tool alone can guarantee compliance, ThreatDown equips organizations with the security evidence and resilience needed to prepare for audits and demonstrate regulatory readiness.

Why Organizations Choose ThreatDown

At ThreatDown, we understand the stakes for businesses that must meet regulatory obligations while defending against sophisticated cyber threats.

Our portfolio spans endpoint, network, email, and detection technologies — the same types of capabilities called for in frameworks like SOC 2, ISO 27001, PCI DSS, HIPAA, and GDPR. ThreatDown solutions help you:

- Enforce access controls and secure configurations
- Monitor systems 24/7 for threats and anomalies
- Detect and respond to incidents quickly
- Retain and report security logs for audit evidence

ThreatDown develops its security technologies with widely adopted compliance frameworks in mind. By aligning product capabilities to common control requirements, such as access management, logging, and threat detection we help organizations strengthen their security posture while supporting their compliance objectives.

Compliance Frameworks at-a-Glance

Use this page as a quick reference to identify frameworks by region and key requirements.

Framework	Region	Applies to	What's typically required
ISO/IEC 27001	Global	All industries	Security policies, training, asset management, patching
PCI-DSS	Global	Retail, Finance, eCommerce	Payment data security
SOC 2	Global	SaaS/Finance	Logging, alerting, vulnerability management, backup policies
PIPEDA	CA	All industries	Canadian data protection
GDPR	EU	All industries	Data mapping, MFA, access controls, breach response
UK Cyber Essentials	UK	All industries	Basic Security controls
NIS2	EU	Critical Sectors	Critical infrastructure security
DORA	EU	Finance	Resilience planning, playbooks, response testing
CCPA/CPRA	US, California	All industries	Consumer data privacy
HIPAA	US	Healthcare	Email encryption, audit logs, MDR, breach notification
NIST 800-53	US	Public Sector	Access controls, monitoring, incident response plans
CMMC 2.0	US	Public Sector, Defense	Defense contractor cybersecurity

Ready to strengthen your security and compliance posture?

Empower your business with compliance-ready protection. Let's connect to explore how our solutions fit into your compliance-ready security strategy

Contact us today

THREATDOWN™

threatdown.com