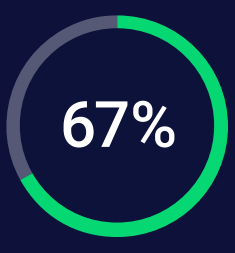
THREATDOWN™

Navigating Compliance for Business Leaders

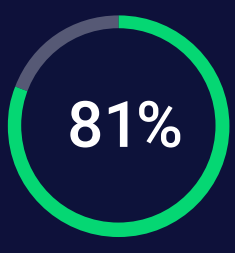
Simplify the complexity. Protect your organization. Stay audit-ready.

Compliance frameworks don't have to be overwhelming. Whether you're pursuing your first certification or managing multiple regulatory requirements, this infographic breaks down what matters most — the key frameworks, what they typically require, and the security tools that help you stay compliant.

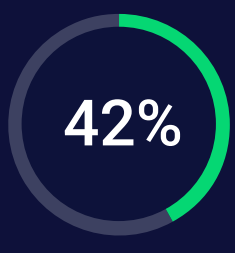
Why Compliance Matters



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



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



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

[1] ISACA State of Cybersecurity 2025

[2] Verizon 2025 DBIR

[3] A-LIGN 2025 Compliance Benchmark Report

Key Compliance Frameworks by Region

North America:

- HIPAA (Healthcare)
- NIST 800-53 (Gov/Contractors)
- CMMC 2.0 (Defense)
- CCPA/CPRA (Consumer Privacy)

EMEA:

- GDPR (All Industries)
- DORA (Finance)
- UK Cyber Essentials (Basic Controls)
- NIS2 (Critical Infrastructure)

Global:

- ISO 27001 (ISMS)
- SOC 2 (SaaS, Finance)
- PCI-DSS (Retail, Finance)

What Compliance Readiness Looks Like

- 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

What's Typically Required

Encryption
(Email & Data)

Policies
(Access Control, Retention, Use)

Security Tools
(EDR, MDR, Patch, DNS)

Logging & Monitoring

Role-based & MFA Access

Breach Notification

Incident Response Plans

Audit Readiness

Empowering your Organization to Meeting Evolving Regulatory Requirements

- 24/7 MDR (SOC 2, ISO, NIST)
- Email Security (HIPAA, GDPR, PCI)
- DNS Filtering, Patch Management, App Control (NIS2, Cyber Essentials)

Learn How ThreatDown Supports your Compliance Efforts

Contact us