ThreatDown™
Powered by Malwarebytes

Demystifying Compliance Frameworks for MSPs

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

Contents

The MSP's Compliance Advantage: Win Business, Reduce Risk 3

Introduction: What MSPs Need to Know About Compliance Frameworks 4

Global Compliance Frameworks in Detail 5

North America Compliance Frameworks 6

EMEA Compliance Frameworks 8

Conclusion: Supporting Clients on Their Compliance Journey 10

Why Service Providers Choose ThreatDown 11

Compliance Frameworks at-a-Glance 12

The MSP's Compliance Advantage: Win Business, Reduce Risk

MSPs today don't just protect systems — they're on the frontlines of helping clients meet regulatory demands. Compliance is no longer optional. It's a competitive advantage and a trust driver.

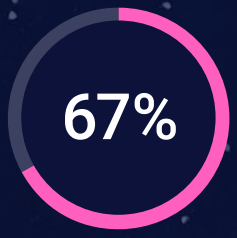
Why This Guide? This guide equips MSPs with clarity on key compliance frameworks by region and industry — and how ThreatDown empowers MSPs to deliver compliant-aligned security services that protect clients and drive business growth.

Introduction: What MSPs Need to Know About Compliance Frameworks

MSPs today face more than just technical threats — they must also support clients navigating a maze of regulatory compliance frameworks across industries and regions. This guide is designed to demystify the compliance landscape so MSPs can identify which frameworks matter most to their clients and how to support them — without over-promising or over-extending.

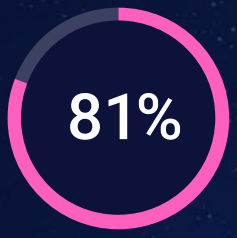
Compliance is not just a checkbox. It's about building trust, protecting sensitive data, and meeting rising client expectations. This guide breaks it down clearly — by region, by industry, and by what actions are actually needed on the ground.

Fast facts MSPs should know about compliance



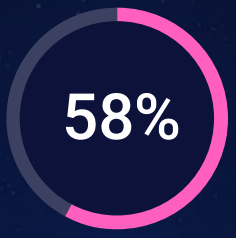
of SMBs say regulatory compliance is now a top driver for cybersecurity investment.[1]

[1] ISACA State of Cybersecurity 2025



of data breaches in 2024 involved records protected under at least one compliance regulation.[2]

[2] Verizon 2025 DBIR



of MSPs report rising client requests for compliance support as a top business challenge.[3]

[3] Channel Futures MSP 501 2025

The MSP role in compliance — what's really required?

MSPs aren't certifiers — but they provide critical technical controls, monitoring, logging, and incident response that compliance frameworks demand (like SOC 2 and ISO 27001). Understanding the key standards ensures MSPs deliver real value without over-promising. That's why understanding the relevant frameworks matters — you're a critical part of your client's compliance picture.

Global Compliance Frameworks in Detail

	SOC 2	PCI-DSS	ISO/IEC 27001
MSP Scenario	A managed provider serving fintech firms ensures compliance by using centralized log management, automated alerting, and quarterly vulnerability assessments to align with SOC 2 control criteria.	An MSP supporting a retail chain configures secure payment processing environments with encrypted point-of-sale systems, segmented networks, and continuous vulnerability scans to meet PCI-DSS requirements. They provide quarterly ASV scans, manage firewall rules, and deploy EDR to monitor endpoints handling payment data.	An MSP partnering with a multinational manufacturing firm implements centralized logging, access control policies, and endpoint security aligned with ISO/IEC 27001 ISMS controls. They schedule annual internal audits, enforce patching and configuration baselines, and provide risk assessment reporting for client ISMS documentation.
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).
Regions it applies to	North America/Global	Global	Global
Industries it applies to	All service-based industries	Retail, eCommerce, Finance	All industries
Why it's relevant to MSPs	MSPs often manage or secure systems that fall under the scope of SOC 2 compliance, supporting client efforts in meeting security, privacy, and operational requirements.	MSPs often manage or secure systems that fall under the scope of PCI-DSS compliance, supporting client efforts in meeting security, privacy, and operational requirements.	MSPs often manage or secure systems that fall under the scope of ISO/IEC 27001 compliance, supporting client efforts in meeting security, privacy, and operational requirements.
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

North America Compliance Frameworks

	HIPAA	NIST 800-53	CMMC 2.0
MSP Scenario	A healthcare MSP in Texas deploys MDR and encrypted email to ensure HIPAA-compliant incident response and PHI protection. They also assist clients in setting up audit trails and secure backups for medical records.	A U.S. federal contractor relies on their MSP to implement layered access controls, host-based firewalls, and real-time monitoring to meet NIST 800-53 expectations.	An MSP supporting U.S. defense contractors implements strict access controls, multi-factor authentication, and continuous monitoring to help clients meet CMMC 2.0 compliance.
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)
Why it's relevant to MSPs	MSPs often manage or secure systems that fall under the scope of HIPAA compliance, supporting client efforts in meeting security, privacy, and operational requirements.	MSPs often manage or secure systems that fall under the scope of NIST 800-53 compliance, supporting client efforts in meeting security, privacy, and operational requirements.	MSPs managing IT for defense contractors are responsible for enforcing technical controls, managing system security plans, and supporting clients in audits.
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
MSP Scenario	A California-based MSP helps a retail client enforce data access policies and breach notification processes to align with CCPA/CPRA requirements.	A Canadian MSP secures client environments with encryption, access controls, and incident response plans in line with PIPEDA requirements.
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
Why it's relevant to MSPs	MSPs managing IT infrastructure, security, or data systems for California clients must ensure proper data handling, breach notifications, and access control mechanisms.	MSPs help clients protect personal information, comply with breach reporting requirements, and implement appropriate safeguards for personal data.
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
MSP Scenario	An EU-based MSP working with an eCommerce client enforces encryption-at-rest and in-transit, applies DNS filtering for malicious sites, and integrates email security to prevent data leakage. They support data mapping exercises, automate breach notification workflows, and assist with implementing user consent and deletion requests.	A European MSP serving financial services builds custom playbooks and incident workflows tied to operational resilience, in line with DORA's new regulatory guidance.
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
Why it's relevant to MSPs	MSPs often manage or secure systems that fall under the scope of GDPR compliance, supporting client efforts in meeting security, privacy, and operational requirements.	MSPs often manage or secure systems that fall under the scope of DORA compliance, supporting client efforts in meeting security, privacy, and operational requirements.
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
MSP Scenario	A UK MSP serving SMBs deploys ThreatDown EDR, enforces MFA across Microsoft 365 tenants, and configures secure endpoint baselines to meet Cyber Essentials controls. They manage firewall rules, provide phishing-resistant email protection, and offer vulnerability scanning with monthly compliance reports for certification readiness.	An MSP supporting an EU-based energy provider builds resilience by implementing 24/7 MDR monitoring, patch management, and incident response plans aligned to NIS2. They manage supply chain risk assessments, automate audit logging retention, and conduct quarterly tabletop exercises to meet continuity and reporting requirements.
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
Why it's relevant to MSPs	MSPs often manage or secure systems that fall under the scope of UK Cyber Essentials compliance, supporting client efforts in meeting security, privacy, and operational requirements.	MSPs often manage or secure systems that fall under the scope of NIS2 compliance, supporting client efforts in meeting security, privacy, and operational requirements.
What's typically required	Firewalls, secure configuration, access control, malware protection	Risk management, incident reporting, business continuity, supply chain security, governance policies

Conclusion: Supporting Clients on Their Compliance Journey

Three immediate actions MSPs can take now

1. **Map your clients to Frameworks**
   Industry + Region = Your Compliance Focus. Conduct a quick framework mapping exercise for your top clients — industry and region usually dictate 80% of what's needed.

2. **Review your logs & reporting**
   Are you meeting data retention and reporting needs? Review your MDR and email security logs to ensure reporting, alerts, and retention align with your clients' compliance expectations.

3. **Make compliance a QBR topic**
   Drive strategic conversations and deepen client trust. Start including compliance-relevant discussions in your QBRs and security reviews — position yourself as a strategic advisor.

This guide is your starting point to understand the compliance expectations your clients may face based on their region and industry. As an MSP, your role in securing systems, managing endpoints, and guiding clients through foundational security controls is critical to their success.

Want help identifying tools or services aligned to these frameworks? Contact ThreatDown to explore how we support MSPs like you across the compliance lifecycle.

Why Service Providers Choose ThreatDown

At ThreatDown, we understand the unique challenges MSPs face in securing client environments while navigating an evolving compliance landscape.

While no cybersecurity tool can guarantee compliance, ThreatDown offers a powerful suite of endpoint, network, and detection technologies that align with best practices required by many frameworks — including logging, threat detection, access control, and secure configuration.

Our Partner Program is designed to help MSPs grow confidently, with sales enablement, dedicated support, and solutions purpose-built for the compliance-aware client. Join thousands of MSPs who trust ThreatDown to protect their clients — and drive their business forward.

ThreatDown's MDR (Managed Detection and Response) offering provides 24/7 threat monitoring, alert triage, and expert incident investigation — a critical capability for clients aiming to meet security requirements found in frameworks like SOC 2, NIST 800-53, and ISO 27001.

In addition, our upcoming Email Security solution will help MSPs better protect against phishing, malware, and data loss — key considerations in GDPR, HIPAA, and PCI-DSS compliance readiness. These tools are built to support MSPs like you in delivering secure, compliant-aligned services — without the burden of managing complex infrastructure alone.

Compliance Frameworks at-a-Glance

Use this page as a quick reference to identify frameworks by region and what your clients might typically need.

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 grow your MSP with compliance-aligned services?

Empower your business with compliance-ready protection. Let's connect and explore how ThreatDown supports MSPs with powerful, compliance-ready solutions.

Contact us today

threatdown.com

Copyright © 2025, ThreatDown. All rights reserved. ThreatDown and the ThreatDown logo are trademarks of ThreatDown. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind. 08/25