



SPECTRA

Introduction to SPECTRA Certification Standards

The **SPECTRA Certification** sets a minimum baseline for Managed Service Providers (MSPs) to demonstrate their ability to secure both their own operations and the customer environments they manage. It is designed to enhance trust with clients, support risk modeling for insurers, and strengthen resilience across digital supply chains.

PURPOSE AND SCOPE OF CERTIFICATION

- Establishes **objective, practical controls** tied to the main causes of cyber-related losses.
- Provides a **vendor-neutral framework** aligned with industry expectations.
- Encourages **continuous improvement** to adapt to evolving cyber threats.
- Used by insurers for **underwriting and actuarial risk analysis**.

CORE CERTIFICATION STANDARDS

To achieve SPECTRA Certification, MSPs must meet key cybersecurity and operational benchmarks across two core areas: **Internal Security** and **Managed Services**. These standards ensure consistent, verifiable protection within MSP operations and client environments—driving continuous improvement, resilience, and trust.

INTERNAL SECURITY

IT Support & Governance

- Defined **SLAs and incident response** procedures.
- Regular staff training.
- Risk assessment of third-party providers.
- Threat intelligence integrated into strategy.

Protective Controls

- Regular **penetration testing and vulnerability scanning**.
- Security awareness & phishing training.
- Secure device configuration and remote access controls.
- Endpoint protection with MDM policies.
- Zero-trust access and segmentation to prevent systemic compromise.



SPECTRA

WHY CERTIFICATION MATTERS

- **For MSPs:** Demonstrates service quality and strengthens customer confidence.
- **For Clients:** Provides assurance of robust, standardized cybersecurity protections.
- **For Insurers:** Supports accurate risk assessment and underwriting.
- **For the Industry:** Contributes to systemic resilience and reduced impact of cyber threats.

A TRUSTED MARK OF CYBERSECURITY EXCELLENCE

Achieving SPECTRA Certification demonstrates an MSP's compliance with industry-aligned cybersecurity benchmarks, spanning governance, protection, detection, and recovery. It serves as a trusted mark of quality and risk management maturity in a rapidly evolving threat landscape.



MANAGED SERVICES

ELIGIBLE MANAGED SERVICES	CONTROL STANDARDS
MANAGED DETECTION AND RESPINSE	<ul style="list-style-type: none">• ≥99% of customer endpoints (and 100% of servers), 100% of network edge systems, and all in-scope identities and mailboxes are enrolled, and actively reporting to the centralized management console.• Continuous (24x7x365) security monitoring and incident response for all in-scope assets.• Active response capabilities to contain and mitigate detected security events.
FIREWALL	<ul style="list-style-type: none">• Running the latest stable release• Configured for high availability (where required)• DDoS resilient
DISASTER RECOVERY	<p>Replication maintained of production systems, which:</p> <ul style="list-style-type: none">• Utilizes independent infrastructure• Maintains production equivalent degree of security• Logically segregated• Tested annually



MANAGED SERVICES

BACKUP	<ul style="list-style-type: none">• 2+ instances of segregated recovery data maintained• 1 immutable and isolated copy maintained• Undertaken automatically, and incidents are managed• Tested quarterly
ENDPOINT SECURITY	<ul style="list-style-type: none">• EDR is installed on 99%+ of endpoints• Backups of critical files on endpoints are undertaken• 24x7 monitoring and response available
BUSINESS EMAIL COMPROMISE (BEC) PROTECTION	<ul style="list-style-type: none">• Identity & Access Management (IAM) controls established, including MFA• DMARC in place• Secure email; solution deployed, including ATP features• Employee security training and awareness program in place

