Compliance Readiness Checklist for MSPs

Support client expectations – not certify compliance

Use this checklist to assess whether you're equipped to support your clients' compliance needs — based on the region, industry, and frameworks that matter most. This isn't about certification — it's about showing your clients you're aligned with their regulatory expectations.

1. Understand Your Client Landscape

- ☐ Have you identified the industries and regions your clients operate in?
- ☐ Have you matched applicable compliance frameworks to each client (e.g., HIPAA, GDPR, SOC 2)?
- ☐ Do you understand which frameworks are mandatory vs. recommended?

2. Review Technical Security Controls

- ☐ Are you delivering or reselling MDR services (like ThreatDown's 24/7 monitoring) to support incident detection and audit logging?
- ☐ Is email security in place for phishing and data loss protection?
- ☐ Are backups encrypted and protected from ransomware?
- ☐ Is MFA enforced for all administrative access?

3. Help Clients Formalize Policies

- ☐ Do your clients have documented Acceptable Use, Retention, and Access Control policies?
- ☐ Is there a written Incident Response Plan that includes your role as the MSP?
- ☐ Are roles and responsibilities clearly documented and agreed upon?

4. Reporting & Compliance Communication

- ☐ Are security events and logs reviewable for compliance needs (e.g., SOC 2)?
- ☐ Do you offer summary reporting or compliance-readiness checks during QBRs?
- ☐ Are breach notification timelines understood by you and your clients?

5. Your MSP Action Plan

- ☐ Include compliance relevance in every QBR or security strategy review.
- ☐ Use this checklist as a starting point for client discovery or onboarding.
- ☐ Lean on your security vendors for guidance, tools, and expertise.