PROMETHEUS CONSULTING

Cyber-Insurance Readiness Checklist

The controls carriers check at renewal and what to have documented.

In 2026, carriers expect proof that each control is enforced, not simply present. A failed renewal can mean higher premiums, exclusions, or denial. Use this checklist before renewal and keep the evidence together.

THE 8 CORE CONTROLS CARRIERS CHECK

- ☐ **Multi-factor authentication (MFA)** For email, remote access, administrator accounts, and cloud apps.
- ☐ **Endpoint detection and response (EDR)** On every device and actively monitored. Not just antivirus.
- ☐ **Tested, immutable backups** Proven by a real restore test and protected from tampering.
- ☐ **Email authentication** SPF, DKIM, and DMARC configured and enforced.
- ☐ **Least-privilege access control** Unique accounts, separate administrator logins, and prompt offboarding.
- ☐ **Security logging and monitoring** Sign-ins, MFA changes, privileged activity, and meaningful alerts.
- ☐ **Patch and vulnerability management** Systems kept current, with known gaps tracked and closed.
- ☐ **Written incident-response plan** Named decision makers, counsel, insurer, and notification steps.

RED FLAGS THAT STALL A RENEWAL

- **No MFA on all accounts.** This is a common reason coverage is denied or restricted.
- **Backups never restore-tested.** A backup you have not proven may not protect the business.
- **Shared or standing administrator accounts.** There is no separation, accountability, or reliable offboarding.
- **No documented incident-response plan.** Writing the plan during an incident is too late.

Which rules apply to your practice?

Map your controls to the framework that governs you.

FRAMEWORKS AND OBLIGATIONS

- **NIST CSF and CIS Controls.** The structured foundation every assessment should map to.
- **HIPAA Security Rule.** Medical and dental practices need risk analysis, access controls, audit logging, and PHI safeguards.
- **FTC Safeguards Rule (GLBA).** Financial and accounting firms need a written program, MFA, encryption, and monitoring.
- **Bar confidentiality and ABA Rule 1.6.** Law firms must make reasonable efforts to protect client and matter data.
- **Florida FIPA (Fla. Stat. section 501.171).**
  Notice may be required within 30 days. Incidents affecting 500 or more Florida residents must also be reported to the state.

WHAT A REAL READINESS ASSESSMENT GIVES YOU

- **Framework-mapped findings.** Every control is tied to the rule or requirement it supports.
- **Evidence, not assertions.** You receive documented proof instead of a self-reported checklist.
- **Prioritized gaps.** You know what to remediate first and why it matters.
- **A report you can hand a carrier.** Findings are structured for a clear underwriting conversation.

Not sure where you stand?

We run a forensic-grade readiness assessment mapped to NIST CSF and the CIS Controls. The assessment is informed by real incident-response experience and built to produce clear evidence.

prometheusconsultinglabs.com | (561) 216-8323