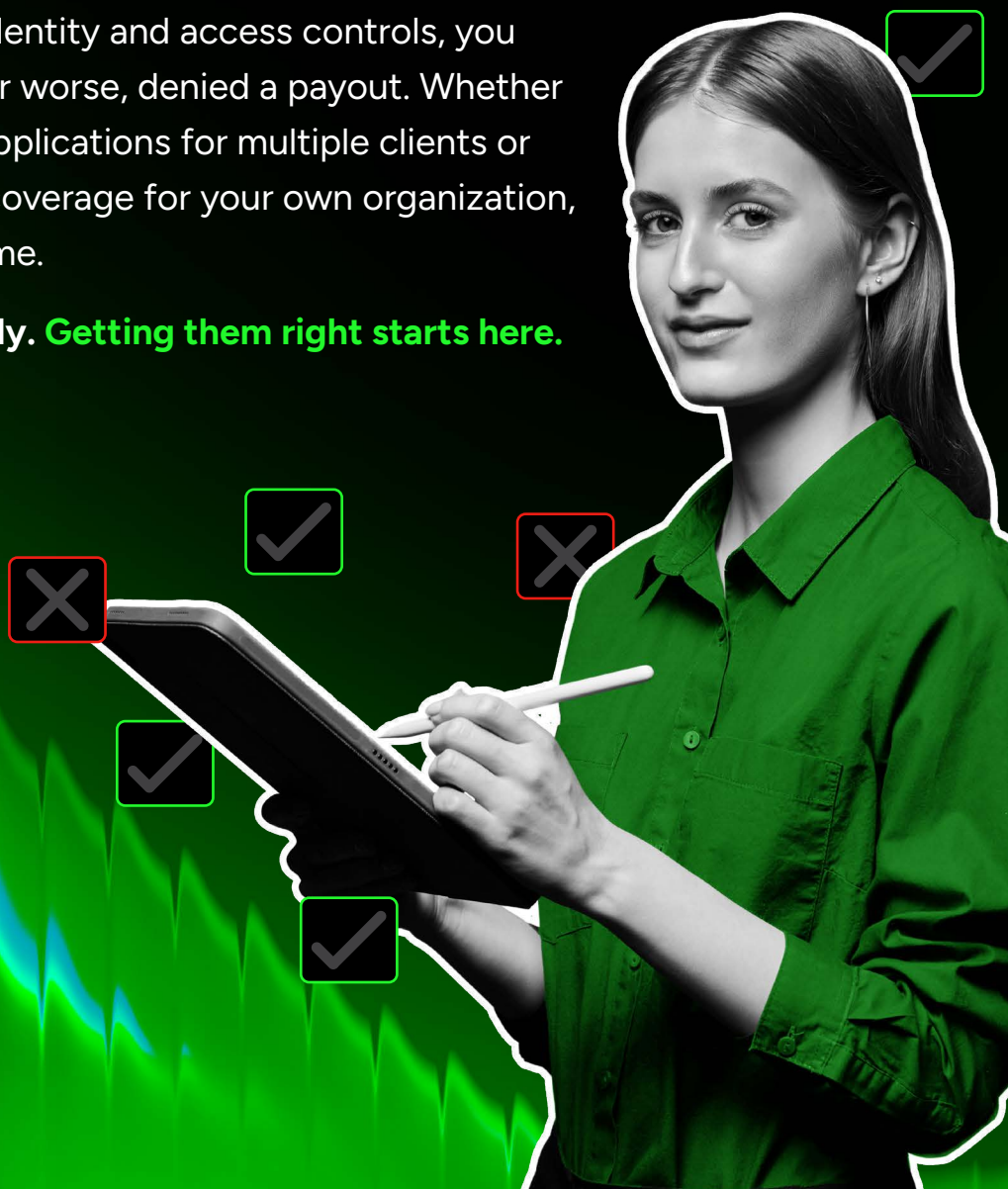
CyberQP

Cyber Insurance Readiness Checklist

Secure Coverage & Prove Compliance in 2026

Claims are rising, and underwriters are tightening standards. If your MSP lacks the right identity and access controls, you may be denied coverage—or worse, denied a payout. Whether you're an MSP completing applications for multiple clients or an internal IT team seeking coverage for your own organization, the requirements are the same.

Getting them wrong is costly. Getting them right starts here.



CyberQP

The Questions You'll Be Asked and How to Answer Them

These questions are pulled directly from real cyber insurance applications. Underwriters don't just want "yes" or "no" answers—they want evidence. Use this checklist to ensure your security posture is ready and provable.

Insurance Question	How to Check the Box with CyberQP
☐ **Do you require MFA for all remote and privileged access, including VPN, RDP, and cloud resources?**	**Yes** CyberQP enforces MFA for privileged accounts across Active Directory, Entra ID, and local Windows admin accounts.
☐ **Do you use Privileged Access Management (PAM) tools to protect admin accounts?**	**Yes** CyberQP applies zero trust principles, including just-in-time access, time-bound tokens, full logging, and rotation after every use.
☐ **Do non-IT users have local admin rights on their endpoints?**	**No** CyberQP removes standing local admin rights and provides just-in-time elevation with approvals through QDesk.
☐ **Are Domain Administrators configured with unique, random, long passwords?**	**Yes** CyberQP issues unique MFA tokens for each session, eliminating the risk of password reuse.
☐ **Do you restrict access to sensitive systems based on job function?**	**Yes** CyberQP restricts access to privileged systems using policy-based access tied to identity and role.
☐ **Can you verify all of this with documentation and logs?**	**Yes** CyberQP provides audit-ready evidence aligned with CMMC, NIST, and HIPAA frameworks, plus a Shared Responsibility Matrix for MSPs.

CyberQP

When “Yes” Isn’t Verifiable

Underwriters don’t just want the right answers; they want proof. We’ve seen applications approved on paper but denied at claim time because MFA, PAM, or access controls couldn’t be verified.

> I spoke with an MSP partner whose application missed an MFA requirement, and their client was later denied a ransomware claim. Your answers must be correct, complete, and verifiable.
>
> — Stephan Tomecko, Director of Partner Success at CyberQP

If you can’t produce evidence, your coverage may not apply when you need it most.

Make It Easy on Yourself

The application process doesn’t have to be so daunting. CyberQP maps identity and access controls directly to underwriting requirements, ensuring your answers are accurate, defensible, and ready when carriers or auditors request proof.

Let CyberQP do the heavy lifting for you.

CyberQP

Take the Next Step

- [ ] Download the CyberQP CMMC Shared Responsibility Matrix
- [ ] CIS Product Mapping
- [ ] NIST Product Mapping
- [ ] HIPAA Product Mapping
- [ ] ISO Product Mapping
- [ ] Schedule a 15-min consultation to verify you're ready for the next policy cycle

Glossary: Know the Terms

Privileged Access Management (PAM)

The practice of controlling, monitoring, and securing access to systems and data by users with elevated permissions. CyberQP enables scalable PAM for IT environments where admin access must be tightly governed.

Multi-Factor Authentication (MFA)

A security method requiring users to verify identity using two or more methods, such as a password and a mobile code, before granting access. Required by most insurers for admin, remote, and email access.

Service Accounts

Non-human accounts used by applications, scripts, or automated services to interact with systems. These accounts often go unmanaged and unmonitored, making them a common blind spot in audits.

Audit-Ready Evidence

Logs, policies, reports, and mappings that demonstrate security controls are active, effective, and reviewed. CyberQP packages evidence in a format aligned with common compliance and insurance needs.

Shared Responsibility Matrix (SRM)

A framework used to define ownership of security tasks and controls between MSPs and their clients. CyberQP's SRM is purpose-built to support CMMC and insurer documentation workflows.

Compliance Frameworks

Regulatory or best-practice standards such as CMMC, HIPAA, and NIST 800-171 that outline required security controls. Many cyber insurers align their questionnaires with one or more of these.