

CHECKLIST

Cyber Insurance Evidence Checklist

Gather these records before your next application or renewal.

Cyber insurance applications ask what security controls you have. Every answer is a statement your organization signs, so it should match a record you can produce. Use this checklist to see what you can already prove and what is missing. Requirements vary by carrier and policy; confirm specifics with your broker.

Governance and documents

- ☐ Written information security program (WISP), with the date it was last reviewed
- ☐ Named person responsible for the security program
- ☐ Current risk assessment, written and dated
- ☐ Acceptable Use Policy with employee acceptance records
- ☐ Inventory of your most critical data and where it lives

Identity and email

- ☐ Multi-factor authentication (MFA) settings report for email, remote access and administrator accounts, with any exceptions listed
- ☐ Email domain protection review: Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC)
- ☐ List of administrator accounts and who holds them

People

- ☐ Security awareness training completion records for all staff
- ☐ Onboarding training records for new hires
- ☐ Phishing simulation results, if you run them (at BTI these come from the separate [email security and security awareness training](https://www.btigroup.com/it-services/cybersecurity/email-security-awareness-training/) service, not Cyber Watch: www.btigroup.com/it-services/cybersecurity/email-security-awareness-training/)

Note: BTI is not an insurance agency and does not decide coverage or pricing. Confirm requirements with your broker.

Testing and vulnerability management

- ☐ Recent vulnerability scan results, internal and external
- ☐ Most recent penetration test report, with the date and who performed it
- ☐ Remediation records and retest results for each finding
- ☐ Documented risk acceptances for anything not fixed, with owner and review date

Response and recovery

- ☐ Written incident response plan with roles, contacts and escalation steps
- ☐ Record of the last time the plan was reviewed or updated
- ☐ Evidence that backups exist and that a restore was tested (ask your IT provider)

Vendors

- ☐ List of vendors with access to your systems or data, and how they are reviewed

Tip: If an honest answer is "mostly yes", write down the exceptions. An accurate answer with noted gaps is easier to defend than an optimistic one.

Abbreviations used: WISP, written information security program. MFA, multi-factor authentication. SPF, DKIM and DMARC, email authentication records for your domain. FTC, Federal Trade Commission.

BTI Cyber Liability Essentials keeps the documents. Cyber Watch adds independent testing and the records to prove it.

[Book a free consultation](https://www.btigroup.com/freeconsultation/)

<https://www.btigroup.com/freeconsultation/>
BTI Communications Group | Los Angeles main 562-298-5000 | www.btigroup.com

KNOW THE DIFFERENCE

Pen test vs vulnerability scan

They answer different questions. Your insurer may ask about both.

Compared	Vulnerability scan	Penetration test
Question it answers	Where are known weaknesses?	Could an attacker get in, and how far?
How it works	Automated check against lists of publicly known issues	Authorized, simulated attack that tries to exploit and chain weaknesses
Exploits findings?	No	Yes, in controlled, non-destructive steps
Output	List of potential issues ranked by severity	Proven attack paths, evidence and prioritized fixes
Best for	Frequent, broad checks	Proving real-world impact
In Cyber Watch	Monthly, internal and external	Quarterly, plus retest after fixes

External test: starts from the internet and checks whether an outsider could get in.

Internal test: assumes the attacker is already inside and measures how far they could move.

What a useful pen test record includes

1. Scope and written authorization
2. Leadership summary in plain language
3. Findings ranked by risk, with recommended fixes
4. Attack path detail
5. Signed, reproducible evidence
6. Retest results
7. A record across quarters that shows the trend

How often?

Common practice is at least once a year and after major changes. Some rules set a minimum, for example the Federal Trade Commission (FTC) Safeguards Rule for covered businesses. Cyber Watch tests quarterly because results age quickly.

Where BTI fits

Cyber Liability Essentials is the required foundation for BTI managed security clients: your WISP, policy templates for internal work, incident response plan and an evidence locker for your compliance program, if you have one. Cyber Watch adds recurring testing by an independent testing partner, monthly scans, quarterly Microsoft 365 analysis and the governance tools to keep it all current.

Cyber Watch testing is done remotely through agents installed on your machines, so no one needs to be on site, and each quarterly test ends with a readout with BTI.

Phishing simulations are not part of Cyber Watch; they are part of BTI's separate [email security and security awareness training](https://www.btigroup.com/it-services/cybersecurity/email-security-awareness-training/) service (www.btigroup.com/it-services/cybersecurity/email-security-awareness-training/).

Sources: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115 (csrc.nist.gov/pubs/sp/800/115/final); FTC Safeguards Rule guide (ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know).

[Book a free consultation](https://www.btigroup.com/freeconsultation/)

<https://www.btigroup.com/freeconsultation/>
BTI Communications Group | Los Angeles main 562-298-5000 | www.btigroup.com