ITVORTEX
SIMPLIFY. PROTECT. EVOLVE.

FREE RESOURCE · MAY 2026

The Cyber Insurance Readiness Playbook.

The 14 controls modern underwriters actually require, the documentation they expect to see, and the step-by-step path to a passing renewal questionnaire. Without panic-buying tools you do not need.

UNIVERSAL TIER
5
controls every carrier requires before quoting

CRITICAL TIER
5
controls that move premiums up or down materially

GOVERNANCE
4
controls that prove your program actually runs

PATH TO RENEWAL
90 days
week-by-week roadmap to renewal-ready

ITV-CIRP-2026 · v1.0

The renewal questionnaire is the audit.

Cyber underwriting changed for good around 2022. The form your broker hands you each year is no longer a marketing exercise. It is a documented attestation that drives the quote, the exclusions, and whether the carrier even wants to bind the policy at all.

01 Why modern underwriters reject more applications than they approve

EVIDENCE-BASED UNDERWRITING

Carriers learned hard lessons from the 2020-2022 ransomware wave. Loss ratios spiked, capacity tightened, and the entire market shifted to **evidence-based underwriting**. The questionnaire stopped being a series of yes/no boxes you self-attest to and became a structured discovery of whether you actually run the controls you claim to run.

Roughly three out of every four carriers now run **external attack surface scans** against your perimeter before quoting. They see your exposed RDP, your unpatched edge devices, your weak DMARC posture, your forgotten subdomain, and your vendor data leak history before your broker even submits the application. The "no" comes back before you can clarify.

The good news: the controls that get you to renewal-ready are **finite, named, and largely the same across carriers**. Get them right and you move from declined to quoted to favorably priced. This playbook is the map.

02 What the data says about the market right now

2024-2026 INDUSTRY RESEARCH

~75%

of carriers run external attack surface scans before quoting, and adjust the offer based on what they find.

Industry consensus, 2024 carrier surveys

15-20%

projected cyber premium growth in 2026 as demand outpaces capacity for evidence-light applicants.

S&P Global Ratings, 2025 outlook

20-40%

premium swing between an evidence-rich applicant and an evidence-light one with the same revenue and industry.

Broker estimates, mid-market segment

03 How to use this playbook

8 PAGES · 11 SECTIONS

A practitioner-facing playbook based on observed carrier behavior in the 2024-2026 mid-market cyber insurance segment. Not insurance advice. Specific control requirements and underwriting standards vary by carrier; work with a qualified broker and apply this playbook in coordination with your underwriter.

What the carrier already knows about you.

04 What the external scan picks up

BEFORE YOU SUBMIT ANYTHING

Modern cyber underwriters run external attack surface management tools against your perimeter as soon as your application lands. This is not a hack and it is not adversarial. It is the same data anyone with a credit card can pull about your environment from the outside, organized through the underwriter's risk model.

Here is what they actually see:

DMARC

Your published email authentication posture. **p=none** reads as ungoverned. **p=reject** reads as mature.

Resolved via public DNS lookup

Edge

Exposed services on your perimeter. Open RDP, unpatched VPN appliances, exposed admin panels each move the score.

Resolved via internet-wide port scans

Leaks

Your domain in known credential dumps and dark web sales. Stale employee credentials count against you.

Resolved via threat intelligence feeds

What this means for the playbook. Before the questionnaire even matters, your perimeter needs to be quiet. The cheapest premium reduction in the entire process is fixing the externally visible posture: enforce DMARC, close exposed admin services, rotate any credentials in public dumps. None of this costs money. All of it gets noticed.

05 The three-tier framework

14 CONTROLS · 3 TIERS

UNIVERSAL

5 controls. Carriers will not quote without all five. Missing one usually means the application is declined or the broker is asked to re-submit after remediation.

See page 4 for the full list

CRITICAL

5 controls. Carriers heavily weight these. Strong evidence here moves your premium down materially. Weak evidence moves it up, often with exclusions added.

See page 5 for the full list

GOVERNANCE

4 controls. Carriers use these to verify your program is operating, not just documented. Strong governance signals you would handle a claim well.

See page 6 for the full list

How the tiers interact. A perfect Universal Tier with a weak Critical Tier still gets you quoted, just at a higher premium with more exclusions. A strong Universal and Critical Tier with weak Governance still gets you a competitive quote, but the carrier may push for additional warranties or sub-limits on the most exposed coverage categories. The strongest premium leverage comes from running all three tiers in concert and producing the evidence quickly when asked.

External attack surface scan behavior reflects industry consensus across major cyber underwriters as of mid-2026. Specific scoring methodologies are proprietary to each carrier and vary in weight and inputs.

Universal Tier · five non-negotiables.

UNIVERSAL TIER · CONTROLS 01 THROUGH 05

Without these five, no quote.

Every carrier in the mid-market segment expects all five. Missing any one usually results in the application being declined or returned for remediation before quoting begins.

5 controls required

01 Multifactor Authentication

WANT TO SEE	**MFA enforced on email, VPN, all remote access, and every admin account.** Phishing-resistant methods (FIDO2, security keys) for privileged users.
DOCUMENTATION	Conditional access policy export. List of accounts excluded from MFA with business justification.
COMMON GAP	"MFA on most things" with quiet exceptions for service accounts, legacy applications, or VPN secondary auth.

02 EDR / MDR on every endpoint

WANT TO SEE	Endpoint detection and response deployed to **100% of workstations and servers**, with 24/7 monitoring or named incident response retainer.
DOCUMENTATION	Coverage report from the EDR console. SOC engagement letter or MDR statement of work.
COMMON GAP	Coverage gap on engineering or production workstations carved out for "performance reasons" months ago.

03 Immutable backups + tested restore

WANT TO SEE	Backups in **immutable storage or air-gapped media**. Restore tested at least annually with documented results. Offsite copy separate from production credentials.
DOCUMENTATION	Last restore test report. Backup configuration export showing retention and immutability settings.
COMMON GAP	"Backups run nightly" but no documented restore in the past 12 months, and production admin credentials can delete backup copies.

04 Written IR plan + recent tabletop

WANT TO SEE	Incident response plan reviewed within the past 12 months. **Tabletop exercise conducted** within the past 12 months with documented after-action report.
DOCUMENTATION	Current IR plan PDF. Tabletop AAR including scenario, participants, and decisions captured.
COMMON GAP	An IR plan exists somewhere as a Word document, but the last tabletop was the consultant onboarding three years ago.

05 Documented patch management

WANT TO SEE	Documented patch SLAs by severity. **Critical patches inside 15 days**, high-severity inside 30 days. Evidence of consistent execution against the SLA.
DOCUMENTATION	Patch policy document. Recent patch compliance report with SLA tracking.
COMMON GAP	Patches deploy regularly but there is no written SLA, so the questionnaire answer is "we patch" with no evidence of cadence.

Universal Tier requirements reflect carrier consensus across the mid-market segment. Specific thresholds (such as patch SLA windows) vary by carrier and may be tightened during a hardening cycle.

Critical Tier · where the premium moves.

CRITICAL TIER · CONTROLS 06 THROUGH 10

Strong evidence here drops the premium.

Carriers heavily weight these five. A well-documented Critical Tier is the difference between a quote that lands at market and one that lands at a meaningful discount.

5 controls weighted heavily

06 Privileged Access Management

WANT TO SEE	Admin credentials **vaulted**, just-in-time elevation for privileged actions, session recording for high-risk admin work, no shared admin accounts.
DOCUMENTATION	PAM tool configuration. List of named privileged accounts. JIT elevation policy.
COMMON GAP	Standing local admin rights on workstations, or a shared "IT_Admin" account that three people know the password for.

07 Email security stack

WANT TO SEE	**DMARC at p=reject**, attachment sandbox, URL rewrite, business email compromise detection. Phishing simulation results tracked.
DOCUMENTATION	DNS records for SPF/DKIM/DMARC. Email security gateway configuration export.
COMMON GAP	DMARC published at p=none for the past 18 months because "we did not want to break anything" during the testing phase.

08 Network segmentation

WANT TO SEE	**Corporate isolated from operational technology.** Production isolated from development. East-west traffic monitored. Lateral movement controls in place.
DOCUMENTATION	Network diagram with zone boundaries. Firewall rule audit. Microsegmentation policy if applicable.
COMMON GAP	Flat /16 network where the receptionist's PC can route directly to the SCADA gateway or the finance database.

09 Vulnerability management program

WANT TO SEE	Recurring vulnerability scans on a documented cadence. **Risk-ranked remediation SLAs.** Evidence that critical and high findings are closed inside SLA.
DOCUMENTATION	Scan tool dashboard export. Last quarter's remediation tracking.
COMMON GAP	Scans run quarterly but findings sit open for 9 months because nobody owns the remediation tracking.

10 Endpoint encryption (FDE)

WANT TO SEE	**Full-disk encryption on every laptop and desktop.** Recovery keys escrowed centrally. Encryption enforced via MDM, not user-initiated.
DOCUMENTATION	MDM compliance report showing encryption status. Key escrow location.
COMMON GAP	BitLocker available, but not enforced. Some users have it, some do not, and nobody knows which lost laptop fell into which category.

Critical Tier controls reflect the categories carriers most consistently use to differentiate premiums between applicants. Verification depth varies by carrier and by primary line size.

Governance Tier • proving the program actually runs.

GOVERNANCE TIER · CONTROLS 11 THROUGH 14

The carrier is asking: can you operate this?

These four controls signal that the program is alive, monitored, and improving. Carriers use this evidence to model how well you would handle a real claim.

4 controls operational

11 Phishing simulation + awareness training

WANT TO SEE	**Quarterly phishing simulations.** Annual baseline awareness training. Failure rate tracked and remediated. Role-based content for finance and IT.
DOCUMENTATION	Simulation results from the past 12 months. Training completion records.
COMMON GAP	Annual training compliance at 96%, but no phishing simulations have run because "we did not want to demoralize the team."

12 Vendor / third-party risk management

WANT TO SEE	Vendor inventory with risk tier. **SOC 2 or ISO 27001 attestations** on file for critical vendors. Annual review cadence documented.
DOCUMENTATION	Vendor register with attestation status and last review date.
COMMON GAP	A vendor list exists in a spreadsheet, but no one tracks when SOC 2 reports expire, so several critical vendors are quietly out of compliance.

13 Centralized logging / SIEM

WANT TO SEE	**Logs aggregated centrally** from identity, endpoint, network, and cloud. Documented retention. Alerts triaged by a SOC, internal or managed.
DOCUMENTATION	SIEM source inventory. Retention policy. Alert response runbook.
COMMON GAP	Logs collected but never reviewed. The SIEM exists, but nobody acts on the alerts overnight or on weekends.

14 Cyber insurance program management

WANT TO SEE	A **named insurance program owner**. RACI for claim notification. Evidence package maintained year-round, not built in a panic at renewal.
DOCUMENTATION	Insurance binder summary. Claim notification process document. RACI matrix.
COMMON GAP	Nobody knows who calls the carrier at 2am during a ransomware incident, so the first call goes to legal counsel instead.

What "governance" actually means to an underwriter. The carrier is trying to predict how your team behaves on Day Zero of a claim. Strong governance evidence signals you would call the carrier inside the notification window, preserve evidence properly, and follow the incident response process they expect to see in the post-incident review. Weak governance evidence signals the opposite. The premium difference reflects that prediction.

Governance Tier controls are the operational evidence underwriters use to differentiate between programs that exist on paper and programs that run in practice.

What the question actually asks.

09 Three question patterns and how to answer them

RENEWAL QUESTIONNAIRE

PATTERN 01 / THE YES-BUT-ACTUALLY-PARTIAL TRAP

"Is multifactor authentication enforced on all administrative accounts?"

WEAK ANSWER

"Yes." The carrier follows up. You explain that MFA is enforced "for most administrative accounts" with carve-outs for three service accounts and a legacy ERP integration. The underwriter now flags the application as inconsistent with the attestation, which materially harms the quote.

STRONG ANSWER

"Yes, with the following documented exceptions: three service accounts using IP allowlist as the compensating control, and one legacy ERP integration scheduled for retirement in Q3." The honesty reads as program maturity. The exceptions read as managed risk, not blind spots.

PATTERN 02 / THE CADENCE QUESTION

"When was your last incident response tabletop exercise?"

WEAK ANSWER

"In the past year." No date. No participants. No scenario. The underwriter reads this as a check-box answer and weighs the control downward.

STRONG ANSWER

"March 14, 2026. Scenario: ransomware on production ERP. Participants: CEO, CFO, GC, CISO, IT Director. After-action report attached as Exhibit C." Specific. Recent. Documented. The carrier moves on.

PATTERN 03 / THE COMPENSATING CONTROL QUESTION

"Are all endpoints covered by an EDR solution?"

WEAK ANSWER

"Yes, except some manufacturing endpoints." No explanation of what compensates for the gap. The carrier assumes the worst and prices accordingly, or adds a sub-limit on operational technology coverage.

STRONG ANSWER

"All corporate endpoints, 100%. Production-floor HMI workstations excluded due to vendor compatibility, with the following compensating controls: full network segmentation, no internet egress, removable media policy, daily integrity verification." The gap is named, the compensation is concrete.

The principle behind all three patterns. Carriers prefer honest specificity over checkbox confidence. The questionnaire is not a test you pass by saying yes. It is a structured conversation about how your program actually operates, and the carriers who score you have seen every flavor of evasion before. Honesty plus documentation almost always beats over-claiming, even when honesty surfaces gaps.

Questionnaire patterns are illustrative of common renewal forms across the mid-market segment. Your specific carrier's questionnaire and follow-up protocol may vary in structure and emphasis.

90 days to renewal-ready.

10 The 90-day path

WEEK BY WEEK

DAYS 1-30

Audit and close the obvious gaps

- **Week 1:** External attack surface scan against your own perimeter, using a free tool or a broker-provided service.
- **Week 2:** MFA coverage audit. Find every exception, document the compensating control, plan retirement.
- **Week 3:** EDR coverage audit. Identify every endpoint without the agent and plan rollout.
- **Week 4:** Backup restore test. Document the result whether good or bad. A bad result with a plan reads better than no test at all.

DAYS 31-60

Run the program and build evidence

- **Week 5:** Tabletop exercise on a realistic scenario. Capture the after-action report.
- **Week 6:** Vulnerability scan with documented remediation SLAs. Close critical and high findings.
- **Week 7:** DMARC moved to p=quarantine or p=reject after testing. Email security stack reviewed.
- **Week 8:** Vendor inventory refresh. Pull updated SOC 2 reports for the top 10 vendors.

DAYS 61-90

Package and submit

- **Week 9:** Build the evidence package. Pull every report, policy, and configuration export the questionnaire will ask for.
- **Week 10:** Broker walk-through of the questionnaire. Identify any remaining red flags and final fixes.
- **Week 11:** Final review with the IR program owner. Sign attestations. Submit.
- **Week 12:** Underwriter follow-up. Have the evidence package ready for any drill-down questions.

11 What you do NOT need to buy

AVOID THE PANIC PURCHASE

- ✕ **A second EDR.** One properly configured EDR with documented coverage beats two competing tools running side by side.
- ✕ **A SOAR platform.** Useful for mature SOCs, not required for a passing application. Skip unless the operational case stands on its own.
- ✕ **Penetration testing in the renewal week.** A pen test reveals findings you cannot close before submission, which reads worse than not testing yet.
- ✕ **A standalone DLP appliance.** Carriers want to see **data classification**, not a specific product category. The work matters more than the tool.
- ✕ **"AI-powered" anything as a separate purchase.** The features matter, not the marketing label.
- ✕ **Zero-trust as a product.** Carriers want segmentation, identity, and conditional access. Buy the controls, not the rebranded bundle.