CONFIDENTIAL · PREPARED FOR ACME CAPITAL (DEMO)

CARRIER · COALITION CYBER

Coalition Cyber cyber-insurance auto-fill

A pre-completed cyber-insurance questionnaire for Acme Capital (demo), sourced directly from intake answers, configuration-review findings, and posture telemetry. Every answer carries a confidence rating and a premium-impact signal so the broker can underwrite from defensible data.

16	1	7	17
AUTO-FILLED	CISO TO CONFIRM	PREMIUM-LOADED	QUESTIONS
definite + inferred answers	human-required prompts	fix before binding	Coalition Cyber

DEMO — NOT YOUR TENANT DATA

This document was generated from CyberTwin's Acme Capital reference fixture so prospects can evaluate the artefact format. It is not derived from your environment. Do not circulate as if it were your own tenant's assessment.

ORGANIZATION

Acme Capital (demo)

17 questions across 8 sections

AUTO-FILLED

94%

01 Executive summary

The CISO + broker read this page before underwriting.

This packet pre-fills the Coalition Cyber cyber-insurance questionnaire for Acme Capital (demo). **16 of 17** questions (94%) were filled directly from intake + configuration data. **1** require CISO sign-off before submission. **7** answers are likely to load the premium — each is flagged in the premium-impact section with a remediation suggestion.

94%	1	7	8
AUTO-FILL RATE	CISO SIGN-OFF	PREMIUM-LOADED	SECTIONS
16 / 17	human-required answers	fix before binding	Coalition Cyber

How to read this packet

Each answer carries two tags:

· **Confidence** Definite (direct intake / config), Inferred (chained calculation), or Human-required (CISO to fill).
· **Premium signal** Helpful (positive control evidence), Neutral (informational), or Loaded (likely to push premium up).

PREMIUM IMPACT

7 premium-loaded answers above the carrier's underwriting threshold. Closing the MFA-on-admin gap (q-mfa-admin) and standing up 24/7 SOC monitoring (q-edr-alerting) are the two highest-impact fixes before binding — Coalition typically discounts 12-18% combined when both are addressed. The IR-plan-not-tabletoped gap is straightforward to close in a single afternoon and removes another loading factor.

Sections in this packet

· Identity & access (4 questions)
· Endpoint protection (3 questions)
· Network (2 questions)
· Data (2 questions)
· Backup & recovery (2 questions)
· Ransomware (3 questions)

- Awareness & training (1 questions)
- Third-party (1 questions)

02 Premium impact

Answers ranked by premium-loading weight. Closing the top items before binding has the highest probability of premium reduction.

#	QUESTION	ANSWER	WEIGHT	SIGNAL
#1	Is MFA enforced for all administrative accounts? A "no" here typically loads premium 15-30%. The single highest-impact fix before binding.	No — CloudOps group is excluded from the admin CA policy	5/5	Loaded
#2	Are EDR alerts monitored 24/7 by a SOC? Without 24/7 SOC monitoring, MTTD on credential theft + ransomware extends from minutes to hours.	No — alerts route to a shared inbox; no 24/7 monitoring	4/5	Loaded
#3	What percentage of users have MFA enforced? Carriers price MFA gaps directly. <95% typically loads premium 8-15%.	88%	5/5	Loaded
#4	When was your last full disaster-recovery drill? Carriers want a drill within the last 12 months.	Q3 2024 — over 12 months ago	4/5	Loaded
#5	Is there a documented IR plan tabletop-tested in the last 12 months? Tabletop within 12 months is a positive signal.	IR plan exists but no tabletop in the last 12 months	4/5	Loaded
#6	Are critical vendors reviewed annually for security posture?	No — sub-processors listed but not reviewed annually	3/5	Loaded
#7	Is annual phishing-simulation training enforced?	Partial — Engineering team only (47 of 220 users)	3/5	Loaded

The top three to close before binding

#1 · WEIGHT 5/5 · LOADED

Is MFA enforced for all administrative accounts?

Current answer: No — CloudOps group is excluded from the admin CA policy

A "no" here typically loads premium 15-30%. The single highest-impact fix before binding.

#2 · WEIGHT 4/5 · LOADED

Are EDR alerts monitored 24/7 by a SOC?

Current answer: No — alerts route to a shared inbox; no 24/7 monitoring

Without 24/7 SOC monitoring, MTTD on credential theft + ransomware extends from minutes to hours.

#3 · WEIGHT 5/5 · LOADED

What percentage of users have MFA enforced?

Current answer: 88%

Carriers price MFA gaps directly. <95% typically loads premium 8-15%.

Identity & access

4 questions in this section. Each carries its source + confidence.

`q-mfa-coverage` Inferred Loaded weight 5/5

What percentage of users have MFA enforced?

Carriers price MFA gaps directly. <95% typically loads premium 8-15%.

ANSWER

88%

EVIDENCE

· entra-ca-policies
· tenant-stats: 197/220 users registered for MFA
· CloudOps group (23 users) excluded

`q-mfa-admin` Definite Loaded weight 5/5

Is MFA enforced for all administrative accounts?

A "no" here typically loads premium 15-30%. The single highest-impact fix before binding.

ANSWER

No — CloudOps group is excluded from the admin CA policy

EVIDENCE

· entra-ca-exclude-001
· AWS-iam-admin-mfa-001 (cloudops-admin user lacks console MFA)

`q-sso` Definite Helpful weight 4/5

Is SSO enforced for SaaS applications handling regulated data?

SSO + SCIM provisioning is a positive control signal.

ANSWER

Yes — Okta SSO + SCIM provisioning across 22 SaaS apps

EVIDENCE

· intake: identity.sso_enforced=true
· okta-app-list (22 apps)

`q-password-policy` Definite Helpful weight 3/5

Does the password policy meet NIST 800-63B guidance?

NIST-aligned password policies are a baseline expectation.

ANSWER

Yes — NIST 800-63B aligned (12-char min, breach-list check, no rotation)

EVIDENCE

· intake: identity.password_policy=nist_aligned

E Endpoint protection

3 questions in this section. Each carries its source + confidence.

q-edr-coverage **Inferred** **Helpful** weight 4/5

What percentage of endpoints run a modern EDR?

EDR coverage <90% loads premium. 100% is a positive signal.

ANSWER

96% (212 of 220 endpoints)

EVIDENCE

· mde-tenant-stats: 212 active sensors
· asset-inventory: 220 endpoints

q-edr-alerting **Definite** **Loaded** weight 4/5

Are EDR alerts monitored 24/7 by a SOC?

Without 24/7 SOC monitoring, MTTD on credential theft + ransomware extends from minutes to hours.

ANSWER

No — alerts route to a shared inbox; no 24/7 monitoring

EVIDENCE

· intake: ops.soc_24×7=false
· CC7.2 audit-evidence gap

q-asr-rules **Definite** **Helpful** weight 3/5

Are MS Defender ASR rules enforced (not in audit mode)?

Microsoft hardening guidance.

ANSWER

Yes — 14 of 16 ASR rules in block mode

EVIDENCE

· mde-asr-policy: 14 rules in block mode, 2 in audit mode

N Network

2 questions in this section. Each carries its source + confidence.

q-segmentation **Definite** **Helpful** weight 4/5

Are production environments network-segmented from corporate?

Lateral-movement defence.

ANSWER

Yes — FortiGate VDOMs separate corp + prod + DMZ

EVIDENCE

· fortinet-vdom-config

q-external-scan **Definite** **Helpful** weight 3/5

Is the external attack surface continuously scanned?

ANSWER

Yes — daily scans via Tenable + Coalition Control

EVIDENCE

· intake: ops.external_attack_surface_scan=true

D Data

2 questions in this section. Each carries its source + confidence.

q-pii-volume **Definite** **Neutral** weight 3/5

Approximate count of PII records held?

ANSWER

~145,000 customer PII records

EVIDENCE

· intake: data.pii_records=145000

q-data-encryption **Definite** **Helpful** weight 3/5

Is sensitive data encrypted at rest with customer-managed keys?

ANSWER

Yes — AWS KMS customer-managed keys for prod databases + S3

EVIDENCE

· aws-kms-policy
· intake: data.cmk=true

B Backup & recovery

2 questions in this section. Each carries its source + confidence.

q-backup-immutable Definite Helpful weight 4/5

Are backups immutable / WORM?

Immutable backups defeat ransomware double-extortion playbooks.

ANSWER

Yes — S3 Object Lock (governance, 90 days) + Veeam Insider Protection

EVIDENCE

· intake: backup.immutable=true
· aws-s3-objectlock-policy
· veeam-config

q-recovery-drill Definite Loaded weight 4/5

When was your last full disaster-recovery drill?

Carriers want a drill within the last 12 months.

ANSWER

Q3 2024 — over 12 months ago

EVIDENCE

· intake: bcdr.last_drill=2024-Q3

R Ransomware

3 questions in this section. Each carries its source + confidence.

q-rw-payment **Definite** **Helpful** weight 5/5

Has the organisation paid ransom in the last 24 months?

Prior payment loads premium materially.

ANSWER

No — no ransom payments in the period

EVIDENCE

· intake: incidents.ransom_paid_24mo=false

q-ir-plan **Definite** **Loaded** weight 4/5

Is there a documented IR plan tabletop-tested in the last 12 months?

Tabletop within 12 months is a positive signal.

ANSWER

IR plan exists but no tabletop in the last 12 months

EVIDENCE

· intake: ir.tabletop_in_12mo=false
· CC7.3 audit-evidence partial

q-ir-retainer **Human-required** **Neutral** weight 4/5

Is an IR firm on retainer with documented response time?

ANSWER

— (CISO to confirm before submission)

CISO PROMPT

If you have an IR retainer, document the firm + response-time SLA. If not, plan to engage one before binding — Coalition discounts 5-10% when an IR retainer with documented SLA is in place.

A Awareness & training

1 question in this section. Each carries its source + confidence.

`q-phishing-training` **Definite** **Loaded** weight 3/5

Is annual phishing-simulation training enforced?

ANSWER

`Partial — Engineering team only (47 of 220 users)`

EVIDENCE

· intake: training.phishing_sim=engineering_only
· CC1.4 audit-evidence partial

T Third-party

1 question in this section. Each carries its source + confidence.

q-vendor-review **Definite** **Loaded** weight 3/5

Are critical vendors reviewed annually for security posture?

ANSWER

No — sub-processors listed but not reviewed annually

EVIDENCE

· intake: vendor.annual_review=false
· CC9.2 audit-evidence gap

CLOSING · DECISIONS REQUESTED

Broker negotiating asks

The top 3 premium-loaded answers in this fill. Each one is either a control to remediate before binding (preferred) or a context the broker should pitch the carrier on (alternative).

1. Is MFA enforced for all administrative accounts?

Current answer: No — CloudOps group is excluded from the admin CA policy. A "no" here typically loads premium 15-30%. The single highest-impact fix before binding.

Owner: Broker + CISO **By:** Before carrier submission **Cost:** Premium weight 5/5

2. Are EDR alerts monitored 24/7 by a SOC?

Current answer: No — alerts route to a shared inbox; no 24/7 monitoring. Without 24/7 SOC monitoring, MTTD on credential theft + ransomware extends from minutes to hours.

Owner: Broker + CISO **By:** Before carrier submission **Cost:** Premium weight 4/5

3. What percentage of users have MFA enforced?

Current answer: 88%. Carriers price MFA gaps directly. <95% typically loads premium 8-15%.

Owner: Broker + CISO **By:** Before carrier submission **Cost:** Premium weight 5/5

Methodology + sources

How every answer was derived.

CITATION PATTERN

This pack uses **per-answer source-confidence labels + carrier-filtered end-of-document bibliography**. Audience: brokers preparing to submit to the underwriter, who need to defend each answer when challenged. Per-answer source labels (definite / inferred / human-required) let the broker know which answers will hold under questioning; the bibliography names the carrier application form so the underwriter knows which form-version this fill maps to.

Confidence ratings

DEFINITE

Direct read from intake or aggregate finding

Example: 'MFA enforced organisation-wide' from intake key identity.mfa_enforcement.

Source

INFERRED

Derived from a chained calculation with citation

Example: 'EDR coverage 95%' derived from endpoint_count × edr_deployed_count.

Source

HUMAN-REQUIRED

Flagged for the CISO to fill in their own words

Intake didn't cover it; the carrier asks specifics that need a person.

Source

Premium signal

We classify each answer's likely effect on the premium based on the carrier's public underwriting heuristics:

- **Helpful** — positive control evidence (typically a discount factor)
- **Neutral** — informational, no rate effect
- **Loaded** — "no" answer that increases the rate; ranked first in the premium-impact section

Carrier coverage

Carrier question catalogs reflect the public 2024 / 2025 forms for AIG CyberEdge, Chubb CERM, Beazley Breach Response, Coalition Cyber, and At-Bay Cyber. Common questions (cross-carrier) are included in every fill. CyberTwin does not represent or guarantee that auto-filled answers will be accepted by the carrier without underwriter review.

Provenance + freshness

SOURCE FINGERPRINT

`f3b9d4-13f-12i`

DOCUMENT HISTORY

VERSION	GENERATED	ENGINE	ENVIRONMENT	CHANGES
–	5/7/2026, 12:00:00 PM	`cybertwin-engine 0.1.0`	`acme-capital-(demo)`	Generated

FULL METHODOLOGY

cybertwin.io/methodology — the full catalog of entries, calibration sources, and cross-vendor stitching rules behind the numbers in this report.

SIGNATURES

Prepared by CyberTwin
CyberTwin Engine
Date: 5/7/2026
Auto-generated from tenant evidence; not warranted as the carrier-final answer set.

Reviewing broker
Date: _____
Sign on behalf of the broker acknowledging review before underwriter submission.

Cyber-Insurance Auto-Fill prepared by CyberTwin · Generated 5/7/2026, 12:00:00 PM

APPENDIX · GLOSSARY

Glossary of terms

Definitions for technical terms used throughout this report. Citations link to the source authority for each definition where applicable.

ALE	Annualized Loss Expectancy. The expected dollar loss per year from a given threat, computed as breach probability × impact. Reported as p10 / p50 / p90 (best / median / worst case) to make the variance honest. *NIST SP 800-30 Rev 1 risk-assessment methodology.*
EDR	Endpoint Detection and Response. Defender for Endpoint, CrowdStrike Falcon, SentinelOne, etc. Distinguished from "AV" by behavioral detection + investigation tooling beyond signature-based malware blocking.
MFA	Multi-Factor Authentication. CyberTwin distinguishes basic MFA (SMS, push) from "phishing-resistant MFA" (FIDO2 / WebAuthn / smartcards) — the latter satisfies stricter framework controls.
MITRE ATT&CK	Adversary tactics + techniques knowledge base maintained by MITRE. CyberTwin annotates every attack-path edge with a tactic code (TA0001 Initial Access, TA0008 Lateral Movement, etc.) and a technique code (T1078.004 Valid Accounts: Cloud Accounts, T1190 Exploit Public-Facing Application, etc.), sourced from the v15.1 Enterprise matrix. Every technique cited in this report traces to a specific edge — the codes are not a fixed count. *attack.mitre.org/matrices/enterprise*
POSTURE SCORE	A 0–100 score CyberTwin computes per Configuration Review upload reflecting the percentage of vendor-baseline checks the configuration passes weighted by severity. 100 = passes every check at the deepest depth available; 0 = fails every check.

APPENDIX · BIBLIOGRAPHY

Sources cited

Authoritative sources backing the claims in this report. Primary-source documents, published benchmarks, and vendor-cited references. Inline-cited sources throughout the body trace back to entries here.

AICPA Trust Services Criteria
2017 with 2022 points of focus
https://www.aicpa-cima.com/resources/landing/trust-services-criteria
Accessed 2026-04-01

CIS Critical Security Controls v8
https://www.cisecurity.org/controls/v8
Accessed 2026-04-01

Coalition Cyber Risk Application
Accessed 2026-04-01

HIPAA Security Rule
45 CFR Part 164, Subpart C
https://www.hhs.gov/hipaa/for-professionals/security/index.html
Accessed 2026-04-01

IBM Cost of a Data Breach Report 2025
industry-baseline ALE inputs
https://www.ibm.com/security/data-breach
Accessed 2026-07-01

ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection
https://www.iso.org/standard/27001
Accessed 2026-04-01

ISO/IEC 27002:2022
Information security controls — Annex A reference
https://www.iso.org/standard/75652.html
Accessed 2026-04-01

NCA ECC v2
Saudi Arabia National Cybersecurity Authority Essential Cybersecurity Controls
https://nca.gov.sa/ecc
Accessed 2026-04-01

NIST Cybersecurity Framework v2.0
https://www.nist.gov/cyberframework
Accessed 2026-04-01

NIST SP 800-53 Rev 5
Security and Privacy Controls for Information Systems
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
Accessed 2026-04-01

PCI DSS v4.0
Payment Card Industry Data Security Standard
https://www.pcisecuritystandards.org/document_library
Accessed 2026-04-01

PDPL-KSA SDAIA Implementing Regulations
Saudi Personal Data Protection Law
https://sdaia.gov.sa/pdpl
Accessed 2026-04-01

SAMA Cybersecurity Framework v1.0
Saudi Arabian Monetary Authority
https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurityFramework
Accessed 2026-04-01