

MY FRACTIONAL CISO™

A service of Mission Cyber Group · myfractionalciso.com

Security Readiness Package Sample Deliverable Excerpt

A representative excerpt of the penetration test, shareable test summary letter, security gap readout, incident response plan, core policies, and vendor risk statement included in every Security Readiness Package.

Prepared for: Acme SaaS, Inc. (fictional company — illustrative purposes only)

Prepared by: Mission Cyber Group / My Fractional CISO™

Assessment scope: Up to 50 IP addresses or devices, automated penetration testing

Frameworks: NIST Cybersecurity Framework (CSF) 2.0 · SOC 2 Security criteria

Engagement: 2 weeks, fixed scope, fixed price



HOW TO READ THIS SAMPLE

What's Inside

A Security Readiness Package gives your team the test results and documents an enterprise security questionnaire asks for — in 2 weeks. This sample shows a representative excerpt of each deliverable so you can see the depth and format before you commit.

01	Executive Summary	Page 3
02	Penetration Test (excerpt)	Page 4
03	Penetration Test Summary Letter (excerpt)	Page 5
04	Security Gap Readout (excerpt)	Page 6
05	Incident Response Plan & Core Policies (excerpt)	Page 7
06	Vendor Risk Statement (excerpt)	Page 8
07	Questionnaire Working Session (excerpt)	Page 9
08	Next Steps	Page 10

A NOTE ON CONFIDENTIALITY

Every real engagement is confidential. Acme SaaS, Inc. and every finding, policy excerpt, and vendor in this sample are fictional and created for illustration only. Your actual deliverables will be built around your real environment, your real risks, and the real questionnaire in your inbox.

SECTION 01

Executive Summary

Acme SaaS, Inc. is a fictional 28-person Series A software company. A Fortune 500 prospect sent Acme a 120-question security questionnaire, due back in three weeks, and Acme had no security policies, no penetration test, and no one who owned security full time. Acme engaged Mission Cyber Group for a Security Readiness Package to get the test results and documents the questionnaire asked for.

Metric	Result
Assets tested	38 of 50 included IP addresses and devices (cloud infrastructure, corporate network, endpoints)
Technical findings	14 total — 2 Critical, 4 High, 8 Medium/Low
Security gap readout	11 of 30 sampled controls in place; top-10 prioritized fix list
Documents delivered	Test summary letter, incident response plan, 5 core policies, vendor risk statement, Board-ready one-page summary
Questionnaire support	60-minute working session mapping the new documents to the live questionnaire
Engagement duration	2 weeks, fixed scope, fixed price

The sections that follow show a representative excerpt of each deliverable. Full versions are provided in the actual engagement.

SECTION 02

Penetration Test

Automated penetration testing — not a vulnerability scanner. The test attempts the same attack paths an attacker would across your environment (up to 50 IP addresses or devices), then reports exactly what it was able to achieve.

Severity	Count	Example Category
CRITICAL	2	Default credentials, path to production deployment
HIGH	4	Internet-reachable database port, missing MFA on cloud console
MEDIUM/LOW	8	Outdated software versions, weak TLS settings

Below: two representative findings from the full report.

Finding #1 — Default Credentials on Internal Build Server

CRITICAL

Impact: Starting from a single workstation on the office network, the test signed in to a build server's admin console using factory-default credentials, then reached the pipeline that deploys code to production.

Recommendation: Change the default credentials today, restrict the console to single sign-on, and rotate every secret stored in the deployment pipeline.

Finding #2 — Staging Database Reachable from the Internet

HIGH

Impact: A staging database accepted connection attempts from any internet address. No data was accessed, but an attacker could try passwords against it indefinitely.

Recommendation: Limit access to the application servers only, and move staging behind the private network within 2 business days.

SECTION 03

Penetration Test Summary Letter

Enterprise customers ask whether you've had an independent penetration test — and some ask for the report. The summary letter answers that without exposing your detailed findings. It's written to share with customers and prospects.

MISSION CYBER GROUP

225 Wilmington West Chester Pike, Suite 202-177 · Chadds Ford, PA 19317

October 23, 2026

Re: Penetration Test Summary Letter — Acme SaaS, Inc. (fictional)

Mission Cyber Group confirms that it performed an automated internal/external penetration test of Acme SaaS, Inc.'s environment between October 13 and October 16, 2026, as described below.

Scope: 38 IP addresses and devices across cloud infrastructure, the corporate network, and endpoints.

Method: Automated attack-path testing that attempts exploitation of discovered weaknesses, with results reviewed by a CISSP-certified security engineer.

Results: 14 findings were identified and ranked by severity. Acme has a prioritized remediation plan, with Critical findings scheduled for remediation by October 30, 2026.

What this letter confirms: that the testing above was performed, on the scope, dates, and method stated. It does not confirm that the findings have been fixed, that the environment is free of vulnerabilities, or that Acme meets any compliance standard. It is not a certification, an audit opinion, or a SOC 2 report. Detailed findings are not included.

Sincerely,

[Name], [Title]

Mission Cyber Group | My Fractional CISO™

SECTION 04

Security Gap Readout

Your current controls, measured against NIST CSF 2.0 and the SOC 2 Security criteria, so you know exactly where you stand and what to fix first.

NIST CSF 2.0 Function	Status	What we found (illustrative)
Govern	PARTIAL	The CTO owns security informally; no written policies before this engagement
Identify	GAP	No current inventory of systems and devices
Protect	PARTIAL	MFA on email, but not on the cloud admin console
Detect	GAP	Logs are collected but not reviewed or alerted on
Respond	IN PLACE	Incident response plan delivered in this engagement
Recover	PARTIAL	Daily backups run; restores have never been tested

Top fixes (5 of 10 shown)

- Remove default credentials and rotate pipeline secrets (Critical finding #1)
- Enforce MFA on every cloud admin account
- Close internet access to the staging database
- Build a system and device inventory, and keep it current
- Test a full backup restore and record the result

SOC 2 readiness (illustrative): 11 of 30 sampled controls in place — early stage. The full readout includes a one-page, Board-ready summary you can present as-is.

SECTION 05

Incident Response Plan & Core Policies

Written around how your company actually operates — not a generic template. Each document is mapped to NIST CSF 2.0.

Incident Response Plan — Severity Tiers (excerpt)

RS.MA

Severity	Definition	Who is notified, and when
SEV 1	Confirmed unauthorized access to customer data	CEO and CTO within 15 minutes; affected customers per contract terms
SEV 2	Compromise of an internal system with no evidence of data access	CTO within 1 hour
SEV 3	Suspicious activity or a policy violation	Security owner within 1 business day

Core policy	NIST CSF 2.0
Information Security Policy	GV.PO
Access Control Policy (including MFA)	PR.AA
Acceptable Use Policy	GV.PO
Vendor Management Policy	GV.SC
Data Protection & Retention Policy	PR.DS

Access Control Policy — Section 2.3 (excerpt)

"Multi-factor authentication is required for every account with administrative access to production systems, the cloud console, and the source code repository. Exceptions require written approval from the CTO and are reviewed quarterly..."

SECTION 06

Vendor Risk Statement

Enterprise buyers want to know your vendors won't become their risk. We list your 10 most critical vendors and sub-processors, check each one's security attestation, and summarize it on one page.

Vendor (Fictional)	Data / Access Type	Risk Tier	Attestation Status
CloudHost Inc.	Production infrastructure	CRITICAL	SOC 2 Type II on file
IdentityHub	Single sign-on for all staff	CRITICAL	SOC 2 Type II on file
SupportDesk	Customer support tickets, PII	HIGH	ISO 27001 certificate expired — renewal requested
MetricsCo	Product analytics, no PII	LOW	Public security summary accepted

Statement excerpt

"Acme SaaS maintains an inventory of vendors and sub-processors with access to customer data. Each is assigned a risk tier, and critical vendors are required to provide a current SOC 2 Type II report or equivalent certification..."

SECTION 07

Questionnaire Working Session

Enterprise security questionnaires can stall a deal for weeks. In a 60-minute working session, we take the questionnaire in your inbox and map each key question to the Package document that answers it — so your team can respond accurately and confidently.

Sample Questionnaire Question	Prepared Response (illustrative)	Supporting Document
Do you conduct independent penetration testing?	Yes. An independent automated penetration test was completed in October 2026. A test summary letter is available on request.	Test summary letter
Do you have a documented incident response plan?	Yes. Our plan defines severity tiers, roles, and notification timelines, and is reviewed annually.	Incident response plan
Is MFA enforced for administrative access?	Yes. MFA is required for all administrative access under our Access Control Policy.	Access Control Policy
Can you provide a SOC 2 report?	Not yet. We completed a SOC 2 readiness assessment in October 2026 and are working through a prioritized plan.	Gap readout summary
How do you manage vendor risk?	Critical vendors are tiered by risk and required to provide current security attestations.	Vendor risk statement

Result for Acme SaaS (illustrative): the questionnaire went back with honest, documented answers and three supporting documents attached — instead of blank fields and a stalled deal.

SECTION 08

Next Steps

The Package answers today's questionnaire. When you're ready for a full security program, the entire Package fee is credited toward the next step.

1 • Security Readiness Package

2 weeks. Penetration test, summary letter, gap readout, incident response plan, core policies, vendor risk statement.

2 • GRC Launch Package

6 weeks. The full program: all core policies, a complete vendor review, and a Board-ready roadmap. Package fee credited toward this or Compliance Accelerate if started within 30 days.

3 • My Fractional CISO™ Retainer

Ongoing security executive support, continuous penetration testing, and questionnaire defense.

Add-On: Retest Your Fixes for \$1,500

After you fix your critical and high findings, we retest them and confirm which ones are closed, so you can show your customer the issues are resolved. Add it at the readout or anytime after.

You're Not Alone in the Room

A dedicated, CISSP-certified security engineer owns your Package from kickoff to readout. When your customer's security team has follow-up questions, you have someone who can answer them.

READY TO SEE WHAT THIS LOOKS LIKE FOR YOU?

Book a free 15-minute review, or reach out directly at info@missioncybergroup.com to discuss a Security Readiness Package for your company.

[Book Your Free 15-Minute Cybersecurity Review →](#)

Acme SaaS, Inc. is a fictional company created solely for illustrative purposes. No real client names, data, findings, environments, or vulnerabilities are represented anywhere in this document. This sample does not constitute an actual security assessment, audit opinion, or compliance certification.