SAMPLE DELIVERABLE — ILLUSTRATIVE ONLY. NOT AN ACTUAL CLIENT REPORT.

MY FRACTIONAL CISO℠

A service of Mission Cyber Group · myfractionalciso.com

GRC Launch Package
Sample Deliverable Excerpt

A representative excerpt from the Full Security & Compliance Program Buildout, Technical Environment Assessment, and Board-Ready Security Roadmap included in every GRC Launch Package engagement.

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

Prepared by: Mission Cyber Group / My Fractional CISO

Assessment scope: Up to 75 IPs, powered by Horizon3.ai NodeZero

Framework: NIST Cybersecurity Framework (CSF) 2.0

SAMPLE DELIVERABLE — ILLUSTRATIVE ONLY. NOT AN ACTUAL CLIENT REPORT.

HOW TO READ THIS SAMPLE

What's Inside

A full GRC Launch Package engagement produces a complete program, a full technical assessment across your environment, and a full board-ready roadmap — typically 30–40 pages in total. This sample shows a representative excerpt of each component so you can see the depth and format before you commit.

A NOTE ON CONFIDENTIALITY

Every real engagement is confidential. Acme SaaS, Inc. and every finding, policy excerpt, and roadmap item in this sample are fictional and created for illustration only. Your actual deliverable will be built entirely around your real environment, your real risks, and your real priorities.

SECTION 01

Executive Summary

Acme SaaS, Inc. is a fictional 35-person Series A software company preparing for its first SOC 2 Type II audit while closing two enterprise contracts, each requiring a completed security questionnaire. Acme engaged Mission Cyber Group for a full GRC Launch Package to build its security program, assess its technical environment, and produce a board-ready roadmap ahead of its Q1 board meeting.

Metric	Result
Assets assessed	62 of 75 licensed IPs (cloud infrastructure, endpoints, SaaS integrations)
Policies delivered	14 core policies mapped to NIST CSF 2.0
Technical findings	23 total — 3 Critical, 6 High, 14 Medium/Low
Roadmap horizon	90-day prioritized plan across 3 phases
Engagement duration	6 weeks, fixed scope

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

SECTION 02

Security & Compliance Program Buildout

Every policy is mapped directly to a NIST CSF 2.0 Function, tailored to how Acme actually operates — not a generic template. Below: two of the fourteen policies delivered in the full engagement.

GOVERN | IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

Access Control Policy PR.AA

Purpose: Defines how Acme grants, reviews, and revokes access to production systems, customer data, and internal tools.

Excerpt — Section 3.2, Access Review Cadence: "Access to production AWS accounts and the primary customer database shall be reviewed on a [redacted] basis by the [redacted]. Any account inactive for more than [redacted] shall be automatically flagged for revocation..."

Incident Response Policy RS.MA

Purpose: Establishes roles, escalation paths, and communication protocols during a security incident.

Excerpt — Section 2.1, Incident Severity Tiers: "A Severity 1 incident is defined as any event involving confirmed unauthorized access to customer data. Upon declaration, the [redacted] and [redacted] must be notified within [redacted]..."

Full engagement includes: Access Control, Incident Response, Data Classification, Vendor Risk Management, Acceptable Use, Business Continuity, Change Management, Asset Management, Password & Authentication, Security Awareness Training, Data Retention, Encryption Standards, Remote Work Security, and Third-Party Risk Assessment policies — all mapped to NIST CSF 2.0.

SECTION 03

Technical Environment Assessment

Powered by Horizon3.ai NodeZero — an autonomous penetration testing platform, not a vulnerability scanner. NodeZero actively attempts real attack paths across your environment (up to 75 IPs) the same way an attacker would, then reports exactly what it was able to achieve.

Severity	Count	Example Category
CRITICAL	3	Exposed credentials, unpatched remote access
HIGH	6	Weak password policies, missing MFA on admin accounts
MEDIUM/LOW	14	Outdated software versions, misconfigurations

Below: two representative findings from the full report.

Finding #1 — Exposed Cloud Storage Credentials

CRITICAL

Impact: NodeZero successfully used exposed credentials found in a public code repository to gain read access to a production cloud storage bucket containing customer records.

Recommendation: Rotate exposed credentials immediately, enable secret-scanning on all repositories, and move to short-lived, role-based credentials for cloud storage access.

Finding #2 — Missing MFA on Administrative Accounts

HIGH

Impact: 2 of 6 accounts with administrative privileges on the primary identity provider do not have multi-factor authentication enabled, creating a single-factor path to full environment compromise.

Recommendation: Enforce MFA org-wide for all privileged accounts within 5 business days; disable password-only authentication for admin roles.

SECTION 04

Vendor & Third-Party Risk Review

Every vendor with access to your systems or customer data is a potential entry point. We tier every vendor by risk, review what's on file, and hand you a program you can maintain going forward — not a one-time spreadsheet that goes stale.

Vendor (Fictional)	Data / Access Type	Risk Tier	Review Status
CloudHost Inc.	Production infrastructure	CRITICAL	Reviewed — SOC 2 Type II on file
PayFlow	Payment processing	CRITICAL	Reviewed — PCI DSS attestation on file
SupportDesk	Customer support tool, PII access	HIGH	Reviewed — gap identified (see below)
MetricsCo	Product analytics, no PII	LOW	Reviewed — public SOC 2 summary accepted

Vendor Finding — SupportDesk Encryption Gap

HIGH

Impact: SupportDesk (fictional vendor) could not provide evidence of encryption at rest for stored customer support tickets, which may include personally identifiable information.

Recommendation: Request updated data handling documentation before contract renewal; add an encryption-at-rest requirement to the vendor's contractual terms.

Full engagement includes: a complete vendor inventory, risk tiering for every vendor with system or data access, documentation review (SOC 2, PCI DSS, security questionnaires), and a maintainable process for reviewing new vendors going forward.

SECTION 05

Security Questionnaire Response Support

Enterprise security questionnaires can take days per deal without a prepared response library. We build yours once, backed by the program and assessment above, then reuse and tailor it for every future deal — including your next three enterprise contracts.

Sample Questionnaire Question	Prepared Response
Do you encrypt data at rest and in transit?	Yes. All customer data is encrypted at rest using AES-256 and in transit using TLS 1.2 or higher.
Do you have a documented incident response plan?	Yes. Our Incident Response Policy defines severity tiers, escalation paths, and notification timelines, reviewed annually.
Do you conduct regular technical security assessments?	Yes. Technical environment assessments are performed using Horizon3.ai NodeZero, an autonomous penetration testing platform, on a recurring basis.
Do you maintain a vendor risk management program?	Yes. All vendors with system or data access are tiered by risk and reviewed against current documentation on a recurring basis.

Result for Acme SaaS (illustrative): response library used across 3 enterprise questionnaires this quarter — reducing average turnaround from roughly 3 weeks to 4 business days per deal.

SECTION 06

Board-Ready Security Roadmap

A single page you can hand directly to your board or investors — prioritized, time-bound, and free of technical jargon.

NOW (0–30 Days)

- Rotate exposed cloud credentials
- Enforce MFA on all admin accounts
- Publish Access Control & Incident Response policies

NEXT (30–60 Days)

- Complete vendor risk reviews for top 10 vendors
- Roll out security awareness training
- Finalize data classification policy

LATER (60–90 Days)

- Complete remaining 8 core policies
- Conduct tabletop incident response exercise
- Prepare for SOC 2 Type II readiness review

This roadmap is designed to be presented as-is in a board meeting — each phase answers "what are we doing, and why does it matter," without requiring the board to understand the underlying technical detail.

SECTION 07

Ongoing Support & Next Steps

This is a shortened excerpt. The full GRC Launch Package includes complete versions of every section shown here, scoped entirely around your real environment, your real risks, and your real board's priorities.

You're Not Alone in the Room

Beyond the documents above, we show up. Board meetings, vendor security reviews, cyber insurance renewals — when the technical questions start, we're there as your subject matter expert. Many clients extend this into an ongoing Fractional CISO retainer once the initial roadmap is delivered.

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 the GRC Launch Package for your company.