MY FRACTIONAL CISO™

A service of Mission Cyber Group · myfractionalciso.com

Compliance Accelerate Package
Sample Deliverable Excerpt

A representative excerpt from the SOC 2 Readiness Assessment, Gap Analysis, and Automated Evidence Playbook included in every Compliance Accelerate Package engagement.

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

Prepared by: Mission Cyber Group / My Fractional CISO

Assessment scope: SOC 2 Type II Readiness Assessment (Security category)

Framework: AICPA Trust Services Criteria (TSC)

HOW TO READ THIS SAMPLE

What's Inside

This excerpt shows a representative slice of a full Compliance Accelerate Package deliverable. In an actual engagement, this document is significantly more comprehensive and tailored specifically to your environment, your target framework, and your audit timeline.

1. **Executive Summary & Readiness Score**
   A plain-language overview of where you stand today against your target framework, with a readiness score your leadership team can track over time.

2. **Full Trust Services Criteria Mapping**
   Every applicable control across all nine TSC categories — Control Environment, Communication, Risk Assessment, Monitoring, Control Activities, Logical & Physical Access, System Operations, Change Management, and Risk Mitigation — mapped to your actual environment.

3. **Gap Analysis & Remediation Roadmap**
   A prioritized list of exactly what's missing, what it takes to fix it, and in what order — so your team knows where to focus first.

4. **Automated Evidence Playbook**
   Step-by-step guidance for collecting and organizing the evidence your auditor will request, so nothing gets scrambled together at the last minute.

5. **Auditor-Ready Documentation Package**
   Policies, procedures, and supporting documentation formatted the way auditors expect to see them — not just the way they were written internally.

SAMPLE EXCERPT · ITEM 1 OF 5

Executive Summary & Readiness Score

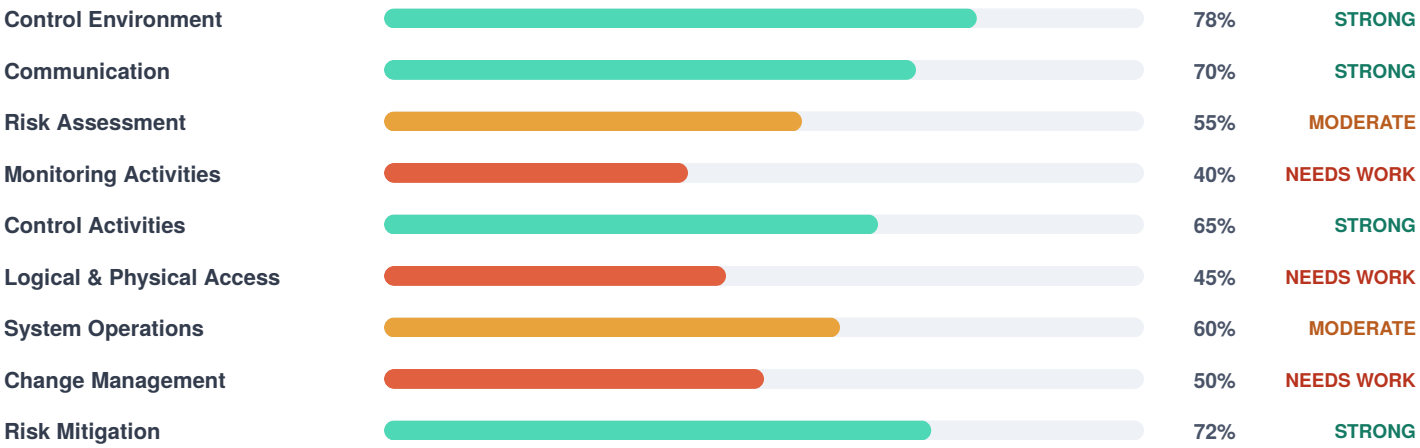
A plain-language overview of where Acme SaaS stands today against the SOC 2 Trust Services Criteria, with a readiness score leadership can track from kickoff through audit.

64/100

Moderate Readiness

Acme SaaS has strong foundational governance in place, but meaningful gaps remain in Logical & Physical Access and Change Management — both addressable within the 12-week engagement window.

Readiness by TSC Category



Key Findings

- Governance and leadership commitment are well established — the foundation an auditor looks for first is already in place.
- Access review cadence is the single largest gap, spanning both Logical & Physical Access and Monitoring Activities.
- Change management is functionally sound but inconsistently documented, which is a common and fast-to-close gap.
- No findings identified that would block a Type II audit window from being scheduled within the next quarter.

SAMPLE EXCERPT · ITEM 2 OF 5

Trust Services Criteria Mapping

Below is a representative excerpt from the full TSC mapping, showing two of the nine control categories assessed during a Compliance Accelerate engagement. Each control is assessed against your actual environment, with gaps identified and a clear recommendation for closing them.

CC1.1 · CONTROL ENVIRONMENT

The entity demonstrates a commitment to integrity and ethical values.

Trust Services Criteria, AICPA

CURRENT STATE

Acme SaaS has an informal code of conduct communicated during onboarding, but it has not been formally reviewed or re-approved by leadership within the past 12 months.

GAP IDENTIFIED

No documented annual review and approval process for the code of conduct.

RECOMMENDATION

Establish an annual review cycle with formal sign-off from company leadership, and require all employees to acknowledge the policy annually as part of onboarding and yearly refresh.

PRIORITY MEDIUM

SAMPLE EXCERPT · ITEM 2 OF 5 (CONTINUED)

Trust Services Criteria Mapping

CC6.1 · LOGICAL & PHYSICAL ACCESS

The entity implements logical access security measures to protect information assets.

Trust Services Criteria, AICPA

CURRENT STATE

Acme SaaS requires multi-factor authentication (MFA) for all production access, but does not currently perform a periodic review of who retains that access.

GAP IDENTIFIED

No documented quarterly access review process to confirm least-privilege access remains appropriate as roles change.

RECOMMENDATION

Implement a quarterly access review owned by engineering leadership, with documented sign-off and a ticketing trail for any access that's removed or modified.

PRIORITY HIGH

A full engagement covers all applicable controls across all nine TSC categories, not the two shown here.

SAMPLE EXCERPT · ITEM 3 OF 5

Gap Analysis & Remediation Roadmap

Every gap identified during the TSC mapping is consolidated here into a single, prioritized roadmap — so your team always knows what to work on next, and why.

GAP	TSC CATEGORY	PRIORITY	EST. EFFORT	TARGET WEEK
No documented quarterly access review process	Logical & Physical Access	HIGH	Medium	Week 3–4
Change approvals not consistently logged	Change Management	HIGH	Low	Week 3
No configured alerting on production monitoring tools	Monitoring Activities	HIGH	Medium	Week 4
No annual vendor risk reassessment process	Risk Assessment	MEDIUM	Medium	Week 5–6
No documented incident response tabletop testing	Risk Mitigation	MEDIUM	Low	Week 5
Code of conduct not formally reviewed annually	Control Environment	MEDIUM	Low	Week 2
No documented patch-management SLA for production systems	System Operations	LOW	Low	Week 6

A full engagement covers every gap identified across all nine categories, sequenced against your actual audit timeline — not a generic template.

SAMPLE EXCERPT · ITEM 4 OF 5

Automated Evidence Playbook

For every control in scope, the playbook tells your team exactly what evidence an auditor will ask for, where to pull it from, and how often it needs to be refreshed — so nothing gets assembled at the last minute.

Evidence Checklist — CC6.1 · Logical & Physical Access

- [ ] Export of quarterly access review approvals, covering the last four quarters
- [ ] Screenshot of MFA enforcement policy configured in the identity provider
- [ ] Current list of all privileged accounts, with date of last access review
- [ ] Termination tickets for all departed employees in the last 12 months, showing access removal timestamp
- [ ] Data center or cloud provider physical/logical access attestation (SOC 2 or ISO 27001 report)

Evidence Checklist — CC8.1 · Change Management

- [ ] Sample of change tickets showing requestor, approver, and deployment timestamp
- [ ] Screenshot of branch protection / required-approval settings in your source control system
- [ ] Rollback or incident record for any emergency change made in the last 12 months

In your full engagement, this playbook is built out for every control in scope — not just the two shown here — and is refreshed as your environment changes.

SAMPLE EXCERPT · ITEM 5 OF 5

Auditor-Ready Documentation Package

A snapshot of the policy and procedure documentation reviewed and finalized as part of the engagement — formatted the way an auditor expects to see it, not just the way it was originally written internally.

DOCUMENT	STATUS	NOTES
Information Security Policy	READY	Reviewed and formally approved by leadership
Access Control Policy	NEEDS UPDATE	Missing a defined quarterly review cadence
Incident Response Plan	READY	Validated via tabletop exercise this quarter
Change Management Policy	DRAFT	Approval workflow not yet formally documented
Vendor Risk Management Policy	NEEDS UPDATE	No annual reassessment process defined
Business Continuity / Disaster Recovery Plan	READY	Last tested six months ago; within policy window
Data Classification & Handling Policy	DRAFT	Classification tiers defined; handling rules in progress

A full engagement includes every policy and procedure document required for your target framework, delivered in the format your chosen audit firm expects.

READY FOR THE REAL THING?

Let's Get You Audit-Ready.

The full Compliance Accelerate Package includes everything shown here — built specifically for your environment, your target framework, and your timeline.

Questions about your SOC 2 or ISO 27001 readiness?

Email info@missioncybergroup.com or book your free scoping call directly.

Schedule Your Compliance Accelerate Scoping Call →