MY FRACTIONAL CISO℠

A service of Mission Cyber Group · **myfractionalciso.com**

SEED-STAGE SECURITY PLAYBOOK

The 15-Point NIST CSF 2.0 Compliance Checklist for Seed-Stage SaaS Startups

The exact security foundation you need to pass your first enterprise procurement review — without hiring a security team or slowing down engineering.

15	6	0
FOUNDATIONAL CONTROLS	CSF 2.0 FUNCTIONS	SECURITY HIRES REQUIRED

Mapped to NIST CSWP 29 — CSF 2.0

For Founders & Technical Leaders

WHY THIS EXISTS

You don't need all of NIST. You need the 15% that closes deals.

The full NIST CSF 2.0 Core contains over 100 Subcategories across six Functions. That's built for banks, hospitals, and federal contractors — not a 12-person SaaS company trying to close its first six-figure enterprise contract before the runway runs out.

Here's the truth every enterprise security reviewer already knows: they don't expect you to be SOC 2 certified at Seed. They expect you to demonstrate **foundational control** — that someone is accountable, that access is locked down, that data is encrypted, and that you'd notice if something went wrong. This checklist is that bar.

> **How to use this:** Work top to bottom. Govern and Identify come first because you can't protect what you haven't named and can't prioritize what you haven't assessed. Most of these items can be implemented in a single engineering sprint using tools you probably already pay for (Google Workspace, AWS/GCP IAM, GitHub, your IdP).

73%
of enterprise security questionnaires reject vendors on MFA, access control, and encryption gaps alone

1 sprint
is typically enough to close 10+ of these 15 items if you start today

$0
additional headcount required — every item below is CTO-executable

GOVERN

Someone owns this. It's written down. Vendors are vetted.

1 Name a Security Owner — Even If It's Just the CTO

`GV.RR-02`

Startup Translation: Put one named human's name next to "security decisions" in your org chart and internal docs — it can absolutely be your CTO or founder wearing two hats. Enterprise buyers reject vendors with no clear owner because "everyone's responsible" means no one is accountable when something breaks.

2 Write a One-Page Security Policy (Not a 40-Page PDF)

`GV.PO-01`

Startup Translation: Document your actual practices — MFA required, laptops encrypted, access reviewed quarterly — in a single page, then have leadership sign off on it. This single artifact answers 20% of every security questionnaire you'll ever receive and proves you're operating with intent, not luck.

3 Vet Every Vendor Before You Wire Them Money or Data

`GV.SC-06`

Startup Translation: Before connecting a new SaaS tool or subprocessor to production data, spend 15 minutes checking they have SOC 2 or equivalent, then log the decision. Your own enterprise customers will ask for your subprocessor list — you need to already know what's in it.

IDENTIFY

You can't protect assets you haven't inventoried.

4 Build a Living Asset Inventory

`ID.AM-01 / ID.AM-02`

Startup Translation: Keep one spreadsheet or lightweight CMDB listing every repo, cloud account, SaaS tool, and production system your company runs, and update it whenever something new gets spun up. Auditors' first question is always "what do you have?" — and "we're not totally sure" is an instant red flag.

5 Tag and Classify Your Crown-Jewel Data

`ID.AM-05`

Startup Translation: Identify where customer PII, payment data, and proprietary source code actually live, and label those systems as "Critical" so they get extra scrutiny. Enterprise buyers need to know you can answer "where does our data go" in seconds, not weeks.

6 Run Quarterly Vulnerability Scans

`ID.RA-01`

Startup Translation: Turn on an automated scanner (AWS Inspector, GitHub Dependabot, or a free-tier tool like a basic Nessus/Qualys scan) against your infrastructure and dependencies every quarter, and keep the reports. This turns "we think we're secure" into "we can prove it," which is exactly what a due-diligence checklist is looking for.

PROTECT The controls that actually stop breaches — and the ones every questionnaire asks about first.

7 Enforce Phishing-Resistant MFA Everywhere

PR.AA-03

Startup Translation: Turn on hardware-key or authenticator-app MFA (not SMS) across your IdP, cloud consoles, GitHub, and email — no exceptions, including the founders. This is the single most-asked question on every enterprise security questionnaire, and answering "no" here ends the deal before it starts.

8 Kill Standing Admin Access — Enforce Least Privilege

PR.AA-05

Startup Translation: Audit who has "Owner" or "Admin" on your cloud, database, and SaaS accounts, and cut that list down to the people who genuinely need it day-to-day. Reviewers want to see that a single compromised engineer laptop can't take down your entire production environment.

9 Encrypt Data At Rest and In Transit — Everywhere

PR.DS-01 / PR.DS-02

Startup Translation: Confirm your database, backups, and file storage use encryption at rest (usually a checkbox in AWS/GCP/Azure) and that every endpoint enforces TLS 1.2+ in transit. This is table-stakes, near-zero-effort configuration that removes an entire category of questionnaire failures.

10 Automate Security Awareness Training

PR.AT-01

Startup Translation: Run every new hire (and existing team) through a short annual training on phishing, password hygiene, and data handling using a cheap tool like KnowBe4 or even a recorded Loom plus a quiz. Human error causes the majority of breaches, and "we train our people" is a checkbox nearly every SOC 2 auditor and enterprise questionnaire requires.

11 Bake Security Checks Into Your CI/CD Pipeline

PR.PS-06

Startup Translation: Add automated SAST/dependency scanning (GitHub Advanced Security, Snyk free tier, or similar) directly into your pull request pipeline so vulnerable code and secrets never reach main. This proves security is built into how you ship, not a once-a-year afterthought — exactly what sophisticated buyers dig into during technical due diligence.

12 Patch and Retire Software on a Fixed Schedule

PR.PS-02

Startup Translation: Set a recurring calendar reminder (monthly is fine at this stage) to apply OS, dependency, and third-party library patches, and formally decommission anything you no longer use. Unpatched, forgotten systems are the number one way small companies get breached — and the easiest thing for an auditor to catch.

DETECT

If you can't see it, you can't catch it before your customer does.

13 Centralize Your Logs Before You Need Them

PR.PS-04

Startup Translation: Ship logs from your app, cloud infrastructure, and auth provider into one place — even a low-cost tool like CloudWatch, Datadog free tier, or a self-hosted ELK stack counts — and retain them for at least 90 days. When (not if) a customer asks "can you tell us exactly who accessed what and when," this is the only way to answer with confidence.

14 Monitor Admin Activity Across Your Cloud and SaaS Stack

DE.CM-06

Startup Translation: Turn on alerts for privileged actions — new admin users, IAM policy changes, mass data exports — in AWS/GCP CloudTrail-equivalents and your core SaaS tools. This is the cheapest possible tripwire for both external attackers and insider risk, and it's a specific line item on most vendor security reviews.

RESPOND

The plan you write once so you're not improvising during a breach.

15 Draft — and Actually Test — an Incident Response Plan

RS.MA-01

Startup Translation: Write a one-to-two-page plan naming who does what during a breach (who investigates, who notifies customers, who talks to legal), and run a 30-minute tabletop exercise once a year to pressure-test it. Every serious enterprise contract will ask for this document by name, and having a tested plan is the difference between a controlled response and a PR disaster.

15 controls. 1 sprint. Zero new headcount.

This checklist won't make you SOC 2 certified overnight — but it will put you ahead of 90% of Seed-stage startups walking into an enterprise security review, and it lays the exact groundwork your future SOC 2 audit will build on.

GOVERN Own it, write it down, vet vendors.

IDENTIFY Inventory assets, classify data, scan for gaps.

PROTECT MFA, least privilege, encryption, training, secure CI/CD, patching.

DETECT Centralize logs, monitor privileged activity.

RESPOND Write and test an incident response plan.

NEXT STEP

Turn this checklist into a signed Organizational Profile you can hand directly to enterprise procurement teams — and start closing deals that were previously stuck in security review.

Stuck, or would rather not spend the cycles? That's what My Fractional CISO is for — get a free, no-obligation review of your cybersecurity and compliance architecture. A 15-minute call, no pitch deck required.

Email **info@missioncybergroup.com** to book yours.

My Fractional CISO℠ — a service of Mission Cyber Group
