IMPLEMENTATION PLAN

Fully managed SaaS

What gets stood up, in what order, and who does each part.

Pattern Multi-tenant SaaS, operated by Iron Fort **For** Founders, startups and small businesses

IRON FORT YOU TOGETHER

Nothing is deployed and nothing is operated by you, so this plan is mostly about granting access carefully and deciding scope. Most of the work is in phases 2 and 3.

> **BEFORE YOU START**
>
> - A Microsoft or Google account for each person who needs access.
> - Administrative access to the cloud accounts and workspaces you want read.
> - Whoever can approve a CloudFormation stack in your AWS account.

1

Tenant and access IRON FORT

- We provision your tenant in ca-central-1 and confirm the region on the record.
- You name the first administrators; sign-in is Microsoft or Google, with two-factor enforced.
- Set roles now rather than later — administrator, contributor, read-only auditor.

DONE WHEN

Your administrators can sign in and see an empty but correctly scoped tenant.

2

Connect your systems TOGETHER

- AWS: deploy our published CloudFormation stack, which creates a read-only cross-account role with an external ID. Review it before you run it — it is short and it is meant to be read.
- Azure and Microsoft 365: create an app registration with read scopes.
- Google Cloud and Google Workspace: a service account with viewer roles.
- GitHub, Vercel, Cloudflare, Okta and the rest: OAuth, read scopes only.

DONE WHEN

Every in-scope system returns data on a test collection.

3

Scope the programme TOGETHER

- Record the organisation, its systems, departments and applications. This is what controls attach to.
- Install the framework you need and choose a control profile.
- Mark which systems hold regulated data — it drives most of the classification work later.

DONE WHEN

The control set is installed and every control has a scope.

4

First collection IRON FORT

- Scans run on schedule; the first full pass establishes a baseline.
- We walk the initial findings with you and separate real gaps from scoping errors.
- Assign owners to findings so the queue belongs to people, not to the platform.

DONE WHEN

A coverage figure exists and the team agrees it is honest.

5

Policies and evidence YOU

- Bulk-upload the policies you already have; each is parsed, matched to the framework and shown to you before anything is saved.
- Fill the gaps from the policy library rather than from scratch.
- Set review cycles so the clock starts running now.

DONE WHEN

Every required policy exists, has an owner and has a next review date.

6

Reporting and trust TOGETHER

- Schedule the recurring reviews: access recertification, risk assessment, DR test, penetration test.
- Generate the reports your assessor expects and read them before they do.
- Publish the trust page and take the embed badge for your own footer.

DONE WHEN

You can hand an assessor a link and a report pack on the same day they ask.

Sequence, not schedule. The phases are ordered by dependency. Elapsed time depends on your change process, your approvals and how much of the estate is in scope, so this plan does not guess at it. Ask us and we will estimate it against your specifics.

Iron Fort Solutions · goironfort.com/reference-architecture