IMPLEMENTATION PLAN

Dedicated Iron Fort infrastructure

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

Pattern Dedicated infrastructure, open only to your IP ranges **For** Small and mid-sized enterprises

IRON FORT YOU TOGETHER

Everything in Pattern 1, plus a dedicated environment we build for you and a firewall that only your addresses get through. The extra work is a networking conversation, and it is worth having early because it gates access for everyone.

BEFORE YOU START

- Your office and VPN egress IP ranges, confirmed by whoever owns the firewall.
- A decision on region, if residency matters to you.
- A Microsoft or Google account for each person who needs access.

1

Design and region TOGETHER

- Confirm the AWS region, including Canadian residency if that is a requirement you have to evidence.
- Agree the encryption posture: a KMS key scoped to you alone, and who may administer it.
- Collect your egress ranges. Get these from the network team, not from a spreadsheet — stale ranges are the most common cause of a day-one lockout.

DONE WHEN

Region, key policy and allowlist are agreed in writing.

2

Build your environment IRON FORT

- We provision a dedicated VPC, a dedicated database and evidence bucket, and your KMS key.
- Data subnets are created with no route to the internet.
- The application is deployed behind a WAF configured to admit only your ranges.

DONE WHEN

A request from an allowlisted address succeeds; one from anywhere else is refused at the edge.

3

Access and sign-in TOGETHER

- Administrators sign in with Microsoft or Google, two-factor enforced. There is no local password path.
- Test from every location your team actually works from, including home VPN egress.
- Agree the change process for adding an address range later, so it does not become a ticket nobody owns.

DONE WHEN

Every person who needs access has it, from every network they use.

4

Connect your systems TOGETHER

- The single managed scanner worker inside your VPC is the only component that reaches your systems.
- Grant read-only credentials as in Pattern 1 — CloudFormation stack, app registration, service account, OAuth.
- Confirm the worker's egress is outbound only; nothing inbound to your network is required.

DONE WHEN

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

5

Scope, collect, populate TOGETHER

- Record the organisation and its systems; install the framework and choose a profile.
- Run the first collection and separate real gaps from scoping errors.
- Bulk-upload existing policies and set review cycles.

DONE WHEN

A coverage figure exists and every required policy has an owner and a review date.

6

Reporting and trust TOGETHER

- Schedule the recurring reviews and tag them to the frameworks they satisfy.
- Generate the assessor reports and read them before the assessor does.
- Publish the trust page — it is public by design, and separate from the allowlisted application.

DONE WHEN

The programme runs without anyone touching infrastructure.

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