Security Assessment Framework

A practical GRC walkthrough

djerhy.tech

By Djerhy Jn Baptiste (CISSP, Cloud Security, GRC)

Table of Contents

2. Don’t Start Before You Start

Before you run your first scan or request a SOC 2 report, pause. You’re not just here to find flaws. You’re here to understand the terrain.

- Secure Access: Get credentials, NDA, laptop provisioning sorted first.
- Scope Alignment: What’s in scope this week? Don’t assume. Confirm it.
- Map Influence: Who owns what? Who blocks what? Note it now, not later.
- Executive Buy-In: Ask how urgent this is to leadership. The answer shapes your tone.
- Soft Signals: Casual comments often reveal more than policy documents. Listen closely. Great GRC work doesn’t start with a checklist. It starts with context.

3. How to Approach Week One

- You’re stepping into a fictional mid-sized fintech called Richtomet Financial Services. They handle sensitive customer data with a mix of on-prem and cloud systems. Your goal: build momentum, not perfection.
- Read the Room: Start with conversations. Human insights beat tools early on.

- Don’t Boil the Ocean: Focus where the risk is loudest, data flows, access points.
- Pro Tip: As a CISSP holder, lean on Domain 1 principles: Prioritize visibility over everything.
- Balance Tech and People: Tools like Checkov are great, but stakeholder buy-in makes them stick. This entry-level walkthrough keeps things simple: context first, action second.

4. Quick System and Compliance Landscape

For Richtomet, here’s a snapshot of what you’re assessing:

Category	Details
Infrastructure	AWS EC2/S3, Okta, Snowflake, Checkov for IaC misconfigurations
Compliance	SOC 2, PCI-DSS (Verify early)

This landscape guides targeted assessments.

5. Red Flags

Red Flags to Watch For

In this fictional setup, flag these early:

Issue	Risk Level	Action
Unmapped Assets	High	Map immediately. Leads to breaches
Weak Credential Policies	Medium	Enforce MFA
Outdated Compliance Docs	Low	Schedule review

These risks inform actionable deliverables.

6. Deliverables

- Risk Prioritization Matrix (highlight high-impact areas)
- AssetHunt Template (download at asset-walkthrough.pdf)

- Compliance Checklist (align with SOC 2/PCI-DSS)

These tools drive momentum, not perfection.

7. Analyst Perspective

week one is about momentum. You’re not fixing everything; you’re setting the stage. For Richtomet, focus on visibility, it's 80% of the battle. Listen more than you scan, and remember: GRC is people-first.

This fictional angle keeps it practical for starters.

8. Next Steps

- Stay tuned for deeper dives into GRC best practices
- Download resources:
  - AssetHunt Template
  - Security Framework