

Week One Security Assessment Framework

A Fictional Scenario for Practical GRC Walkthroughs

Djerhy Jn Baptiste – CISSP | Cloud Security | GRC

Page 1 of 8

djerhy.tech



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.



How to Approach This Assessment

There's no perfect formula, but a good approach combines instinct, alignment, and a strong signal-to-noise filter. Here are key principles:

- **Data Flow ≠ Information Flow:** Don't just trace the packets—trace the human routes. Look for printouts, shoulder surfing, meeting leaks, and insecure disposal habits.
- **Speed > Polish:** It's better to map imperfect reality fast than chase ideal documentation too slowly.
- **Risks First:** Don't boil the ocean. Surface what's loudest, most impactful, or neglected.
- **Read the Room:** Tone matters. A confrontational style shuts down collaboration.
- **Human Before Tech:** The fastest wins often involve people, not tools. Observe behavior before you prescribe tools.

Infrastructure & Compliance Landscape

Systems Overview

- **Cloud:** AWS (EC2, S3, Lambda), Azure AD
- **SaaS Stack:** Salesforce, Slack, Jira, Confluence
- **Identity:** Okta (SSO), MFA enforced
- **Data Layer:** PostgreSQL, Redshift, Snowflake
- **Vendor APIs:** Plaid, Equifax, TransUnion, Yodlee
- **Endpoints:** CrowdStrike, Jamf, MDM for BYOD
- **DevSecOps:** GitHub, Terraform, Checkov






Compliance Requirements

- SOC 2 Type II
- PCI-DSS (partial scope)
- NYDFS Part 500
- GLBA applicability under review

GRC Red Flags – Week One Observations

Red Flag	Risk Level	Concern
Outdated access logs	⚠ High	No centralized access review
Okta groups loosely managed	⚠ High	Excessive admin access
Devs bypass VPN for testing	⚠ Medium	Unmonitored access paths
ML engine lacks audit trail	⚠ Medium	Explainability + compliance gaps
No vendor onboarding workflow	⚠ High	Unvetted third-party tools
No system-wide DLP policy	⚠ Medium	Risk of data leakage
Missing endpoint agents	⚠ High	15% of contractor/remote machines
Security training not enforced	⚠ Low	Poor security hygiene

Week One Deliverables Toolkit

-  Intake Checklist (systems, stakeholders)
-  Kickoff Agenda (first GRC team meeting)
-  Access Review Template (who has what)
-  Vendor Mapping Sheet (API and vendor risk)
-  Interview Scripts (Sales, Ops, Engineers)

Pro Tip: Focus on visibility first. Even simple templates drive massive clarity during GRC ramp-up.







Analyst Perspective

"In organizations like Richtomet Financial Services, GRC starts late—but gets urgent fast. Your job isn't to audit everything. It's to prioritize. Start where the risk is loudest. Don't chase perfection—chase momentum."

Use your judgment. Flag what's urgent. Frame what's missing. This is where real GRC work begins.

Want More Like This?

If this guide sparked ideas, you're not alone. I'm building a full Richtomet GRC Series:

-  30-Day Assessment Plan
-  Editable Templates + Checklists
-  GRC Interview Training Scenarios
-  Start-from-Scratch GRC Toolkit

 Join the list or send me feedback: djerhy.tech

 Or DM me on LinkedIn: [linkedin.com/in/djerhybaptiste](https://www.linkedin.com/in/djerhybaptiste)