Week One Security Assessment Framework

A Fictional Scenario for Practical GRC Walkthroughs

Djerhy Jn Baptiste – CISSP | Cloud Security | GRC

🏙️ FinSage Capital – Company Snapshot

- Industry: Financial Technology (FinTech)
- Size: 200 employees
- Business Model: B2B digital lending and credit services for SMBs
- FinSage Capital is a cloud-native FinTech platform offering credit lines and financial analytics tools to small and mid-sized businesses. Their platform integrates with Equifax, Plaid, and regional banking APIs to automate onboarding, underwriting, and servicing.

Department	Headcount	Key Roles
Product & Engineering	60	Devs, DevOps, QA
Customer Ops	50	Loan Officers, CS Reps
Sales & Partnerships	30	AEs, Partner. Managers
GRC & Security	10	Analysts, Compliance Officer
Back Office	20	HR, Legal, Finance
Leadership	5	CEO, CISO, CTO, COO, CCo

☁️ Infrastructure & Compliance Landscape

systems	Compliance
1)Cloud Infrastructure: • AWS (EC2, S3, Lambda) • Azure AD 2) SaaS Stack: • Salesforce • Slack • Jira 3) Identity & Access: • Okta (SSO) • MFA enforced (mostly) 4) Data Layer: • PostgreSQL (hosted) • Redshift • Snowflake 5) Endpoints: • CrowdStrike • Jamf • MDM for BYOD	Compliance Overlap: • SOC 2 Type II • PCI-DSS (partial scope) • NYDFS Part 500 • GLBA (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Outdated access logs	⚠️ High	No centralized access review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	Many have admin-level acces
Devs bypass VPN for test envs	⚠️ Medium	Risk of unmonitored activity
ML loan engine lacks audit trail	⚠️ Medium	Explainability & compliance
Vendors onboarded without due diligence	⚠️ High	Third-party risk exposure
No system-wide DLP policy	⚠️ Medium	Data leakage risks
Endpoint agents missing (15% devices)	⚠️ High	Remote + contractor exposure
Security training not enforced	⚠️ Low	Low awareness & hygiene

📋 Week One Deliverables Toolkit

Intake Checklist

Who to meet,
what access to request, which systems are critical

Kickoff Agenda

First meeting with the CISO, Ops, and stakeholders to establish scope

Access Review

Template Quick audit of privileged access and RBAC gaps

Vendor Mapping Sheet

Track all third-party data processors, APIs, and risk owners

Interview Scripts

Suggested questions for Sales, Engineering, and Customer Ops teams

Analyst Perspective

“In organizations like FinSage Capital, 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.*

💬 DM me on LinkedIn: linkedin.com/in/djerhybaptiste

🔗 Visit: djerhy.tech