Vendor Risk Portfolio Summary

Overview

This portfolio demonstrates practical, job-ready Third-Party Risk Management (TPRM) skills through real assessments, structured documentation, and governance artifacts. Each deliverable reflects the workflows, analysis methods, and security expectations used by modern SaaS security organizations.

What This Portfolio Demonstrates

This collection shows the ability to evaluate vendors, interpret SOC 2 reports, build scoring models, write security policies, and document findings clearly and professionally. It represents the full lifecycle of vendor risk work: intake, assessment, analysis, risk scoring, remediation, approval, and monitoring.

Core Competencies

• SOC 2 analysis and evidence interpretation

• Vendor intake and tiering methodology

• Risk scoring using likelihood and impact

• Governance and policy writing

• Data handling and access control expectations

• Security questionnaires and due diligence

• Workflow documentation and clear communication

Key Deliverables

• SOC 2 Analysis

• Vendor Risk Assessment

• TPRM Methodology

• TPRM Workflow

• Vendor Policy Suite

Each deliverable is written using professional security documentation standards.

Evidence of Operational Skill

These documents mirror the work performed by Vendor Risk Analysts, GRC Analysts, Security Analysts, and other assurance roles. They show the ability to break down complex evidence, identify gaps, assign risk ratings, and create actionable recommendations.

How to Use This Portfolio

Review each document in the order listed to understand the complete picture of the vendor risk lifecycle. Recruiters and hiring managers can use this portfolio to evaluate analytical depth, documentation quality, and understanding of security frameworks.