NIST Risk Register - Cloud Compliance Use Case

Project Overview

This project simulates a GRC analysis for a fictional health-tech startup called BrightBridge Health. It focuses on assessing risks related to cloud infrastructure, user access, and third-party integrations. Controls are mapped to the NIST Cybersecurity Framework (CSF), and risks are prioritized by impact and likelihood.

What's Included

- Structured risk register with common cloud assets and threats
- Likelihood and impact-based scoring
- Justified control suggestions mapped to NIST CSF
- Summary tab highlighting prioritization logic and control strategy

Why This Matters

This demonstrates practical GRC skills in risk documentation, control mapping, and audit preparation. It reflects the kind of deliverables expected in cybersecurity compliance and governance roles.

Referenced Frameworks and Resources

- NIST Cybersecurity Framework
- AWS Well-Architected Framework (Security Pillar)
- OWASP Top 10
- EDR (Endpoint Detection and Response) Tools