## ■ Project Title:

# Data Risk Assessment and Least Privilege Implementation Review

### Summary for GitHub Portfolio

This project involved analyzing a real-world data privacy incident through the lens of the principle of least privilege. As a cybersecurity analyst for an educational technology company, I evaluated the causes of a data leak, reviewed the organization's data handling controls, and proposed security control enhancements aligned with NIST SP 800-53 (AC-6). The activity demonstrated the importance of implementing granular access control and enforcing data handling policies to prevent unauthorized information exposure.

#### Scenario Overview

The organization developed a teacher-assistance application that manages sensitive student and instructor data. During a sales call, an employee accidentally shared a link to a confidential folder containing internal business documents. The incident resulted from a failure to revoke sharing permissions and a lack of oversight in applying least privilege principles.

### Issues Identified

The data leak occurred because of excessive access permissions and failure to enforce access control hygiene. The folder containing internal business plans was shared without restrictions, violating the least privilege principle. The employee also lacked training on secure data sharing practices, leading to unintended public exposure of sensitive information.

Review of NIST SP 800-53: AC-6

The AC-6 control in NIST SP 800-53 mandates that access to information systems and resources be limited to authorized users based on their role and necessity. It emphasizes applying the principle of least privilege by restricting access rights to only those required for job functions. The control also encourages periodic audits and monitoring of access rights to ensure compliance and prevent privilege creep.

**Recommended Control Enhancements**

- Implement automated access control tools that enforce least privilege by role and periodically review permissions.
- Enforce mandatory access revocation when sharing periods expire, ensuring that sensitive data is not exposed beyond intended recipients.

**Justification of Recommendations**

These recommendations strengthen least privilege enforcement by ensuring that employees only retain access to the data they need for active tasks. Automating access reviews and implementing time-based permissions reduce the likelihood of human error, while enforcing revocation policies minimizes exposure risks. These controls directly address the root causes of the data leak and improve organizational resilience against insider threats and accidental disclosure.

**Key Takeaways**

This project reinforced the critical role of access control in information privacy management. I learned to map real incidents to NIST framework controls and identify control gaps that lead to data exposure. The analysis strengthened my understanding of least privilege, data risk mitigation, and compliance frameworks central to modern cybersecurity operations.