Overview

This project brings together everything you've learned in the *Resilience and Recovery* modules — from Business Impact Analysis (BIA) and Risk Assessment to Integration and Application. You'll review real-world resilience and recovery case studies, analyze what went right or wrong, and connect your findings to the frameworks we've studied (risk, BIA, resilience planning, and recovery strategy).

The project should take about **2 hours** to complete and will be done individually or in pairs.

Your Mission

You're a resilience analyst reviewing incidents that tested an organization's ability to recover from disruption. You'll choose one real or fictional case study, analyze its resilience and recovery performance, and present what lessons can be learned.

You can choose examples from:

- Real corporate disasters (e.g., AWS outage, Maersk ransomware, British Airways IT failure).
- Natural disasters (e.g., floods, earthquakes, wildfires).
- Public service disruptions (e.g., hospitals or cities losing systems).
- Fictional but realistic scenarios (e.g., a SaaS platform hit by ransomware).

Your Objectives

By the end of this project, you will:

- Identify key risk and impact factors in a real or simulated event.
- Explain how resilience and recovery principles applied (or failed).
- Connect lessons to BIA, risk management, and recovery planning concepts.
- Recommend improvements that would strengthen organizational resilience.

Project Steps

Step 1: Choose a Case Study
Pick one case that clearly shows a disruption and a recovery process. Use reputable sources (articles, reports, or company statements).

Step 2: Summarize the Event
Write a short overview (about one paragraph) covering:

- What happened
- When and how it occurred
- What business functions or systems were affected

Step 3: Analyze Risks and Impacts
Identify:

- The top 3 risks that materialized
- Which BIA categories were affected (financial, operational, legal/regulatory, reputational)
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) considerations

Step 4: Evaluate the Recovery
Answer:

- How well did the organization respond?
- What went well?
- What failed or was missing in their plan?
- Did the recovery align with resilience best practices?

Step 5: Integrate Lessons with Frameworks
Use concepts from class to connect the case to resilience planning:

- Risk Assessment findings
- BIA integration
- Incident response and testing practices

- Long-term resilience governance

Step 6: Recommend Improvements
List 3–5 practical steps the organization could take to improve.
Example:

- Update disaster recovery testing frequency
- Improve cross-department communication
- Redefine critical system RTOs

Deliverable

Submit a **Google Doc** (1–2 pages) or prepare a short presentation with:

- Case study summary
- Risk and impact analysis
- Recovery performance evaluation
- Recommendations
- References or sources used

Tips for Success

- Use bullet points and short paragraphs — clarity matters more than length.
- Avoid copying online summaries — analyze and explain in your own words.
- Choose a case that genuinely interests you; passion improves insight.
- Apply frameworks from our lessons — show understanding, not memorization.

After Submission

During the next class, we'll do a short group discussion where volunteers can share:

- Which case they chose
- Key lessons learned
- What surprised them most about the organization’s recovery