Overview

In this lab, you'll apply what you learned in *Resilience Integration and Application* by running a **Rapid Risk Assessment (RRA)** on a fictional IT system. You'll work as part of a consulting team helping a company identify, evaluate, and connect risks to their BIA findings.

The goal is to help you think like a resilience professional — balancing risk awareness with real-world business impact.

Your Mission

You are part of a consulting group hired by **CloudNova**, a mid-sized SaaS company that runs a customer analytics platform for retail businesses.

The system stores and processes customer data for more than 800 clients. It operates 24/7, and any downtime longer than four hours triggers financial penalties under client SLAs.

CloudNova leadership has asked for a **rapid risk assessment** to go with their ongoing Business Impact Analysis (BIA). Your job is to complete the assessment and present your key findings to the class.

Your Objectives

By the end of this lab, you will:

- Identify key risks that could disrupt CloudNova's IT system.
- Rate those risks by likelihood and business impact.
- Link your risks to specific BIA findings (RTOs, RPOs, dependencies).
- Recommend quick and practical mitigation strategies.

How to Work Together

Form groups of **4–5 students** and split your roles:

1. **Risk Team:** Focus on identifying and scoring risks (likelihood and impact).

2. **Resilience Team:** Connect those risks to the BIA findings — which functions, systems, and dependencies they affect.

You'll collaborate as one team to produce a short, clear summary that you'll share with the class.

Steps to Complete the Lab

Step 1: Identify Core Assets
List 3–5 critical assets or systems (e.g., main database, cloud platform, reporting dashboard). Write down what each asset supports and how it contributes to business operations.

Step 2: Identify Potential Threats
Brainstorm 5–7 realistic threats that could impact those assets. Examples include:

- Cyberattack (ransomware, DDoS)
- Data corruption or loss
- Vendor service failure
- Cloud outage
- Insider misuse
- Natural disaster

Step 3: Score the Risks
Rate each threat based on:

- **Likelihood:** Low, Medium, or High
- **Impact:** Financial, Operational, Legal/Regulatory, Reputational
  Then assign an overall **risk level** (for example: High = both likelihood and impact are High).

Step 4: Connect to the BIA
For each top risk, identify:

- Which critical process or system is affected

- The related RTO or RPO
- Any key dependencies or enablers

Step 5: Recommend Mitigation and Recovery Actions
Suggest one **short-term** and one **long-term** action for each top risk.
Example: For ransomware → short-term: backup verification; long-term: implement immutable storage.

Step 6: Create and Present Your Summary
Use **Google Docs or Sheets** to organize your results in a table or matrix. Include:

- Risk name
- Threat type
- Likelihood and impact
- BIA link
- Recommended actions

You'll present a **3-minute summary** to the class covering:

- The top 3 risks you found
- Their potential business impact
- How they connect to resilience goals

What You'll Deliver

Submit or present a completed **Rapid Risk Assessment Summary** that includes:

- Risk descriptions and ratings
- BIA connections
- Mitigation and recovery strategies

Tips for Success

- Keep it realistic and simple — this is a *rapid* assessment.
- Use the internet to find examples of risk assessment templates or scoring models.
- Focus on how risk and BIA data complement each other.
- Show your reasoning — how each risk impacts the organization's ability to stay resilient.

Class Debrief

After everyone presents, we'll discuss:

- How each group defined and ranked "critical risk."
- Which risks appeared most often and why.
- How integrating risk and BIA results leads to stronger resilience strategies.