

GRC103 Lab: The SecureBrew Risk Assessment

Course: GRC103 - Risk Assessment and Management Techniques

Week: 15 - Practical Risk Assessment Workshop

Lab Title: The SecureBrew Cafe: A Digital Transformation Risk Assessment

Format: Team-based

1. Instructor's Guide & Overview

Objective:

This immersive, team-based lab requires students to act as a GRC consulting team hired to conduct a risk assessment for a local business, "SecureBrew Cafe." They will apply the full risk management lifecycle learned in this course to a realistic, relatable scenario, producing professional-grade deliverables.

Learning Outcomes:

Upon completion of this lab, students will be able to:

- Apply structured risk identification techniques to a novel business scenario.
- Analyze and evaluate identified risks using a qualitative risk matrix.
- Formulate practical risk treatment strategies aligned with business objectives.
- Document findings in a standardized risk register and communicate them effectively to management.

Lab Flow & Timing:

- **Introduction & Team Briefing (15 mins):** Scenario overview and team formation.
- **Part A: Risk Identification (45 mins):** Brainstorming risks.
- **Part B: Risk Analysis & Evaluation (45 mins):** Plotting risks on a matrix.
- **Part C: Risk Treatment Strategies (45 mins):** Developing mitigation plans.
- **Part D: Risk Reporting & Wrap-Up (30 mins):** Documenting and presenting findings.
- **Total: 3 hours**

2. Student Lab Packet

Lab Brief: Welcome, Consultants!

You are a newly formed Risk Management team at a reputable consulting firm. Your new client is **SecureBrew Cafe**, a beloved campus coffee shop.

The Client: SecureBrew's owner, Alex, is a coffee visionary but a tech novice. To compete with big chains, Alex recently launched a "Digital Upgrade":

1. **"BeanStack" Loyalty App:** Customers can load money, pre-order drinks, and earn points. It stores user emails and limited payment info.
2. **Cloud-Based POS System:** A new tablet-based system that processes all credit/debit card transactions.
3. **Free Public Wi-Fi:** An open network to attract students who study in the cafe.

The Problem: Alex has heard news stories about small business data breaches and system failures. They are

worried their new tech investments could become a liability. They've hired your team to answer one big question:

"What are the biggest risks to my business from these new digital systems, and what should I do about them?"

Your mission is to conduct a rapid risk assessment and provide Alex with clear, actionable answers.

Part A: Risk Identification (45 mins)

Technique: Structured Brainstorming & Prompting List

Your Task:

As a team, brainstorm and list as many potential risk events as you can. Think like a hacker, a clumsy employee, or just consider what could go wrong with technology. Use the categories below to spark ideas. **Aim for a list of 10-15 potential risks.**

- **Technical Failures:** (e.g., system crash, software bug, power outage, network failure)
- **Human Error & Malice:** (e.g., employee mistake, insider theft, lack of training, social engineering)
- **External Threats:** (e.g., hacker attack, malware infection, phishing scam, supplier bankruptcy)
- **Physical & Environmental:** (e.g., theft of a POS tablet, coffee spill on a router, fire)
- **Compliance & Legal:** (e.g., violating data privacy laws like GDPR/CCPA, payment card industry (PCI DSS) non-compliance)

Deliverable 1: Brainstormed Risk List

List your team's identified risks in the space below.

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

- 11.
- 12.

Part B: Risk Analysis & Evaluation (45 mins)

Technique: Qualitative Risk Matrix

Your Task:

From your long list in Part A, select the **SIX (6)** most significant risks. Analyze each one based on its **Likelihood** and **Impact**, then plot them on the risk matrix below.

Scoring Guide:

- **Likelihood:** How probable is it that this risk occurs in the next year?
 - **Low:** Unlikely, less than 10% chance.
 - **Medium:** Might happen, 10-50% chance.
 - **High:** Very likely, greater than 50% chance.
- **Impact:** If it happens, how bad will the consequences be for SecureBrew? (Consider: Financial Loss, Operational Shutdown, Reputation Damage, Customer Loss, Regulatory Fines).
 - **Low:** Minor inconvenience, small financial loss (<\$1,000).
 - **Medium:** Significant disruption, noticeable financial loss, some negative reviews.
 - **High:** Business-threatening; major financial loss (>\$10,000), lasting reputation harm, potential legal action.

Deliverable 2: Risk Matrix

Write the number of each risk from your list in the corresponding cell on the matrix.

Impact	Low Likelihood	Medium Likelihood	High Likelihood
High	MEDIUM RISK	HIGH RISK	HIGH RISK
Medium	LOW RISK	MEDIUM RISK	HIGH RISK
Low	LOW RISK	LOW RISK	MEDIUM RISK

Based on your matrix, which 2-3 risks are your highest priority?

(e.g., Risks #3, #7, and #11)

Part C: Risk Treatment Strategies (45 mins)

Technique: Selecting and Justifying Treatment Options

Your Task:

For your **TWO (2) HIGHEST PRIORITY** risks from Part B, develop a specific treatment plan. Choose from the four strategies below and justify your choice.

- **Mitigate:** Implement a control to reduce the likelihood or impact.
- **Accept:** Acknowledge the risk but take no action now (usually for low-priority risks).
- **Transfer:** Shift the risk to a third party (e.g., buying insurance).
- **Avoid:** Eliminate the risk by stopping the activity that causes it.

Deliverable 3: Treatment Plan

High Priority Risk #1:

- **Risk Description:**
- **Recommended Treatment Strategy:** (Mitigate/Accept/Transfer/Avoid)
- **Specific Action Plan:** (e.g., *To mitigate the risk of a hacked POS, we will enforce mandatory multi-factor authentication on all admin accounts and conduct quarterly security training for all staff.*)

High Priority Risk #2:

- **Risk Description:**
- **Recommended Treatment Strategy:** (Mitigate/Accept/Transfer/Avoid)
- **Specific Action Plan:**

Part D: Risk Monitoring & Reporting (30 mins)

Technique: Risk Register Entry & Management Summary

Your Task:

1. Formally document **ONE** of your treated risks in the risk register below.
2. Prepare a 3-bullet executive summary to present to the owner, Alex.

Deliverable 4: Risk Register Entry

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Treatment Strategy	Action Plan	Owner
SB-001	(e.g., Loyalty app database is hacked...)	(High/Med/Low)	(High/Med/Low)	(High/Med/Low)	(Mitigate/Transfer/etc.)	(e.g., Implement MFA...)	(e.g., Cafe Manager)

Deliverable 5: Management Summary

Prepare your 3-bullet summary for Alex below.

TO: Alex, Owner, SecureBrew Cafe

FROM: GRC Consulting Team

SUBJECT: Key Findings from our Risk Assessment

- Bullet 1: Our assessment identified your most significant risk as [Summarize your top risk].
- Bullet 2: If this occurs, it could lead to [Explain the primary business impact].
- Bullet 3: Our top recommendation is to immediately [State your key action plan].

3. Submission & Debrief

Congratulations on completing the assessment! Please submit your team's completed packet.

Class Debrief Questions (Be prepared to discuss):

1. What was the most challenging part of the risk assessment process?

1. What was the most challenging part of the risk assessment process?
2. Did your team disagree on the likelihood or impact of any risks? How did you resolve it?
3. How would you explain the value of this risk assessment to a small business owner like Alex who is worried about the cost?