SecureBrew Cafe –Risk Assessment Report

To: Alex, Owner, SecureBrew Cafe
From: GRC Consulting Team (Group Two)
Date: 10th October 2025
Subject: Risk Assessment for SecureBrew's New Digital Upgrade.

Introduction:
Background
SecureBrew Cafe is a local coffee shop that has a loyal customer base retained through quality service and a welcoming atmosphere. To keep up with modern customer expectations and larger coffee chains, the owner, **Alex**, recently introduced a **Digital Upgrade** to improve efficiency and customer experience. This upgrade includes:

- **BeanStack Loyalty App** – a mobile application that allows customers to pre-order drinks, load credit, and earn loyalty points. It stores customer emails and limited payment information.
- **Cloud-Based Point-of-Sale (POS) System** – a tablet-based payment platform that manages all credit and debit card transactions.
- **Free Public Wi-Fi** – offered to attract customers who want to relax, work, or study in the café.

While these digital modifications add convenience, they also expose SecureBrew to potential **cybersecurity, compliance, and operational risks**. With growing reports of data breaches and attacks targeting small businesses, the understanding of the risks associated with these new technologies is significant, to take the right preventive actions to keep the client data safe from any unauthorized personnel.
Objective

The main objectives of this assessment are to help Alex as the owner of SecureBrew Cafe:

1. **Identification** of potential risks arising from its digital systems upgrade and business operations.
2. **Evaluation** of each risk's likelihood and potential impact on operations, finances, and reputation.
3. **Prioritize** the most critical risks for immediate attention.
4. **Recommendation** of practical treatment measures to minimize risk exposure and enhance overall resilience.

Ultimately, this assessment aims to provide **clear, actionable guidance** to Alex and the SecureBrew team so they can easily apply it to safeguard customer trust and ensure smooth business continuity.
Scope

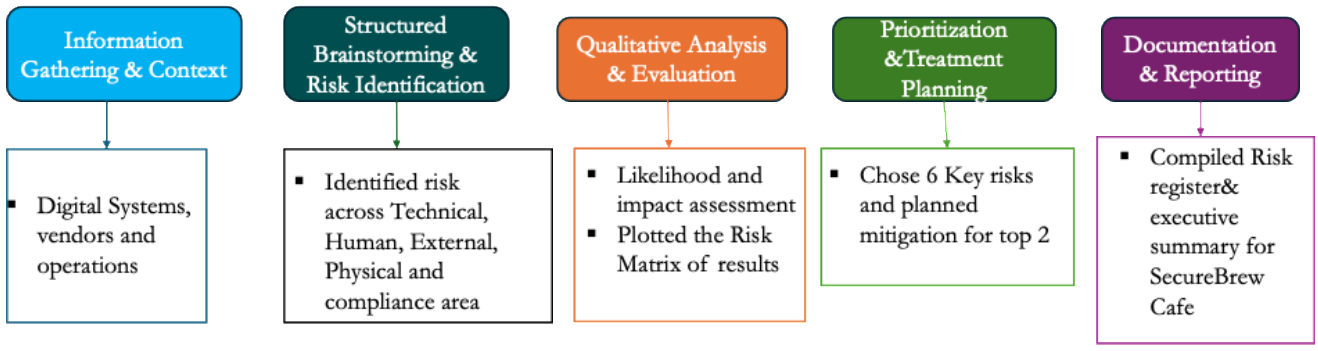
This comprehensive risk assessment covers all aspects of SecureBrew Cafe's operations that could influence the security, reliability, or continuity of its services. The focus areas include both **digital and supporting operational elements**, ensuring a comprehensive understanding of potential threats.

The key areas in scope are:

- **BeanStack Loyalty App** – customer data management, payment storage, and backend security.
- **Cloud-Based POS System** – transaction processing, data integrity, and system availability.
- **Public Wi-Fi Network** – customer access, network segmentation, and potential data interception.
- **Employee Practices** – password hygiene, phishing awareness, and data handling procedures.
- **Physical Devices and Assets** – POS tablets, routers, power sources, and storage equipment.
- **Third-Party Vendors and Suppliers** – service providers or partners whose performance or cybersecurity posture could affect SecureBrew's operations (e.g., payment processors, app developers, and raw material suppliers).
- **Environmental and Operational Dependencies** – power supply, infrastructure, and building safety conditions that could interrupt digital systems or customer service delivery.

This inclusive scope ensures no potential loopholes or blind spots remain unassessed, allowing SecureBrew to take a balanced, proactive approach to risk management across all business areas.

SecureBrew Cafe Risk Assessment Methodology Flow



Part A: Risk Identification: Brainstorming Risk List

1. Employee tricked by a phishing scam.
2. Non-compliance with PCI DSS standards leading to regulatory fines.
3. Ransomware or malware attack on the POS system.
4. Insider threats, such as staff stealing, altering, or selling sensitive information.
5. Unauthorized physical access to secured areas (server or record rooms).
6. A DDoS attack disrupting critical services.
7. A critical third-party vendor suffers a cyberattack or operational failure, affecting deliveries or menu operations.
8. Hacker intercepts data over unsecured public Wi-Fi (Man-in-the-Middle attack).
9. Weak passwords or poor account management leading to unauthorized system access.
10. Server crash, network failure, or system/app downtime.

11. Theft of POS tablet or other critical hardware.
12. Lack of employee training leading to mishandling of sensitive data and potential regulatory fines.
13. Information leakage via improper disposal of gadgets or documents (dumpster diving).
14. Malware infection on customer or staff devices from unsafe sources.
15. Physical damage to equipment (example, coffee spill), disrupting network or POS operations.

Part B: Risk Analysis & Evaluation: Qualitative Risk Matrix

Risk ID	Risk Description	Impact	Likelihood
R01	Employee tricked by a phishing scam	High	High
R02	Non-compliance with PCI DSS standards leading to regulatory fines	High	Medium
R03	Ransomware or malware attack on the POS system	High	Medium
R04	Insider threats, such as staff stealing, altering, or selling sensitive information	High	Low
R05	Unauthorized physical access to secured areas (server or record rooms)	Medium	Low
R06	A DDoS attack disrupting critical services	Medium	Low
R07	A critical third-party vendor suffers a cyberattack or operational failure, affecting deliveries or menu operations	High	Medium
R08	Hacker intercepts data over unsecured public Wi-Fi (Man-in-the-Middle attack)	Medium	Medium
R09	Weak passwords or poor account management leading to unauthorized system access	High	Medium
R10	Server crash, network failure, or system/app downtime	Medium	Medium
R11	Theft of POS tablet or other critical hardware	Medium	Low
R12	Lack of employee training leading to mishandling of sensitive data and potential regulatory fines	Medium	High
R13	Information leakage via improper disposal of gadgets or documents (dumpster diving)	Low	Low
R14	Malware infection on customer or staff devices from unsafe sources	Medium	Medium
R15	Physical damage to equipment (example, coffee spill), disrupting network or POS operations	Medium	Medium

Top 6 Risks Chosen

Risk ID	Risk Description	Impact	Likelihood
R01	Employee tricked by a phishing or social engineering attack.	High	High
R02	Regulatory non-compliance (PCI DSS) leading to fines or operational restrictions	High	Medium
R03	Ransomware or malware attack on the POS system	High	Medium
R04	Loyalty Database Data Breach (PII Theft)	High	High
R05	Man-in-the-Middle (MitM) Attack via Public Wi-Fi	Medium	Medium
R06	Unsecured Internal/Public Network Integration	High	Medium

Likelihood & Impact metrics.
Likelihood (Probability)

Level	Description	Example
High	Expected to occur frequently	Happens several times per year
Medium	Could occur occasionally	Once every 1–2 years
Low	Unlikely to occur	Rare, less than once every 3–5 years

Impact (Consequence)

Level	Description	Example
High	Severe financial, reputational, or regulatory damage	Major data breach, customer loss, or fine
Medium	Noticeable but recoverable impact	Temporary outage, minor data loss
Low	Minor inconvenience	Small technical issue, no long-term harm.

Qualitative SecureBrew Café Risk matrix:

Impact	Low Likelihood	Medium Likelihood	High Likelihood
High		**R02, R03, R06**	**R01, R04**
Medium		**R05**	
Low			

High Priority Risks: **R01, R04** require immediate attention and mitigation.

Part C: Risk Treatment Strategies

Technique: Selecting and Justifying Treatment Option tailored to SecureBrew Café.

High Priority Risks:

Risk ID: R01
Risk Description:
An employee could be tricked by a fake email or message (phishing) into sharing passwords or clicking harmful links. This could allow hackers to get into the café's systems or steal information.

Recommended Treatment Strategy: Mitigate (Reduce the risk)

Why this choice:
This is a common problem that can't be fully avoided because people make mistakes. However, we can **reduce the chances** of it happening and **limit the damage** if it does.

Action Plan:

- Train all employees to **spot fake emails and scams** and show them what to do if they receive one.
- Run **practice tests** every few months(quarterly) to help staff stay alert and improve their response to suspicious emails.
- Set up **two-step verification (MFA)** for logging in, so even if someone's password is stolen, hackers can't easily get in.
- Use **email filters** to block suspicious or spam messages before they reach staff inboxes.
- Have a **clear reporting process** so employees know who to contact if they suspect a phishing attempt.

Risk ID: R04
Risk Description:
Someone could hack into the café's loyalty database and steal customers' personal information, like names, emails, or payment details. This could cause fines, loss of trust, and bad publicity for the business.

Recommended Treatment Strategy: Mitigate (Reduce the risk)

Why this choice:
We can't avoid collecting customer data because it's part of the café's loyalty system, but we can **protect it better** and **monitor who has access** to it.

Action Plan:

- Protect the database by **encrypting customer information**, so even if stolen, it can't be read.
- Only allow **authorized staff** to access the loyalty database, and keep a record of who logs in.
- Regularly **update and secure** the system to fix any weaknesses.
- Carry out **privacy checks** every few months to ensure we follow data protection rules.
- Have a **plan ready** for how to respond quickly if a data breach happens, including notifying affected customers.

Part D: Risk Monitoring & Reporting

Technique: Risk Register Entry

Risk ID	Risk Description	Likelihood	Impact	Risk Level	Treatment Strategy	Action Plan	Owner
R01	Loyalty database could be hacked, exposing customers' personal details (like names, contact info, or payment data). This could cause customer trust issues, fines, and reputational damage.	High	High	High	Mitigate	Encrypt all customer data in storage and during transfer. - Limit access to the loyalty database to only authorized staff. - Apply regular security updates and privacy checks. - Prepare an incident response plan for any data breach.	**Café Manager** (with support from an IT consultant)

Summary of the Register entry

- This risk is rated **High** because of both its likelihood and potential impact on the business.
- The **Mitigation** strategy focuses on prevention, staff access control, and response readiness.
- The **Café Manager** is responsible for ensuring that these actions are carried out, with help from a trusted **IT support consultant.**

To make sure the controls we have recommended continue to work effectively, SecureBrew Café will monitor key risks and review them regularly. The goal is to stay alert, identify any early warning signs, and take action quickly before a small issue turns into a major problem.

1. Monitoring Approach

- **Monthly Checks:**
  The café manager (with support from the IT consultant) will check that all software, payment systems, and Wi-Fi networks are updated and functioning securely.
- **Quarterly Risk Review:**
  Every three months, a short risk review meeting will be held to assess whether new threats have emerged (e.g., new scams, system changes, or third-party issues).
- **Incident Log:**
  Any suspicious activity, system malfunction, or customer data concern will be recorded in a simple logbook or spreadsheet for tracking and follow-up.

2. Reporting

- **Internal Reporting:**
  The café manager will provide a summary of risk status and any incidents to the café owner, Alex, at the end of each quarter.
- **External Reporting:**
  For serious incidents, such as data breaches or card processing issues, the manager must notify the payment provider and follow legal reporting requirements (such as notifying affected customers).

3. Continuous Improvement

- Staff will receive short, practical training on safe online behavior every six months.
- Lessons learned from any incident will be used to update security controls, policies, or vendor requirements.
- The goal is to create a **"security-aware culture"** where everyone plays a role in protecting the café's systems and customer data.

Conclusion

This assessment has provided a clear understanding of SecureBrew Café's key digital and operational risks following its technology upgrade. By acting on the recommended treatments—especially for phishing prevention and data protection, Alex and the café team can greatly reduce exposure to costly incidents.
With regular monitoring, staff awareness, and collaboration with IT support, SecureBrew can maintain customer trust, comply with security standards, and continue serving its community safely and efficiently.

Management Summary

TO: Alex, Owner, SecureBrew Café
FROM: GRC Consulting Team
SUBJECT: Key Findings from Our Risk Assessment

- Our assessment identified your most significant risk as a potential data breach of the loyalty app database, where customer personal information (PII)could be stolen or misused.
- If this occurs, it could lead to serious financial penalties, loss of customer trust, and reputational harm, which could directly affect the café's sales and long-term customer relationships.
- Our top recommendation is to immediately strengthen data protection by encrypting customer data, restricting system access, and setting up regular security checks to prevent breaches and ensure compliance with data protection standards.

GROUP 2 NAMES

1	Gean Bernard
2	Khumo Tsoeu
3	Tosin Oyewole
4	Odion Shalom Ebosetale
5	Akinleye Abidat Bolanle
6	Comfort Tosin Olowookere
7	Muminat Lamidi
8	Vandana Mygapu
9	Precious Ogwumike
10	Nabirye Zahara
11	Dolapo Ajibade
12	Nneamaka Edwin
13	Adeola Bamigboye
14	Hussein Kaosara Dolapo
15	Tinyang Stacey Enjeck
16	Stella Oluwabukola Adejumo
17	Azeezat Animashaun
18	Taiwo Olasupo Owolebi
19	Ibrahim Zainab
20	Oluwatimilehin Oluwagbemi
21	Yusroh Titilayo Oduola
22	Olubukola Esther Obisanya
23	Linda Oluwadamilare Ogunsuyi
24	Rachael Gakanyi
25	Halima Abubakar
26	Magdalene Akpan
27	Ojeah Laura