SecureBrew Cafe –Risk Assessment Report

TO: Alex, Owner, SecureBrew Cafe
FROM: GRC Consulting Team
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

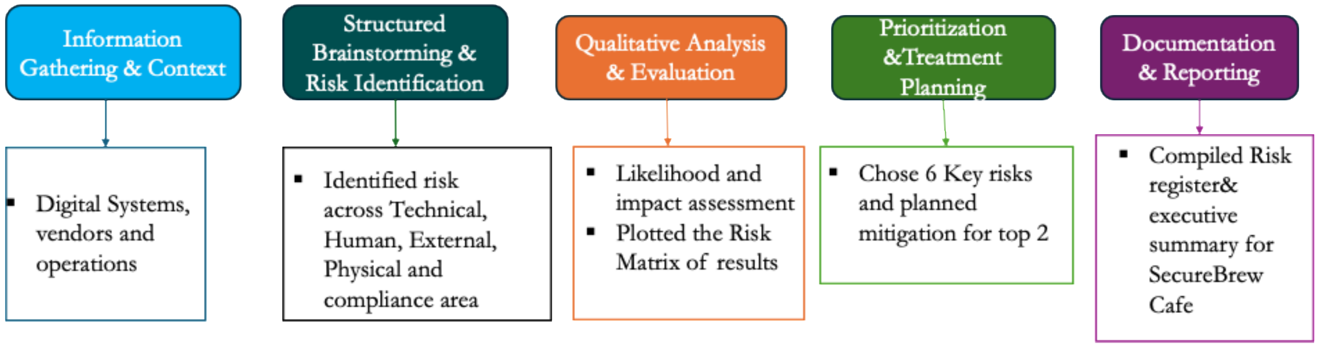
This comprehensive risk assessment covers all aspects of SecureBrew Cafe’s operations that could influence the security, reliability, or continuity of its services. The focus areas include both **digital and supporting operational elements**, ensuring a comprehensive understanding of potential threats.

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


Information Gathering & Context
Digital Systems, vendors and operations
Structured Brainstorming & Risk Identification
Identified risk across Technical, Human, External, Physical and compliance area
Qualitative Analysis & Evaluation
Likelihood and impact assessment
Plotted the Risk Matrix of results
Prioritization &Treatment Planning
Chose 6 Key risks and planned mitigation for top 2
Documentation & Reporting
Compiled Risk register& executive summary for SecureBrew Cafe

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

Qualitative SecureBrew Café Risk matrix: