

We Do Stuffs Security Risk Assessment

Initial Review
.....

Next Review due

1. Purpose and Scope

This assessment identifies and evaluates security risks affecting the coffee shop's:

- Staff and customers
- Physical assets and infrastructure
- Information and financial systems
- Reputation and continuity of business

It focuses on on-site security, cash handling, access control, information security, and emergency response.

2. Risk Rating System

Likelihood Scales	Description	Score	Impact Scale	Description	Score
Rare	May occur in exceptional circumstances	1	Minor	Little to no injury/damage	1
Unlikely	Could occur at some time	2	Moderate	Some damage/injury, manageable	2
Possible	Might occur at some time	3	Major	Significant damage/injury, business impact	3
Likely	Will probably occur	4	Severe	Severe damage/injury, business closure	4
Almost Certain	Expected to occur frequently	5	Critical	Catastrophic loss, fatality, bankruptcy	5

Risk Level = Likelihood × Impact

1–5 = Low | 6–10 = Medium | 11–15 = High | 16–25 = Critical

3. Identified Security Risks

#	Threat / Hazard	Likelihood	Impact	Risk Level	Current Controls	Recommended Controls
1	Theft (tip jar)	4	3	12 (High)	Locked tipped jar, CCTV, Cashless signs displayed.	Ensure all staff follow guidance and empty tip jar regularly. Find a lockable tip jar
2	Break-ins after hours	3	4	12 (High)	Reinforced doors, monitored alarm system, security cameras	Ensure all staff are trained on the alarm system and it is correctly used
3	Robbery during operating hours	2	5	10 (Medium)	Staff trained in comply to demands	Panic alarm, silent alert to authorities, regular security drills
4	Vandalism (graffiti, broken windows)	3	2	6 (Medium)	Lighting left on, CCTV facing doors	CCTV signage, alert 24-hour security on site of the risks
5	Unauthorized access to staff-only areas	3	3	9 (Medium)	“Staff only” signage	Keypad access to BOH areas, staff training during induction around the security
6	Data theft (POS system breach)	2	4	8 (Medium)	Password protection	Two-factor authentication, encrypted Wi-Fi, regular system updates
7	Customer altercation / aggressive behavior	3	3	9 (Medium)	Staff conflict training	De-escalation training, panic button, staff radio
8	Fire / arson	2	5	10 (Medium)	Smoke detectors, extinguishers	Staff fire response training
9	Delivery theft (supplies left outside)	3	2	6 (Medium)	Manual checks and delivery scheduling.	Communicate OOO procedure to suppliers
10	Suspicious packages / bomb	1	5	5 (Low)	Emergency plan	Staff awareness, evacuation plan, investigate city co relationship. ACT-e learning course

4. Additional Considerations

- CCTV Coverage: Ensure clear coverage of entrances, exits, cash register, and seating areas.
- Lighting: Adequate exterior lighting to deter intruders.
- Cash Management: Minimize cash kept on site and use safes with time-delay locks.
- Training: Staff should receive regular training on robbery response, emergency evacuation, and de-escalation.
- Cybersecurity: POS systems should be regularly updated, and Wi-Fi should be segmented (staff vs. guest networks).

5. Emergency & Incident Response Plans

Incident	Response Actions	Responsible Person
Robbery	Stay calm, comply with demands, contact police as soon as possible.	Manager / Shift Leader
Break-in	Do not enter, call police, preserve scene	First arriving staff
Aggressive customer	Use de-escalation, call security or police if needed	All staff
Fire	Evacuate, call emergency services, use extinguisher if safe	All staff
Cyber breach	Disconnect system, contact POS provider, inform customers if required	Manager / IT

6. Review and Monitoring

- Frequency: Every 6 months or after any incident.
- Audit: Security systems and procedures should be audited annually.
- Documentation: All incidents must be logged and reviewed for patterns or gaps.

Sign off

Name	Position	Signature	Date