PREMIUM CAT
DEFENSE

"Guarding Your Feline's World with Excellence"

Protection - "Guarding" reinforces the defense aspect
Care - "Your Feline's World" shows personalized attention
Quality - "Excellence" reflects the premium nature of the brand

***** Internal Confidential *****

Risk Management Plan

Project: *Cybersecurity Awareness & Incident Reporting Tool*
Company: Premium Cat Defense
Version: 1.0
Date: November 2025

1. Objective

The objective of this document is to ensure a proactive and structured approach to identifying, analyzing, mitigating, and monitoring potential risks that may impact the successful delivery and sustainability of the *Cybersecurity Awareness and Incident Reporting Tool*.

This framework blends **analytical precision** with **strategic foresight**, enabling the project to respond intelligently to uncertainty while maintaining excellence — true to our motto:

> *"Guarding Your Feline's World with Excellence."*

2. Methodological Approach

The Premium Cat Defense Risk Management approach follows five key stages:

Phase	**Description**
1. Prepare	Define evaluation structure using the AMDEC Matrix
2. Identify	Detect risks using QQOQCCP and PESTLEO methodologies
3. Analyze	Evaluate risk severity and occurrence using a Criticity Matrix
4. Mitigate	Plan preventive and curative actions
5. Monitor	Continuously track risks and update mitigation strategies

3. Prepare — AMDEC Matrix (Failure Mode and Effects Analysis)

Kindly refer to the following link: Project_Risk

4. Identify — QQOQCCP and PESTLEO Analysis

4.1 QQOQCCP (Who, What, Where, When, How, How Much, Why)

Question	Example in Context
Who	All internal employees and the IT Security Team
What	Reporting cybersecurity incidents through Power Apps
Where	Within the Microsoft 365 ecosystem
When	Any time an incident or suspicious activity is observed
How	Using forms connected to Power Automate & SharePoint
How Much	Minimal operational cost, but high reputational value
Why	To improve awareness, reporting speed, and threat response

4.2 PESTLEO (Macro-Environmental Risk Scan)

Factor	Description	Potential Impact
Political	Changes in data privacy laws	Compliance adjustments required
Economic	Budget constraints for Power Platform licenses	Delayed deployment or scaling
Social	User resistance or lack of cybersecurity awareness	Low tool adoption

Technological	Power Automate or BI service downtime	System unavailability
Legal	GDPR and data protection regulations	Legal and compliance exposure
Environmental	None directly (cloud-based)	Negligible
Organizational	Turnover in security staff	Knowledge gaps, slow response

5. Analyze — Criticity Matrix

5.1 Risk Evaluation Criteria

Impact Level	**Definition**
Low (1–3)	Minor inconvenience, no major effect on the project
Medium (4–6)	Noticeable effect, moderate recovery time
High (7–9)	Major disruption or loss of critical function
Critical (10)	Severe failure, project or data compromise

Probability Level	**Definition**
Low (1–3)	Unlikely to occur
Medium (4–6)	Possible during the project lifecycle
High (7–9)	Likely to occur at least once
Very High (10)	Almost certain occurrence

5.2 Criticity Matrix Visualization

	Low Impact	**Medium Impact**	**High Impact**	**Critical Impact**
Low Probability	Minor	Low	Medium	Medium
Medium Probability	Low	Medium	High	High
High Probability	Medium	High	Critical	Critical
Very High Probability	High	Critical	Critical	Critical

Top Critical Risks Identified:

1. Low user adoption → *High probability* × *High impact*
2. Power Automate workflow failure → *Medium probability* × *High impact*
3. Data loss or corruption → *Low probability* × *Critical impact*

6. Mitigate — Preventive and Curative Actions

Risk	**Preventive Action**	**Curative Action**
Workflow failure	Regular flow testing and automated failure alerts	Restart flow, trigger manual alert protocol
Data corruption	Implement backup and version control in SharePoint	Restore from backup and notify stakeholders
Unauthorized access	Enforce MFA and role-based permissions	Revoke compromised credentials, audit logs
User adoption issues	Conduct awareness training and internal promotion	Re-train teams, simplify UI, monitor usage
Reporting delays	Use Power Automate retry policy	Notify system admin for manual rerun

Preventive = avoid occurrence; **Curative** = minimize impact after occurrence.

7. Monitor — Risk Tracking Framework

Risk ID	Description	Owner	Status	Mitigation Progress	Last Reviewed
R-001	Power Automate workflow failure	DevOps Team	In Progress	Monitoring automated alerts	01-Nov-2025
R-002	SharePoint data corruption	Data Admin	Controlled	Backup scheduled weekly	29-Oct-2025
R-003	Unauthorized access	Security Lead	Controlled	MFA enforced across accounts	30-Oct-2025
R-004	Low adoption	Project Owner	Critical	Awareness campaign ongoing	02-Nov-2025
R-005	Dashboard delays	Analyst	Moderate	Refresh frequency adjusted	01-Nov-2025

Monitoring is performed **bi-weekly** by the Scrum Master and reviewed in sprint retrospectives to ensure continuous alignment between project objectives and risk posture.

8. Continuous Improvement

Risk management at Premium Cat Defense is **not static**. Every identified risk feeds back into:

- **Agile sprint reviews** for operational action
- **Lessons-learned sessions** for preventive reinforcement
- **Dashboard KPIs** for executive visibility

We treat risk not as a threat — but as a **signal for growth and refinement**.

"Premium Cat Defense – Because vigilance is the new strength."