PROJECT PLAN

Pampered Pets Risk Assessment & Digital Transformation Report

Phase 1 – Setup & understanding

Card: Pre-Work – Read & analyse brief

- T**hree business questions**:
    - Could an online presence grow the business by up to 50%?
    - Could changing to an international supply chain reduce costs by up to 24%?
    - Could the business lose up to 33% of its existing customers if the business doesn't provide some online features?
- Note grading weightings & 1,000-word main content limit.

Card: Pre-Work – Lecture Materials

- Lecture 1 (Risk process, qualitative vs quantitative, OCTAVE).
- Lecture 2 (Threat modelling – STRIDE/DREAD, OCTAVE-S, CVSS, attack trees).
- Lecture 3 (GDPR, ISO 27001, PCI-DSS, NIST, COBIT, ITIL).

Card: Pre-Work – Agree Group Workflow

- Trello board? Or Teams Planner (if it works for guest members)
- Google Docs – to work on the report
- Harvard Cite Them Right reference tracking (ongoing)

Card: Pre-Work – Agree roles/tasks

- **Project Lead**: Oversees deadlines, coordinates sections, ensures alignment with the brief and marking rubric.
- **Research Lead**: Gathers relevant data, threat intelligence, and industry references for both current and digitalised risk assessments.
- **Writing & Editing Lead**: Ensures consistency in tone, structure, formatting, and referencing.
- **Graphics/Visuals**: Creates diagrams, Gantt charts, and any visual risk models.

Part 1 – Current State Risk Assessment

(1a) Select & Justify Risk Assessment Methodology

- Small business context.
- Justify choice (Pros/Cons)
- Options:
    - OCTAVE (Variants: OCTAVE, OCTAVE-S, OCTAVE ALLEGRO, OCTAVE FORTE)
    - NIST SP 800-30 Risk Management Guide
    - ISO 27005
    - FAIR (Factor Analysis of Information Risk)

(1b) Risk & Threat Modelling – Current State

Checklist:

- Identify key assets (store, systems, customer data, supplier relationships).
- Create architecture overview.
- Threat model with justification
        - STRIDE
        - DREAD
        - CVSS
        - Attack tree
        - PASTA
        - MITRE ATT&CK
        - OWASP
        - OCTAVE-S
        -

(1c) Mitigations – Current State

Checklist:

- **Physical controls:**.
- **Procedural controls:**
- **Technical controls:**.
- **Regulatory compliance:**

Part 2 – Digitalisation Risk Assessment

(2a) Select & Justify Risk Assessment Methodology

- options.
- Justify choice academically.

(2b) Define proposed digitalisation changes

Checklist:

-
-

(2c) Risk & threat modelling – digitalisation scenario

Checklist:

- Identify new assets (website, payment system, supplier contracts).
- Use threat model (e.g STRIDE) to categorise threats.
- Apply e.g DREAD to rate severity.
- **Q1 – Online growth potential:** assess feasibility of up to 50% increase in sales.
- **Q2 – International supply chain:** assess possible 24% cost reduction.
- **Q3 -**

(2e) Mitigations – Digitalisation Scenario

Checklist:

- **Cybersecurity controls:**
- **Procedural controls:**
- **Technical controls:**
- **Compliance & standards:**

Part 3 – Analysis & recommendation

(3) Compare Risk Profiles

Checklist:

- Create a side-by-side risk matrix: current state vs digitalised scenario.
- Show residual risk after mitigations.
- Highlight Q1, Q2, Q3 findings in comparison.

(4) Final recommendation

Checklist:

- Decide on digitalisation, status quo, or hybrid.
- Justify choice with evidence from both assessments and business viability factors.

Part 4 – Report Writing & Submission

Card: Create report outline

- Sections: Intro, methodology, current state, digitalisation, recommendations, references?

Card: Add diagrams

- E.g. Risk matrix, process flows, Gantt/timeline?

Card: References

- Essex Cite Them Right Harvard style.

Card: Review & proofreading

- Check against brief's points 1–3 and marking criteria.

Card: Submit final version