Group work plan for the Assignment 1

Day	Milestone
Day 1	Distribute sections, set communication plan
Day 3	Individual drafts ready
Day 4	Team meeting to align all work
Day 5	Final write-up, formatting, references
Day 6	Submission

Job to be done in 3 weeks

A risk identification report that:

1. Assesses the current (non-digital) business risks.
2. Assesses future risks from digitalisation.
3. Compares both options and recommends a path.
4. Is clearly structured, referenced, concise (likely ~1000 words).
5. Includes justified methodologies, threat modelling, and risk mitigation.

Report needs to meet following objectives:

- Identify and assess cybersecurity risks arising from digital transformation.
- Evaluate three business scenarios (online presence, international supply chain, loss of customers).
- Recommend cybersecurity controls for the new setup.

1. Introduction (Team Lead)

- Brief overview of Pampered Pets.
- Scope and purpose of the report.
- Importance of cybersecurity and digital risk assessment.

2. Risk Assessment of Current Business (25%) **(Mohamed Harahsheh)**

Assigned To: Cyber Risk Analyst / Researcher

- **Methodology Selection**
  - E.g. *ISO/IEC 27005*, *NIST SP 800-30*, or *OCTAVE*.
  - Justify choice based on scale and nature of business.
- **Threat & Risk Modelling**
  - Identify threats: unsecured Wi-Fi, outdated systems, shared personal devices, lack of backup, no formal access control, etc.
  - Use STRIDE or custom matrix.
  - Rate each threat: *Likelihood* × *Impact*.
- **Risk Mitigation Suggestions**
  - Basic firewall, password policies, disable unused ports, upgrade hardware, use local backup solutions, staff awareness training.

3. Risk Assessment of Digitalisation Plan (15% + 15%)

Assigned To: Application/Tech Analyst + Critical Evaluator

- **Digitalisation Proposals**
  - Online store (e-commerce)
  - ERP/Inventory software
  - Cloud storage
  - Digital marketing (website, social media)
  - Online payments
- **Methodology Selection**
  - Possibly a more dynamic framework like NIST Cybersecurity Framework or Risk Matrix.
  - Justify based on new tech adoption and external interactions.
- **Threat & Risk Modelling**

- Online threats: phishing, DDoS, data breaches, customer data exposure (GDPR), insecure APIs, supply chain cyber risk.
- Use threat tables or diagrams.

- **Risk Mitigation Suggestions**
  - MFA, HTTPS, secure payment gateway, privacy policy, endpoint security, penetration testing, DDoS mitigation tools, staff training.

4. Recommendation Section (10% + 10%) **(Shaikha Al Alawi)**

Assigned To: Strategic Analyst / Lead Writer

- Summary of Key Risks and Benefits
- Decision: Recommend digitalisation, with a phased, secure, and well-funded rollout.
- Include critical reasoning: e.g., competitive pressure, long-term efficiency, customer expectations.
- Highlight importance of ongoing risk monitoring.

Moving this part to the last part of the report before submission

5. Presentation & Style (25%)

Assigned To: Proofreader / Editor / Visual Designer

- Clear structure, good formatting.
- Harvard-style referencing.
- Check spelling, grammar, flow.
- Insert a risk matrix or Gantt chart if needed (showing timeline of digital adoption with security tasks).

Team Roles & Workload Distribution

Team Member	Section	Deadline
Team Leader	Introduction + Coordination + Final Review	Day 1–6
Member A	Section 2: Current Business Risk	Day 1–3
Member B	Section 3: Digitalisation Risks	Day 1–3
Member C	Section 4: Recommendations	Day 3–4
Member D	Proofreading, Visuals, Formatting	Day 5
Whole Team	Peer Review & Discussion	Day 4–5

Recommended References for the work:

1. ISO (2022) *ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. Geneva: International Organization for Standardization.

2. National Institute of Standards and Technology (NIST) (2022) *Guide for Conducting Risk Assessments (SP 800-30 Rev. 1)*. Available at: https://nvlpubs.nist.gov (Accessed: 1 August 2025).

3. European Union Agency for Cybersecurity (ENISA) (2023) *Threat Landscape 2023*. Available at: https://www.enisa.europa.eu (Accessed: 1 August 2025).

4. Sarker, I.H. (2022) 'Cybersecurity risk management in the era of digital transformation', *Journal of Cybersecurity and Privacy*, 2(3), pp. 435–456. https://doi.org/10.3390/jcp2030022

5. Alasmary, W. et al. (2021) 'Secure digital transformation: Threats and risk mitigation strategies', *Computers & Security*, 104, 102165. https://doi.org/10.1016/j.cose.2021.102165

6. Alotaibi, B. (2023) 'Cybersecurity challenges in SMEs adopting cloud solutions: A case-based review', *Information Systems Frontiers*. https://doi.org/10.1007/s10796-023-10378-0

7. National Cyber Security Centre (NCSC) (2023) *Small Business Guide: Cyber Security*. Available at: https://www.ncsc.gov.uk/collection/small-business-guide (Accessed: 1 August 2025).