Unit 6 - Seminar 4 Preparation

Title: Security Standards

Please carry out this activity before joining the seminar this week. Your answers will be discussed during the seminar.

Activity

Review the following links/ websites and answer the questions below:

ICO (2020) Guide to the General Data Protection Regulation (GDPR).

PCI Security Standards.org (2020) Official PCI Security Standards Council Site - PCI Security Standards Overview.

HIPAA (2020) HIPAA For Dummies – HIPAA Guide.

1. Which of the standards discussed in the sources above would apply to the organisation discussed in the assessment? For example, a company providing services to anyone living in Europe or a European-based company or public body would most likely be subject to GDPR. A company handling online payments would most likely need to meet PCI-DSS standards.
2. Evaluate the company against the appropriate standards and decide how would you check if standards were being met?
3. What would your recommendations be to meet those standards?

My preparation:

1. Applicable sources

- **GDPR (ICO, 2020):**
  - Pampered Pets must comply with UK GDPR at home and with EU GDPR when serving customers in EU member states.
  - Although GDPR is an EU Regulation, there are national variations in implementation and enforcement.
  - Beyond Europe, Pampered Pets may face similar GDPR-like regulations in other jurisdictions (e.g., CCPA in California, LGPD in Brazil, PIPL in China and PIPEDA in Canada).

- **PCI DSS (PCI Security Standards Council, 2020):** With the introduction of an **e-commerce platform** and online payments, Pampered Pets must comply with PCI-DSS to ensure the secure processing of cardholder data.

- **HIPAA** (HIPAA, 2020) is not applicable**.** HIPAA regulates healthcare providers and insurers in the United States.

2 <u>Evaluate the company against the appropriate standards and decide how would you check if standards were being met?</u>

How to Check if standards are being met

- Evaluated against GDPR and PCI DSS using a standardised information security framework such as ISO/IEC 27001, which provides a structured way to assess risks, controls, and governance against GDPR obligations.
- Compliance with PCI DSS would be checked using the PCI Self-Assessment Questionnaire (SAQ).

3. <u>What would your recommendations be to meet those standards?</u>

- **Conduct a data audit/mapping (GDPR & PCI DSS):** Identify all personal and payment data collected, stored, and shared to ensure lawful, secure processing.
- **Review documentation and policies (GDPR):** Check privacy notice, consent management, retention schedules, data subject rights procedures, and breach response plan.
- **Carry out a Data Protection Impact Assessment (DPIA) (GDPR):** Assess risks linked to new digital systems and international operations.
- **Establish a process for regular PCI-DSS self-assessments:** Benchmark current practices against PCI requirements for payment security.
- **Verify third-party payment providers (PCI DSS):** Ensure chosen payment processors are fully PCI-DSS certified.
- **Run regular technical tests (GDPR & PCI DSS):** Conduct penetration testing and vulnerability scans.
- **Audit access controls and staff practices (GDPR & PCI DSS):** Confirm only authorised users have access to sensitive data and payment systems.
- **Check training and awareness programmes (GDPR & PCI DSS):** Ensure staff understand obligations under both standards and apply secure practices.

4. <u>What assumptions have you made?</u>

- The IT infrastructure will be modernised.
- Service Level Agreements (SLAs) with third-party suppliers are in place.
- The company has sufficient resources and management commitment to invest in compliance measures (people, assets, budget).