Exercise: Security Standards.

Which of the standards discussed in the sources above would apply to the organisation discussed in the assessment?

Evaluate the company against the appropriate standards and decide how would you check if standards were being met?

What would your recommendations be to meet those standards?

What assumptions have you made?

Summary of Standards

UK GDPR (General Data Protection Regulation)

- Applies to organisations processing personal data of individuals in the UK.
- Focuses on data protection, privacy, consent, data subject rights, and breach notification.
- Requires data controllers and processors to ensure legal, fair and transparent data use.

PCI DSS (Payment Card Industry Data Security Standard)

- Applies to any entity that stores, processes or transmits cardholder data.
- Covers secure network architecture, encryption, access control, regular monitoring and vulnerability management.
- Non-compliance may result in fines, increased transaction fees or the loss of ability to process card payments.

In addition to PCI DSS, the PCI Security Standards Council has developed several other related standards that may also apply depending on how payments are handled. These include:

- Point-to-Point Encryption (P2PE) – for encrypting card data at the point of entry.
- PIN Transaction Security (PTS) – applies to physical card reader devices and terminals.
- Mobile Payments on COTS (MPoC) – for accepting payments using mobile devices.
- Software-based PIN Entry on COTS (SPoC) – for entering PINs securely on mobile devices.

HIPAA (Health Insurance Portability and Accountability Act)

- U.S. based regulation that applies to entities handling Protected Health Information (PHI), such as healthcare providers, insurers and related service providers.
- In UK law, this type of information is called “special category data”, and it is similarly protected under UK GDPR.

Relevant Standards for Papered Pets

UK GDPR – **Applicable**

> Pampered Pets is based in the UK and processes personal data, even if it's just email addresses or purchase records, GDPR applies.

PCI Security Standards – **Applicable**

> PCI DSS: If Papered Pets offers card payments, then PCI DSS applies.

HIPAA – **Not Applicable**

> Papered pets is not in the healthcare sector, does not process health related data and is based in the UK. HIPAA does not apply.

Evaluation Against GDPR

- Collects and processes personal data (email addresses, names, purchases).
- Uses networked computers and wireless internet.
- Stores customer information.

Potential Risks:

- No mention of data protection policies or training.
- No clear consent process when receiving personal data via email.
- Wireless network possibly unsecured or shared with personal phones.
- No mention of antivirus, firewalls or access controls on computers.
- Outdated computer systems increase risk of data breach.

Evaluation Against PCI-DSS

Relevant if Papered Pets offer card payments when the customers pay face to face.

Potential Risks:

- No mention of how card payments are processed or secured.
- Shared Wi-Fi could pose a risk if payment terminals are connected wirelessly.
- No indication of firewall or antivirus protection.
- No awareness training or process for handling payment security.

How to Check If Standards Are Met

- Audit existing systems: Examine data stored on computers (spreadsheets, email clients) to check for customer info and how it is secured.
- Network review: Assess Wi-Fi setup, is it password protected? Segregated for business use?
- Device inspection: Check if security software is up to date, if devices are password protected and if data is backed up securely.
- Payment system check: Review card terminal processes, do they store any card data? Is the network PCI compliant?
- Staff practices: Interview employees on how they handle personal data and what security awareness they have.

Recommendations

For GDPR:

- Create a simple data protection policy tailored to their size and operations.
- Secure wireless network: Use WPA2 or WPA3 encryption and have separate guest access for personal devices.
- Password protect computers and encrypt any files with personal data.
- Install antivirus and a basic firewall on all networked devices.
- Maintain a basic record of processing activities, noting what data is collected, why and for how long.
- Train staff on how to handle data properly and what to do in the event of a breach.
- Appoint someone to oversee data protection.

For PCI-DSS (if taking card payments):

- Use PCI compliant payment terminals.
- Do not store cardholder data on spreadsheets, paper or local systems.
- Ensure network security where card readers are used.
- Train staff to spot tampered devices and be alert to phishing or fraud attempts.

Assumptions Made

- The business accepts card payments, even if not online.
- Email orders contain names/contact info, but not sensitive financial details.
- The wireless network is used by both business devices and personal devices.
- Computers in use are not highly secure or up to date.

References

ICO. (2020) *Guide to the General Data Protection Regulation (GDPR)*. Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf (Accessed: 2 April 2025).

PCI Security Standards Council. (2020) *Official PCI Security Standards Council Site – PCI Security Standards Overview*. Available at: https://www.pcisecuritystandards.org/standards/ (Accessed: 2 April 2025).

HIPAA Guide. (2020) *HIPAA for Dummies – HIPAA Guide*. Available at: https://www.hipaaguide.net/hipaa-for-dummies/ (Accessed: 2 April 2025).