**Unit 3 Exercise:** Review the following links/ websites and answer the questions below.

ICO. (2020) [**Guide to the General Data Protection Regulation**](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr)(GDPR).

PCI Security Standards.org. (2020) [**Official PCI Security Standards Council Site - PCI Security Standards Overview**](https://www.pcisecuritystandards.org/standards/).

HIPAA. (2020) [**HIPAA For Dummies**](https://www.hipaaguide.net/hipaa-for-dummies) – HIPAA Guide.

* **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.**

The most appropriate standards that apply to the organization discussed in the assignment appear to be the Payment Card Industry (PCI) Standards. These standards protect payment data throughout the payment lifecycle, focusing on implementing secure practices, technologies, and processes within the organization (Security Standards Council, n.d.). Another well-known standard that would apply to the organization is GDPR, which aims to protect individuals and the data that describes them (Robinson, 2024).

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

The company's digitalization process should follow PCI Standards, since these addresses payment data, whether they come from an online web application or in face-to-face retail. Point of sale systems, routers, and modems often come with generic passwords, which significantly increases the risk of password theft. Another important aspect is the use of firewalls in online web applications. Firewalls are often considered the first line of defense against hackers as they prevent unauthorized access.

To comply with PCI standards, it is crucial to protect cardholder data. Similarly, GDPR also emphasizes the importance of securing sensitive data. PCI standards additionally focus on software-related risks, such as the importance of antivirus programs, regular software updates, restricted physical access, monitoring logs, and vulnerability scanning. (Groot, 2023).

To ensure that software standards are being met, one should undertake thorough system testing, including penetration testing, to address weak points within the system and payment processes.

* **What would your recommendations be to meet those standards?**

To meet the standards one should be constantly aware of novelties presented within the compliences. Additionally, I would recommend them to be vigilant about possible threats and system vulnerabilities, which can be exposed by outdated software, and improper system configurations.

**References:**

Groot, J. (2023) What is PCI Compliance? 12 Requirements & More. Digital Guardian Blog. Available from: <https://www.digitalguardian.com/blog/what-pci-compliance> [Accessed 2 July 2024]

Robinson, S. (2024) General Data Protection Regulation (GDPR). TechTarget. Available from: <https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR> [Accessed 2 July 2024]

Security Standards Council, (n.d) PCI Security Standards Overview. PCI Security Standards. Available from: <https://www.pcisecuritystandards.org/standards/> [Accessed 2 July 2024]