Question:

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.
* 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?

Answer:

After reviewing GDPR, PCI DSS and HIPAA I have come up with the following conclusions:

Regarding the current way, some customers are ordering from the business via email. GDRP does apply since the customer is providing basic information such as name, address, and possibly phone number and email in their order. Therefore the business must comply with the GDRP. Regarding both PCI-DSS, the business does not offer the option for online payment, so the business does not have to worry about this. Finally, regarding HIPPA, the business does not operate health insurance, so the business does not have to worry about this.

However, after the business moves digitally, things change for PCI-DSS. Since the business will use an e-commerce platform which offers online payment, the business has to comply with PCI-DSS. Regarding GDRP, nothing has changed here. The business has to comply with it. Regarding HIPPA, nothing changes here, and the business does not need to comply with it.