Unit 6 seminar preparation - Security standards

Review the following links and answer the questions below:

1. *ICO (2020) Guide to the General Data Protection Regulation (GDPR).*
2. *PCI Security Standards.org (2020) Official PCI Security Standards Council Site - PCI Security Standards Overview.*
3. *HIPAA (2020) HIPAA For Dummies – HIPAA Guide .*

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

> GDPR standards will need to be adhered to for any company operating within the EU or dealing with citizens inside of the European Union.
>
> PCI-DSS standards will need to be implemented if the amount of card transactions exceed >20k transitions within a year or follow level 4 policies and procedures when the quantity of individual transactions are less than <20k
>
> HIPAA would not be required for this particular business due to Animals being exempt from the standard.

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

> To evaluate if a company is following the correct standards, I would review the company's policies and procedures to establish how they are handling payment card details. This can also be inspected further by carrying out an on-site audit to ensure all requirements align to the standards criteria.

What would your recommendations be to meet those standards?

> Seek a consultancy company to provide an assessment of the company and provide guidance on what standards will be required to meet regulation and compliance. Then begin the process of onboarding an experienced professional or team to begin closing the gap in the analysis and recommendations. Once the policies and procedures are in place, carry out an internal and external audit.

What assumptions have you made?

> Nothing is compliant until the policies and procedures have been audited to meet the required standards.