Security Standards

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.

- GDPR
- PCI-DSS

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

- Based on the description of the company, I highly doubt that the applicable standards are being met. Therefore I would:
- Conduct interviews with business owner and responsible employees about the handling of those standards.
- Conduct an external audit to check whether all standards are being met.

What would your recommendations be to meet those standards?

- Creation of clearly understandable governance and policies in regards to applicable standards.
- Reocurring mandatory training for all emplyees to raise awareness about standards which need to be met.
- Implement technical controls such as detection and monitoring systems.
- Conduct external auditing to make sure regulations and laws are complied with.

What assumptions have you made?

- The organisation is rather small and will not expand significantly in the future. Hence, it makes more sense from a financial point of view to draw on the expertise of external partners (i.e. do not inflate the organisation with various dedicated roles such as security officer, risk officer, internal auditing team, etc.).