**E-portfolio exercise: 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.
  + The organisation discussed in the assessment would need to abide by the **GDPR** directive as they are likely to hold data from customers who are European Union citizens, as well as **PCI-DSS** standards as they are processing digital payments, and the **ISO/IEC 27001:2005** standards to ensure customers’ data are stored and managed securely.
* **Evaluate** the company against the appropriate standards and decide how would you check if standards were being met?
  + Via **threat modelling and penetration testing**, the company can be evaluated against the above-mentioned standards and, based on the risk assessment derived from both these frameworks, it would be decided which standards are met and to what extent. Relevant recommendations are included below.
* What would your **recommendations** be to meet those standards?
  + A **VPN** should be used in the organisation to ensure the data are stored and managed securely, especially considering that the staff use wireless connection to connect to potentially unsafe third-party apps on their smartphones.
  + Customers’ personal and financial data must be **encrypted at rest and in transit** to meet the GDPR directive and the PCI-DSS standards respectively, and the ISO/IEC 27001:2005 standards more holistically.
* What **assumptions** have you made?
  + At least the following two assumptions were made:
    - The computer is always **available** for undergoing the required testing.
    - To ensure **effectiveness** of the testing performed, both manual and automated penetration testing will be carried out regularly and corrective actions will be taken to mitigate any risks identified.