**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 (ICO, 2020) as they are likely to hold data from customers who are European Union citizens, as well as **PCI-DSS** standards (PCI, 2020) as they are processing digital payments, and the **ISO/IEC 27001:2005** standards (Humphreys, 2006) 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**(Novokhrestov *et al*., 2020)**and penetration testing**(Almubairik & Wills, 2016), 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** (Ezra *et al*., 2022) 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**(Cheng *et al*., 2017)to meet the GDPR directive (ICO, 2020) and the PCI-DSS standards (PCI, 2020) respectively, and the ISO/IEC 27001:2005 standards (Humphreys, 2006) 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.

**References**  
  
Almubairik, N. A., & Wills, G. (2016) Automated penetration testing based on a threat model. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 413-414). IEEE.  
  
Cheng, L., Liu, F., & Yao, D. (2017) Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* *7*(5): e1211.  
  
Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damasevicius, R. (2022) Secured communication using virtual private network (VPN). *Cyber Security and Digital Forensics*309-319.  
  
Humphreys, T. (2006) State-of-the-art information security management systems with ISO/IEC 27001: 2005. *ISO Management Systems* *6*(1): 15-18.

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).

Novokhrestov, A., Konev, A., Shelupanov, A., & Buymov, A. (2020) Computer network threat modelling. *Journal of Physics: Conference Series* 1488(1): 012002. IOP Publishing.

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