**Wiki Activity – Security Frameworks**

**FAQ Section:**

* Question: What is the primary difference between COBIT and ISO/IEC 27001?
  + Answer: COBIT focuses on IT governance and alignment with business goals, while ISO/IEC 27001 centers on information security management (De Haes & Van Grembergen, 2015; Humphreys, 2016).
* Question: How does ITIL benefit a large hospital?
  + Answer: ITIL provides a framework for managing IT services, ensuring critical systems in a hospital are reliable and secure (Hochstein et al., 2005).
* Question: Why is Lean Six Sigma important in a manufacturing environment?
  + Answer: Lean Six Sigma combines lean manufacturing principles with Six Sigma methodologies to reduce waste, improve process efficiency, and enhance product quality, which is essential in a competitive manufacturing environment (Antony et al., 2016).
* Question: How do HL7 standards impact healthcare organizations?
  + Answer: HL7 standards facilitate the exchange, integration, sharing, and retrieval of electronic health information, which is critical for improving patient care and ensuring interoperability across different healthcare systems (Braunstein, 2014).

**Responses Section:**

1. **Which of the frameworks do you think would be applicable to the following organisations:**
   1. International bank.
   2. Large hospital.
   3. Large food manufacturing factory.

**Analysing the Frameworks and Their Applicability**

**For an International Bank:**

* **Applicable Frameworks:**
  + **COBIT (Control Objectives for Information and Related Technologies):** COBIT is ideal for banks due to its focus on aligning IT with business objectives, managing risks, and ensuring regulatory compliance (De Haes & Van Grembergen, 2015).
  + **ISO/IEC 27001 (Information Security Management):** This framework is critical for banks to ensure the security and confidentiality of customer data (Humphreys, 2016).
  + **ITIL (Information Technology Infrastructure Library):** ITIL helps in the management of IT services, ensuring reliability and efficiency, which is crucial in a banking environment (Hochstein et al., 2005).

**For a Large Hospital:**

* **Applicable Frameworks:**
  + **ISO 9001 (Quality Management Systems):** ISO 9001 ensures consistent quality management practices, crucial for maintaining high standards of patient care (Hoyle, 2017).
  + **ISO/IEC 27001:** Protecting sensitive patient information is critical, and ISO 27001 provides the necessary framework (Humphreys, 2016).
  + **ITIL:** ITIL’s service management focus supports the critical IT infrastructure of hospitals, ensuring continuous service delivery (Hochstein et al., 2005).
  + **HL7 (Health Level 7):** HL7 standards are crucial in healthcare for the seamless exchange of clinical and administrative data (Braunstein, 2014).

**For a Large Food Manufacturing Factory:**

* **Applicable Frameworks:**
  + **ISO 22000 (Food Safety Management Systems):** ISO 22000 is specifically designed for ensuring food safety, which is a top priority in manufacturing (Kheradia & Warriner, 2013).
  + **ISO 9001:** This ensures consistent product quality and process efficiency in manufacturing (Hoyle, 2017).
  + **ISO/IEC 27001:** Protecting proprietary information such as recipes and production processes is vital (Humphreys, 2016).
  + **Lean Six Sigma:** This approach can significantly improve manufacturing efficiency and reduce waste (Antony et al., 2016).

1. **Summarise the tests and recommendations you would make to the owners/ managers for each of the above businesses to help them use the frameworks and comply with industry standards.**

**Tests and Recommendations to help owners use the frameworks and comply with industry standards**

**International Bank:**

* **Tests:**
  + **COBIT:** Evaluate governance and risk management processes, ensuring alignment with regulatory requirements (De Haes & Van Grembergen, 2015).
  + **ISO/IEC 27001:** Conduct regular risk assessments to ensure data protection (Humphreys, 2016).
  + **ITIL:** Test service management processes for efficiency and reliability (Hochstein et al., 2005).
* **Recommendations:**
  + Implement continuous monitoring and audits to maintain compliance with COBIT.
  + Establish a robust ISMS based on ISO/IEC 27001 standards.
  + Adopt ITIL best practices to enhance service management and reduce downtime.

**Large Hospital:**

* **Tests:**
  + **ISO 9001:** Ensure consistent quality management practices across all departments (Hoyle, 2017).
  + **ISO/IEC 27001:** Test the effectiveness of security measures protecting patient data (Humphreys, 2016).
  + **ITIL:** Assess the reliability of IT services critical to patient care (Hochstein et al., 2005).
  + **HL7:** Verify compliance with HL7 standards for data interoperability (Braunstein, 2014).
* **Recommendations:**
  + Implement a comprehensive quality management system aligned with ISO 9001.
  + Regularly update and review ISMS to protect patient data effectively.
  + Use ITIL to improve IT service management, ensuring critical systems are secure and reliable.
  + Ensure that all healthcare systems are HL7-compliant.

**Large Food Manufacturing Factory:**

* **Tests:**
  + **ISO 22000:** Ensure compliance with food safety standards through rigorous testing (Kheradia & Warriner, 2013).
  + **ISO 9001:** Evaluate process efficiency and product quality consistency (Hoyle, 2017).
  + **ISO/IEC 27001:** Test the security of sensitive information and supply chain data (Humphreys, 2016).
  + **Lean Six Sigma:** Assess manufacturing processes for efficiency and waste reduction (Antony et al., 2016).
* **Recommendations:**
  + Strengthen food safety practices by adhering to ISO 22000 standards.
  + Implement ISO 9001 practices to ensure consistent product quality.
  + Secure sensitive information with an ISMS compliant with ISO/IEC 27001.
  + Apply Lean Six Sigma to optimize manufacturing processes and reduce waste.

**References**

Antony, J., Snee, R. D., & Hoerl, R. W. (2016) Lean Six Sigma: Yesterday, Today and Tomorrow. *International Journal of Quality & Reliability Management* 33(6): 1075-1093. DOI: <https://doi.org/10.1108/IJQRM-03-2015-0035>

Barafort, B. et al. (2018) Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces* 60: 95-111. DOI: https://doi.org/10.1016/j.csi.2018.04.011

Braunstein, M. L. (2014) Health Informatics in the Cloud. *Springer.* DOI: https://doi.org/10.1007/978-1-4614-9529-7

De Haes, S., & Van Grembergen, W. (2015) Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5. *Springer*. DOI: https://doi.org/10.1007/978-3-319-14547-1

Hochstein, A., Tamm, G., & Brenner, W. (2005) Service-oriented IT management: Benefit, cost and success factors. *Proceedings of the European Conference on Information Systems* (ECIS 2005) Available from <https://aisel.aisnet.org/ecis2005/100/> [Accessed 01. September 2024]

Hoyle, D. (2017) ISO 9001:2015: An Introduction to the Global Standard for Quality Management Systems. *Routledge*. DOI: https://doi.org/10.4324/9781315267444

Humphreys, E. (2016) Information Security Management Standards: Compliance, Governance and Risk Management. *BCS, The Chartered Institute for IT*. Available from <https://shop.bcs.org/store/221/detail/workgroup?id=9b70bc9c-7ac0-4a88-8729-e37b5d17d818> [Accessed 01. September 2024]

Kheradia, A., & Warriner, K. (2013) Understanding the Science Behind Food Safety and Its Impact on Public Health. *Microbial Risk Analysis* 1: 43-52. DOI: <https://doi.org/10.1016/j.mran.2015.03.001>

Kirvan, P. (2021) A guide to IT governance frameworks: COBIT, ITIL, ISO/IEC 27001 and more. *TechTarget.* Available from <https://www.techtarget.com/searchcio/tip/A-guide-to-IT-governance-frameworks-COBIT-ITIL-ISO-IEC-27001-and-more> [Accessed 01. September 2024]