Collaborative Wiki Development: Security Frameworks

Q1. Which of the frameworks do you think would apply to the following organisations:

a) International bank.
b) Large hospital.
c) Large food manufacturing factory.

1. Security Frameworks

Effective IT security management requires application security, disaster recovery plans, and robust encryption. Abiding by GDPR, PCI DSS, and HIPAA laws is crucial. Creating an IT security framework with rules and processes is necessary to reduce risk, minimise vulnerabilities, and prepare for IT audits (Kirvan, 2023).

Barafort et al. (2018) state that governance, risk management, and compliance are critical challenges for organisations, especially in the era of digitalisation. Process improvement and maturity models can help organisations enhance their practices. ISO offers several process reference and assessment models for different domains. These models provide a guide and structure for process improvement roadmaps.

FAQ (frequently asked questions)

Q1. Which frameworks are appropriate for an international bank?

According to Payne (2017), the NIST Cybersecurity Foundation is the main foundation for cybersecurity compliance for the country's vital infrastructure, including financial services.

Financial institutions must abide by financial regulations to maintain economic security and stability. Banks and other financial service providers can comply with these

regulations and set up robust security procedures to shield confidential information from online attacks using cybersecurity frameworks. Cybersecurity frameworks serve as instructions to strengthen defences against cyberattacks and comply with legal obligations (Chin, 2023).

These are a few of the best cybersecurity frameworks that a multinational bank may use:

a) **Service Organization Control Type 2 (SOC2)** is a cybersecurity framework developed by AICPA to verify that vendors securely manage client data. It specifies over 60 compliance requirements and extensive auditing processes (Cisternelli, 2024).

b) **The NIST** Cybersecurity Framework is a set of guidelines, best practices and standards for businesses to enhance their cybersecurity practices. It is performance-based and adaptable to meet the needs of any organisation, regardless of their size or industry. The framework focuses on five main pillars: Identify, Protect, Detect, Respond and Recover. It encourages communication and fosters risk management awareness and incident response internally and externally (Chin, 2023).

c) **COBIT,** or **Control Objectives for Information and Related Technologies**, is an internationally recognised paradigm for streamlining information security and IT governance procedures in business settings. COBIT focuses on ensuring IT projects match the organisation's business objectives. It gives company leaders, IT specialists, and compliance auditors a consistent vocabulary when discussing management and business goals (Chin, 2023).

d) **COSO** is a joint initiative of five professional organisations that helps companies achieve a risk-based approach to internal controls. Its Internal Control-Integrated Framework covers five components, while its Enterprise Risk Management-Integrated Framework covers 20 principles across five components, aiming to improve cyber-risk management (Kirvan, 2023).

Q2. Which frameworks are appropriate for a large hospital?

Healthcare is a prime target for hackers due to the large amount of personal information it holds. Many healthcare organisations adopt cybersecurity frameworks to

address these challenges and continually develop risk management programs that provide visibility and insight into systems, networks, and data (Symantec, 2018).

More importantly, Hitrust (2015) highlight that healthcare organisations must implement a thorough risk management strategy that tackles all possible risks to electronically protected health information (ePHI) in light of the increasing regulatory scrutiny and constantly changing cyber threats. A system like this makes it easier for organisations to monitor and enforce policies while identifying and reducing information security threats. For instance, information security risks may be managed using a variety of frameworks, some of which include, but are not limited to:

A) **The HITRUST** Common Security Framework is a set of standards designed to be applied to almost any organisation, including those in the healthcare industry. It comprises 14 control categories that help organisations identify potential risks and develop strategies to manage them (Kirvan, 2023).
The HITRUST Common Security Framework is a widely accepted standard for safeguarding healthcare data and protecting organisations. It establishes a comprehensive set of baseline security controls leveraging existing standards and provides clarity and consistency while reducing compliance burden (Scharnhorst, 2023).

B) **The ISO 27001 standard** is an international information security standard that helps companies manage sensitive information. It provides a blueprint of policies, procedures, and controls to set up an effective information security management system. Companies identify and evaluate weaknesses in their systems through a risk assessment (DataGuard, 2023).

C) **The GDPR** is a framework of security requirements that global organisations must follow to protect the security and privacy of EU citizens' personal information. The requirements include controls for restricting unauthorised access to stored data and access control measures, such as least privilege, role-based access, and multifactor authentication (Kirvan, 2023). The GDPR ensures that organisations handle personal data responsibly by implementing various technical measures, including encryption and appropriate retention and deletion policies (ICO, 2018).

D) **Healthcare Information Management Systems (HIMSS)** is a Framework for evaluating and improving healthcare IT infrastructure and processes. The HIMSS Digital Health Framework connects and empowers people to manage their health and wellness. It involves accessible and supportive providers

working within flexible, integrated, and digitally-enabled care environments. These environments use digital tools and technologies to transform care delivery (Snowdon, N.D.).

Q3. Which frameworks are appropriate for a large food manufacturing factory?

The food industry produces a significant amount of waste and consumes considerable water and energy, which results in higher costs and more stringent regulations. Decreasing food waste and energy and water consumption is crucial to establishing a sustainable food system. This can be achieved by monitoring and identifying areas for improvement in the manufacturing process and implementing an appropriate framework to optimise resource efficiency in the food industry (Jagtapet al. 2021).

The following are some relevant frameworks for a large food manufacturing factory:

- **NIST CSF** is a framework for improving critical infrastructure cybersecurity. It addresses energy production, water supplies, food supplies, communications, healthcare delivery, and transportation. It focuses on cybersecurity risk analysis and risk management using security controls based on the five phases of risk management: identify, protect, detect, respond, and recover (Kirvan, 2023).

- **The CIS Critical Security Controls**, Version 8, is a comprehensive list of technical security and operational controls to reduce risks and enhance resilience for technological infrastructures. It includes 18 CIS controls that emphasise the importance of inventory and control of enterprise assets, data protection, audit log management, malware defences, and penetration testing (Kirvan, 2023).

- **The NERC CIP** is a comprehensive set of 14 standards that pertain to utility companies operating in the bulk power system. This framework establishes controls and policies to safeguard critical infrastructure systems against potential security threats. The CIP standards include Cyber Security, Incident Reporting, Response Planning, Supply Chain Risk Management, and Physical Security (Kirvan, 2023).

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

2.1. International Bank: Testing and Recommendations

- **Tests:** To identify areas where COBIT practices are not being implemented or require improvement, perform a gap analysis. To evaluate compliance with SOC2 regulations, conduct stress testing and risk assessments. To ensure thorough customer identification and verification, review the procedures and controls for Know Your Customer (Scytale, N.D.).

- **Recommendations:** Develop an IT governance strategy that adheres to COBIT guidelines. When using risk management techniques, follow the criteria outlined in the NIST Cybersecurity Framework. To reduce the risk of money laundering and comply with regulations, improve KYC procedures, as emphasised by MSFA (2020).

2.1.2. Large Hospital: Testing and Recommendations

- **Tests:** To examine IT procedures and infrastructure, conduct HITRUST evaluations. Conduct simulated surveys by ISO 27001 guidelines to pinpoint opportunities for enhancing patient safety, care quality, and GDPR interoperability among diverse healthcare systems (Hitrustalliance, N.D.).

- **Recommendations:** To enable smooth data sharing between systems through GDPR compliance, implement HIMSS-suggested best practices for electronic health records (HER) and data management. Address any gaps in ISO 27001 mock surveys to acquire certification (Hitrustalliance, N.D.).

2.1.3. Large Food Manufacturing Factory: Testing and Recommendations

- **Tests:** Verify the effectiveness of the CIS Critical Security Controls in identifying operational and technological security measures. Furthermore, conduct an audit to verify NERC CIP standards compliance to guarantee preventative measures and ongoing enhancement. Throughout the production process, assess compliance with the CIS Critical Security Controls (Stouffer et al. 2015).

- **Recommendations:** Review and update the CIS Critical Security Controls regularly in light of fresh data and risk assessments. Maintain the efficacy of the food safety management system by implementing the remedial measures found during NERC CIP standards audits. To ensure the final product's safety and quality, all manufacturing processes adhere to the CIS Critical Security Controls (Stouffer et al. 2015).

References:

- Kirvan, P. (2023). *Top 12 IT security frameworks and standards explained* | *TechTarget*. [online] Available at: https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one?vgnextfmt=print%20%5bAccessed%201%20July%202022%5d [Accessed 21 Feb. 2024].
- Barafort, B., Mesquida, A.-L. & Mas, A. (2018). ISO 31000-based integrated risk management process assessment model for IT organizations. *Journal of Software: Evolution and Process*, 31(1), p.e1984. doi:https://doi.org/10.1002/smr.1984.
- Payne, P. (2017). *Banking Security Framework – CSIAC*. [online] Available at: https://csiac.org/technical-inquiries/notable/banking-security-framework/ [Accessed 21 Feb. 2024].
- Chin, K. (2023). *Top 10 Cybersecurity Frameworks for the Financial Industry* | *UpGuard*. [online] Available at: https://www.upguard.com/blog/top-cybersecurity-frameworks-finance.
- Cisternelli, E. (2024). *7 Cybersecurity Frameworks To Reduce Cyber Risk*. [online] BitSight. Available at: https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk.
- Chin, K. (2023). *What is the COBIT Framework?* | *UpGuard*. [online] Available at: https://www.upguard.com/blog/cobit.
- Symantec (2018). *Adopting the NIST Cybersecurity Framework in Healthcare*. Available at: https://docs.broadcom.com/doc/adoping-the-nist-cybersecurity-framework-in-healthcare-en.
- HITRUST (2015). *Selecting a Healthcare Information Security Risk Management Framework in a Cyber World.* Available at: https://hitrustalliance.net/content/uploads/HCSC_Childrens_Health_Selecting_Healthcare_Information_Security_RMF_in_a_Cyber_World.pdf.
- Scharnhorst, K. (2023). *5 Ways HITRUST Common Security Framework Protects Data - Health Catalyst*. [online] Available at: https://www.healthcatalyst.com/insights/5-ways-hitrust-common-security-framework-protects-data.
- DataGuard (2023). *How healthcare companies can benefit from ISO 27001 certification*. [online] Available at: https://www.dataguard.co.uk/blog/how-healthcare-companies-can-benefit-from-iso-27001-certification.
- NIST (2020). Security and Privacy Controls for Information Systems and Organizations. *Security and Privacy Controls for Information Systems and Organizations*, [online] 5(5). doi:https://doi.org/10.6028/nist.sp.800-53r5.
- Snowdon, A. (N.D.). *Digital Health: A Framework for Healthcare Transformation.* Available at: https://www.himss.org/sites/hde/files/media/file/2022/12/21/dhi-white-paper.pdf.
- Jagtap, S., Garcia-Garcia, G. & Rahimifard, S. (2021). Optimisation of the resource efficiency of food manufacturing via the Internet of

Things. *Computers in Industry*, 127, p.103397. doi:https://doi.org/10.1016/j.compind.2021.103397.

- ICO (2018). *Guide to the General Data Protection Regulation (GDPR)*. [online] doi:https://doi.org/10.1211/pj.2017.20203048.
- Scytale. (N.D.). *What is Gap Analysis in Compliance*. [online] Available at: https://scytale.ai/glossary/gap-analysis/.
- MSFA (2020). *GUIDANCE ON TECHNOLOGY ARRANGEMENTS, ICT AND SECURITY RISK MANAGEMENT, AND OUTSOURCING ARRANGEMENTS*. Available at: https://www.mfsa.mt/wp-content/uploads/2020/12/Guidance-on-Technology-Arrangements-ICT-and-Security-Risk-Management-and-Outsourcing-Arrangements.pdf.
- Hitrustalliance (N.D.). *Comparing the CSF, ISO/IEC 27001 and NIST SP 800-53*. Available at: https://hitrustalliance.net/uploads/CSFComparisonWhitpaper.pdf.
- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. & Hahn, A. (2015). NIST Special Publication 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). *NIST*. [online] doi:https://doi.org/10.6028/NIST.SP.800-82r2. [Accessed 24 Feb. 2024].