Applicable Frameworks for Different Organisations

1. International Bank

Applicable Frameworks: ISO/IEC 27001, NIST SP 80053, COBIT 2019, COSO ERM, and PCI DSS

Reasoning:

ISO/IEC 27001 provides a comprehensive framework for establishing, implementing, and managing an information security management system (Sharma & Dash, 2012).

ITIL in an international bank enhances IT service management, aligns IT services with business goals, and ensures regulatory compliance, improving service quality, risk management, and customer satisfaction (Nachrowi et al., 2020).

COBIT 2019 helps manage IT governance and align IT processes with business goals, particularly for SOX compliance (Nachrowi et al., 2020).

COSO ERM offers an enterprise-wide approach to identifying and managing risks, aligning with the bank's need for integrated risk management (Bowling & Rieger, 2005)

PCI DSS is mandatory for securing payment card data, which is critical in the banking industry (Willey, L. et al., 2013).

Tests and Recommendations:

IT Governance Assessment: Use COBIT 2019 to evaluate the maturity of IT governance processes, ensuring alignment with business objectives (Legowo & Christian, 2019).

IT Processes: Implementing ITIL processes can significantly streamline IT operations by standardising workflows, improving service management, and ensuring that IT services are aligned with business objectives, ultimately enhancing efficiency and reducing operational risks (Mahalle et al., 2018)

Risk Management Integration: Integrate COSO ERM into the bank’s risk management processes for a holistic approach to risk (Nagumo, 2005).

PCI DSS Compliance Review: Ensure all systems handling payment card data meet PCI DSS requirements (Willey, L. et al, 2013).

Gap Analysis: Conduct a gap analysis against ISO/IEC 27001 and NIST SP 80053 to identify areas for improvement.

2. Large Hospital

Applicable Frameworks: HITRUST CSF, ISO 27799, ITIL 4, NIST SP 800171, and GDPR

Reasoning:

HITRUST CSF integrates multiple healthcare regulations and standards, providing a comprehensive approach to healthcare information security (Udroiu et al., 2022).

ISO 27799 focuses on protecting personal health information (Zarei & Sadoughi, 2016)

ITIL 4 ensures that IT services are aligned with patient care and operational needs (Hoerbst et al., 2011).

NIST SP 800171 is relevant for protecting sensitive data in healthcare environments that interact with federal systems (Udroiu et al., 2022).

GDPR is critical for hospitals handling EU citizens' data, ensuring compliance with stringent data protection laws (Peloquin et al., 2020).

Tests and Recommendations:

Service Management Assessment: Use ITIL 4 to improve IT service management processes, ensuring alignment with healthcare standards (Hoerbst et al., 2011).

Data Protection Assessment: Implement NIST SP 800171 and GDPR controls to protect patient data and ensure compliance (Cawthra et al., 2022) (Yuan & Li, 2019).

Incident Management: Develop ITIL-based incident management processes to address IT disruptions in healthcare quickly (Ahmad et al., 2013).

Integration with HITRUST: Align HITRUST CSF with ISO 27799, NIST SP 800171, and GDPR for comprehensive healthcare data protection (Kandasamy et al., 2022).

3. Large Food Manufacturing Factory

Applicable Frameworks: ISO 22000, NIST CSF, COBIT 2019 and FISMA.

Reasoning:

ISO 22000 is essential for managing food safety risks throughout the supply chain (Chen et al., 2020).

NIST CSF enhances cybersecurity, particularly for industrial control systems in manufacturing (Nagumo, 2005).

COBIT 2019 ensures IT governance aligns with the factory's operational efficiency and regulatory requirements (Bahri & Putra, 2023).

FISMA applies if the factory supplies federal government agencies, ensuring compliance with federal information security standards (Wu & Hsiao, 2021).

Tests and Recommendations:

Governance Framework Implementation: Implement COBIT 2019 to manage IT governance and align with business goals (Rini Audia & Sugiantoro, 2022).

Cybersecurity Enhancement: NIST CSF enhances cybersecurity for industrial control systems and protects the production process (NIST, 2018).

Federal Compliance Review: Assess FISMA compliance if applicable and implement necessary controls.

FAQ Section

Q1: What is the difference between ISO/IEC 27001 and NIST SP 80053?

A1: ISO/IEC 27001 is a global standard focusing on establishing, implementing, maintaining, and improving an information security management system (ISMS). NIST SP 80053 is a U.S. standard that provides a catalogue of security and privacy controls for all U.S. federal information systems except those related to national security. Both standards can be used together, especially in sectors like banking, where comprehensive information security is crucial.

Q2: Why is HITRUST CSF recommended for hospitals instead of just ISO/IEC 27001?

A2: HITRUST CSF is specifically tailored for the healthcare industry, incorporating multiple regulations and standards, including HIPAA, directly relevant to healthcare data protection. ISO/IEC 27001 is broader and more general, while HITRUST CSF provides more specific guidance for managing healthcare information risks.

Q3: How does NIST CSF apply to a manufacturing environment?

A3: NIST CSF is designed to improve the cybersecurity risk management process. In a manufacturing environment, it can be applied to secure industrial control systems (ICS), protect against cyber threats, and ensure the integrity and reliability of production processes. This is especially important for protecting critical infrastructure and maintaining food safety in manufacturing.

Q4: What role does COBIT 2019 play in an international bank's IT governance?

A4: COBIT 2019 is instrumental in aligning IT governance with the bank's strategic goals. It provides a framework for managing and governing enterprise IT, ensuring that IT processes support business objectives, comply with regulatory requirements, and manage risks effectively. It is particularly useful for banks to maintain oversight

and control over IT functions while aligning with global standards like ISO/IEC 27001.

Q5: Why should a hospital consider NIST SP 800171 and GDPR?

A5: NIST SP 800171 is essential for protecting sensitive patient data, especially when the hospital interacts with federal systems. GDPR is crucial if the hospital handles the data of EU citizens, as it sets strict guidelines on data protection and privacy, with heavy penalties for noncompliance.

Q6: How do FISMA and NERC CIP apply to a food manufacturing factory?

A6: FISMA applies if the factory supplies products to the federal government, requiring compliance with federal information security standards. NERC CIP is relevant if the factory is part of the critical infrastructure, particularly in sectors like energy or water, to ensure the security and reliability of operations.

Bibliography

Sharma, N.K. and Dash, P.K., (2012) Effectiveness of ISO 27001 as an Information Security Management System: An Analytical Study of Financial Aspects. Far East Journal of Psychology and Business, 9(3), 42-55. https://scholar.googleusercontent.com/scholar?q=cache:R8NLJX-Ut64J:scholar.google.com/+Effectiveness+of+ISO+27001+as+an+Information+Security+Management+System:+An+Analytical+Study+of+Financial+Aspects.+Far+East+Journal+of+Psychology+and+Business,+&hl=en&as_sdt=0,5 [Accessed 01/09/2024].

Nachrowi, E., Nurhadryani, Y., & Sukoco, H. (2020) Evaluation of Governance and Management of Information Technology Services Using COBIT 2019 and ITIL 4. *RESTI Journal (System Engineering and Information Technology)*, 4(4), pp.764-774. Available at: https://jurnal.iaii.or.id/index.php/RESTI/article/view/2265 [Accessed 01/09/2024].

Willey, L. & White, B. J. (2013) Teaching Case Do you take credit cards? Security and compliance for the credit card payment industry. *Journal of information systems education*. 24 (3), 181-. https://aisel.aisnet.org/jise/vol24/iss3/3/ [Accessed 01/09/2024].

Nagumo, T., (2005) Bank of Tokyo-Mitsubishi Aligns Risk Management with Strategy. *Balanced Scorecard Report*, September–October, pp.41-43. https://scholar.googleusercontent.com/scholar?q=cache:XJncTEJmOJUJ:scholar.google.com/+Bank+of+Tokyo-Mitsubishi+Aligns+Risk+Management+with+Strategy&hl=en&as_sdt=0,5 [Accessed 31/08/2024].

Ahmad, N., Amer, N. T., Qutaifan, F., & Alhilali, A. (2013) Technology adoption model and a road map to successful implementation of ITIL. *Journal of*

Enterprise Information Management, *26*(5), 553–576. https://doi.org/10.1108/JEIM-07-2013-0041/FULL/XML [Accessed 30/08/2024].

Bahri, R. S., & Putra, Y. H. (2023) Improving the Quality of Information System Management in MSMEs Using the COBIT 5 Framework: Preliminary Research. *ICSPIS 2023 - Proceedings of the 9th International Conference on Signal Processing and Intelligent Systems*. https://doi.org/10.1109/ICSPIS59665.2023.10402753 [Accessed 01/09/2024].

Bowling, D. M., & Rieger, L. (2005) Success factors for implementing enterprise risk management: building on the COSO framework for enterprise risk management to reduce overall risk. *Banking Accounting and Finance*. https://go.gale.com/ps/i.do?id=GALE%7CA132240173&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=08943958&p=AONE&sw=w&userGroupName=anon%7Eb7738f55&aty=open-web-entry [Accessed 01/09/2024].

Cawthra, J., Grayson, N., Pulivarti, R., Hodges, B., Kuruvilla, J., Littlefield, K., Snyder, J., Wang, S., Williams, R., & Zheng, K. (2022) *Securing telehealth remote patient monitoring ecosystem*. https://doi.org/10.6028/NIST.SP.1800-30 [Accessed 30/08/2024].

Chen, H., Liu, S., Chen, Y., Chen, C., Yang, H., & Chen, Y. (2020) Food safety management systems based on ISO 22000:2018 methodology of hazard analysis compared to ISO 22000:2005. *Accreditation and Quality Assurance*, *25*(1), 23–37. https://doi.org/10.1007/S00769-019-01409-4/TABLES/9 [Accessed 30/08/2024].

Hoerbst, A., Hackl, W. O., Blomer, R., & Ammenwerth, E. (2011) The status of IT service management in health care - ITIL® in selected European countries. *BMC Medical Informatics and Decision Making*, *11*(1), 1–12. https://doi.org/10.1186/1472-6947-11-76/TABLES/15 [Accessed 01/09/2024].

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022) Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. *IEEE Access*, *10*, 12345–12364. https://doi.org/10.1109/ACCESS.2022.3145372 [Accessed 28/08/2024].

Legowo, N., & Christian. (2019) Evaluation of Governance Information System Using Framework Cobit 5 in Banking Company. *ICSECC 2019 - International Conference on Sustainable Engineering and Creative Computing: New Idea, New Innovation, Proceedings*, 281–286. https://doi.org/10.1109/ICSECC.2019.8907123 [Accessed 28/08/2024].

Mahalle, A., Yong, J., & Tao, X. (2018) ITIL Processes to Control Operational Risk in Cloud Architecture Infrastructure for Banking and Financial Services Industry. *Proceedings - 2018 5th International Conference on Behavioral, Economic, and*

Socio-Cultural Computing, BESC 2018, 197–200. https://doi.org/10.1109/BESC.2018.8697294 [Accessed 28/08/2024].

Peloquin, D., DiMaio, M., Bierer, B., & Barnes, M. (2020) Disruptive and avoidable: GDPR challenges to secondary research uses of data. *European Journal of Human Genetics 2020 28:6*, *28*(6), 697–705. https://doi.org/10.1038/s41431-020-0596-x [Accessed 28/08/2024].

Rini Audia, & Sugiantoro, B. (2022) Evaluation and Implementation of IT Governance Using the 2019 COBIT Framework at the Department of Food Security, Agriculture and Fisheries of Balangan Regency. *IJID (International Journal on Informatics for Development)*, *11*(1). https://doi.org/10.14421/ijid.2022.3381 [Accessed 27/08/2024].

Udroiu, A. M., Dumitrache, M., & Sandu, I. (2022) Improving the cybersecurity of medical systems by applying the NIST framework. *2022 14th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2022*. https://doi.org/10.1109/ECAI54874.2022.9847498 [Accessed 28/08/2024].

Wu, J. Y., & Hsiao, H. I. (2021) Food quality and safety risk diagnosis in the food cold chain through failure mode and effect analysis. *Food Control*, *120*, 107501. https://doi.org/10.1016/J.FOODCONT.2020.107501 [Accessed 28/08/2024].

Yuan, B., & Li, J. (2019) The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. *International Journal of Environmental Research and Public Health 2019, Vol. 16, Page 1070*, *16*(6), 1070. https://doi.org/10.3390/IJERPH16061070 [Accessed 30/08/2024].

Zarei, J., & Sadoughi, F. (2016) Information security risk management for computerized health information systems in hospitals: A case study of Iran. *Risk Management and Healthcare Policy*, *9*, 75–85. https://doi.org/10.2147/RMHP.S99908 [Accessed 30/08/2024].