Security Frameworks

Post by Tobi Zeier

FAQ

What does «SOX» stand for?

Lutkevich (2023) defines SOX in his blog as «The Sarbanes-Oxley Act of 2002 is a federal law that established sweeping auditing and financial regulations for public companies."

Reference:
Lutkevich, B. (2023) Sarbanes-Oxley Act. Available from: https://www.techtarget.com/searchcio/definition/Sarbanes-Oxley-Act [Accessed 31 August 2024]

Applicable frameworks for different industries

Following I will provide IT security framework recommendations which will help the mentioned businesses to comply with industry standards, based on the article by Barafort et al (2018) and the blog by Kirvan (2023).

International bank.

- ISO 31000: Alijoyo & Norimarna (2021) state that "ISO 31000 as an International Standard, gains a very wide acceptance in many countries and large corporations as it is practical and business-oriented."
- GDPR: This framework is mandatory if the business handles EU citizens' personal data (Kirvan, 2023).
- COBIT: Cobit can help to achieve SOX compliance (Kirvan, 2023).

Large hospital.

- ISO 31000: see reasoning above
- HITRUST CSF: Alzuri et al. (2021) state that "HITRUST CSF is a privacy and security framework for health-care organizations. Its approach is based on information security risk management."
- GDPR: This framework is mandatory if the business handles EU citizens' personal data (Kirvan, 2023).
- NIST CSF: Critical infrastructure includes hospitals (Kirvan, 2023).

Large food manufacturing factory.

- ISO 31000: see reasoning above
- ISO 9001: Andres-Jimenez et al. (2020) say that "The ISO 9000 family of standards is a set of quality and quality management standards that specify the requirements for a quality management system (QMS)."

- GDPR: This framework is mandatory if the business handles EU citizens' personal data (Kirvan, 2023).
- NIST CFS: Critical infrastructure includes food supplies (Kirvan, 2023).

Tests and recommendations

Following are the tests and recommendation I would make to owners/managers of each of the above businesses.

Tests

- Vulnearbility scans: detect possible vulnerabilities which could be exploited by attackers.
- Penetration tests: identify vulnerabilities before they can be exploited.
- Network security testing: detect unauthorised access, data leaks, and potential intrusions.
- Application security testing: ensure that all applications handling sensitive data are secure against potential attacks.
- Social engineering testing: valuate the effectiveness of security awareness training and identify weaknesses in human security controls.

Recommendations

- Creation of clearly understandable governance that can be viewed by all employees.
- Reocurring mandatory training for all emplyees to raise awareness about social engineering and security measures.
- Train a person in every team to become security coach.
- Setup risk department which tracks and addresses risks, make them transparent to management and help teams/departments to treat them.
- Setup independet audit department which assesses internal systems and processess regularly.
- Get external auditing to make sure regulations and laws are complied with.

References:

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): e1984. DOI: https://doi.org/10.1002/smr.1984

Kirvan, P. (2023) Top 7 IT security frameworks and standards explained. Available from: https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one [Accessed 2 Semptember 2024].

Alijoyo, A. & Norimarna, S. (2021) The Role of Enterprise Risk Management (ERM) Using ISO 31000 for the Competitiveness of a Company That Adopts the Value Chain (VC) Model and Life Cycle Cost (LCC) Approach. *Proceedings of the 3rd International*

Conference on Business, Management and Finance: 11-14. DOI: https://doi.org/10.33422/3rd.icbmf.2021.03.130

Alzuri, P., Florencia Cabral Berenfus, Paz, S., Nowersztern, A., & Libedinsky, P. (2021) Protecting Digital Healthcare - A Cybersecurity Guide for the Healthcare Sector. *Inter-American Development Bank eBooks*. DOI: https://doi.org/10.18235/0003741

Andres-Jimenez, J., Medina-Merodio, J.-A., Fernandez-Sanz, L., Martinez-Herraiz, J.-J., & Ruiz-Pardo, E. (2020) An Intelligent Framework for the Evaluation of Compliance with the Requirements of ISO 9001:2015. *Sustainability* 12(13): 5471. DOI: https://doi.org/10.3390/su12135471