

Task 'Wiki Activity - Security Frameworks' Unit 5

Framework Suitability Per Organization

International banks should adopt ISO/IEC 27001 together with PCI DSS (for card payment compliance) and optionally NIST Cybersecurity Framework (NIST CSF) to manage broader cyber risks. Sarbanes–Oxley Act (SOX) 2002 is also relevant for an international bank doing business in the US, though it is specific, governance-focused regulation, with some IT-security guidelines, rather than as a full cybersecurity framework.

Large hospital: use ISO/IEC 27001 to institute an Information Security Management System and consider standards tailored to healthcare such as information security for health ISO/IEC 27799 to safeguard patient data and compliance.

Large food manufacturing factory: The NIST CSF for overall risk management is recommended, highly recommended to be complemented by ISA/IEC 62443 as Operational technology (OT) with industrial control systems may very probably be involved in manufacturing.

Recommendations and tests for implementation

Conduct an initial risk assessment & asset inventory to identify critical assets (customer financial data, patient records, industrial control systems). Use NIST CSF “Identify” as baseline.

Develop an Information Security Management System (ISMS) which is aligned with ISO 27001: define policies, roles, and responsibilities; implement access control, data

encryption, backups, logging, and control domains such as confidentiality, integrity, availability.

For organizations processing card payments bank, maybe hospital billing: run a PCI DSS compliance audit where applicable.

For Operational Technology (OT), industrial control systems environments, manufacturing, power plants, perform security tests on OT/ICS network segmentation and segregation between IT and OT, so called Industrial DMZ. vulnerability scans, patch management, as devices in such areas are generally outdated and do not usually support up-to-date security functionality such encryption, authentication and so on, following ISA/IEC 62443 series whom scope is comprehensive.

(Taherdoost, 2022)

Establish asset management, continuous monitoring, incident response, and recovery plans for instance NIST CSF phases: Identify, Detect, protect, Respond and Recover to ensure resilience and audit readiness.

These steps help align organizational practices with internationally recognized frameworks and regulatory obligations, reducing risk exposure and enhancing operational resilience.

Common tests and governance actions: enterprise risk assessment; mapping controls to chosen standard; technical testing, vulnerability scanning, pen testing, OT and ICS scanning, audit and certifications, continuous staff training and incident and crisis exercises. to ensure regulatory compliance and operational resilience.

(Adhillah et al, 2025; Kirvanet et al, 2025)

References

- Kirvan, P., (2025). Top 15 IT security frameworks and standards explained.
Available at: <https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one>. [Accessed 26 November 2025]
- Adhillah, M.N., Syalwa, M., Meilanda, P. and Sari, R., (2025). Systematic Literature Review the Development of Enterprise Risk Management. Jurnal Manajemen Bisnis, Akuntansi dan Keuangan, Available at:
<https://doi.org/10.55927/jambak.v4i1.157> [Accessed 26 November 2025]
- The NIST Cybersecurity Framework (CSF) 2.0 (2024) National Institute of Standards and Technology Available from: <https://doi.org/10.6028/NIST.CSWP.29> [Accessed 26 November 2025]
- Taherdoost H., (2022) Understanding Cybersecurity Frameworks and Information Security Standards, A Review and Comprehensive Overview. Electronics. ;
Available At: <https://doi.org/10.3390/electronics11142181> [Accessed 26 November 2025]

