WIKI Unit 6

FAQ – Security Frameworks

Q1: *What is the difference between a framework and a standard?*

A framework gives structure and guidance for managing security or risk, while a standard defines specific requirements that must be followed. For example, ISO 27001 is a standard, and the NIST Cybersecurity Framework is a framework.

Q2: *Why use different frameworks for different industries?*

Each industry faces different types of risks. A bank must secure financial transactions, a hospital must protect patient data, and a factory must secure both IT and production systems.

Q3: *What is the Purdue model used for?*

The Purdue model is used in industrial environments and Industrial Cyber-Physical Systems (ICPS) to separate IT and OT networks. It helps manage cybersecurity in production systems by creating different layers of protection between business systems and physical machines.

Q4: *What are SCADA and PLC systems?*

SCADA (Supervisory Control and Data Acquisition) systems monitor and control industrial processes such as temperature, pressure, and flow in production lines.

PLC (Programmable Logic Controller) units are hardware devices that control machines and sensors in real time and act as the central control unit of industrial automation.

Applicable Frameworks

International bank

ISO 27001 provides a base for information security governance. The NIST Cybersecurity Framework (CSF) supports risk management, while PCI-DSS protects payment systems. COBIT can also be used to improve governance and meet regulatory needs (Kirvan, 2025). Together, these frameworks help the bank make structured risk-based decisions and keep transparency in how risks are managed, as explained by Aven and Thekdi (2025, pp. 195-223).

Large hospital

ISO 27001 and the sector-specific ISO 27799 help protect patient data and hospital systems. The NIST Cybersecurity Framework is applicable because hospitals are part of the critical infrastructure. GDPR also applies to protect patient data in the EU. Together, these frameworks support better risk control and compliance across the hospital (Adhillah et al., 2025).

Large food manufacturing factory

ISO 27001 gives basic information security. NIST CSF helps to set risk priorities, and IEC 62443 protects industrial control systems. The Purdue model can be used to organise IT and OT networks and manage risks together. Risk management processes can follow an integrated approach as suggested by Barafort, Mesquida, and Mas (2018), while threat modelling should be applied to identify vulnerabilities and improve cyber resilience in smart manufacturing environments (Jbair et al., 2022).

Tests and Recommendations

International bank

Tests:

- Confirm the existence of an ISMS and ISO 27001-style risk assessments.
- Check PCI-DSS controls such as segmentation, encryption and logging.
- Review access control and incident response arrangements.

Recommendations

- Strengthen governance roles.
- Perform regular penetration testing.
- Maintain PCI compliance and integrate cyber risk into wider risk management.

Large hospital

Tests:

- Review access to patient records.
- Check patching and monitoring of clinical systems.
- Assess GDPR compliance and backup procedures.

Recommendations

- Improve monitoring of medical devices.
- Maintain staff security training.
- Review supplier access.
- Formalise incident response in line with ISO 27799.

Large food manufacturing factory

Tests:

- Check segmentation against the Purdue model (Levels 0–5).
- Verify IEC 62443 controls in each zone, including authentication, monitoring and patching.
- Review logging, backups and physical security of Level 0–1 equipment.
- Test IT/OT separation.

Recommendations

- Implement Purdue-aligned zoning and apply IEC 62443 controls.
- Strengthen access control and monitoring on OT systems.
- Use firewalls and a DMZ to separate IT and OT.

- Enforce strict change management for SCADA/PLC devices (industrial control systems that manage and automate production equipment).
- Carry out OT vulnerability assessments in coordination with operations.

References

Adhillah, M.N. et al. (2025)
'Systematic Literature Review the Development of Enterprise Risk Management', *Jurnal Manajemen Bisnis, Akuntansi dan Keuangan*, 4(1), pp. 81–100.

Aven, T. and Thekdi, S. (2025) Risk Science. London: Routledge. Chapter 8.

Barafort, B., Mesquida, AL. and Mas, A. (2018) ISO 31000-based integrated risk management process assessment model for IT organizations.

Jbair, M. et al. (2022) 'Threat modelling for industrial cyber physical systems in the era of smart manufacturing', Computers in Industry, 137, p.103611.

Kirvan, P. (2025) Top 15 IT security frameworks and standards explained.