UNIT 5 - Wiki Activity - Security Frameworks

Read the article by Barafort et al (2018) and the blog by Kirvan (2021). Review the websites listed in the blog and then answer the following questions:

1. **Which of the frameworks do you think would be applicable to the following organisations:**

    a. **International bank.**

    b. **Large hospital.**

    c. **Large food manufacturing factory.**

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

Your responses should be posted in the Module Wiki located in Module Resources.

The Wiki should consist of two sections:

○ **The first section should be a FAQ (frequently asked questions) where you can post questions. In addition, if you have encountered and solved any of the questions/ issues, you should post your responses to the queries.**

○ **The second section involves the responses to the questions above- each of you should post a compilation of your responses in the wiki. Doing so will allow your fellow students to evaluate the recommendations made and also ask questions (in the FAQ) about why certain answers/ decisions were made. Your individual postings should be collated as part of your e-portfolio.**

1. **Which of the frameworks do you think would be applicable to the following organisations:**

Frameworks for the applicable organisations

a. **International bank.**

Chosen Frameworks:

- **COBIT**: Tailored for IT governance and compliance, especially with financial regulations like SOX. Also adopted by central banks to align I&T governance with strategic and regional policy frameworks, such as those promoted by SADC (Soares, 2023).

- **GDPR**: Although GDPR is a regulation rather than a framework, it is mandatory for any bank operating in or serving customers in the EU (EU, 2016)
- **ISO/IEC 27001 or NIST CSF**

  According to an PwC survey 91% of companies surveyed either use NIST CSF or ISO/IEC 27001 (NIST,2017)

  - **ISO 27001**: offers a robust ISMS to support compliance with numerous laws and regulations in the banking sector—such as GDPR, PSD2, SOX, PCI-DSS, and NYDFS—which are essential for protecting sensitive financial data. It can also help banks align with other standards and frameworks like COBIT or NIST (Ewuga et al., 2023)
  - **NIST CSF**: Adopted by many U.S. banks, the NIST Cybersecurity Framework offers a structured, adaptable, and comprehensive approach to managing and mitigating cybersecurity risks (IsoraGRC, 2025). NIST CSF 2.0 aligns with key financial sector standards including regulations for the critical infrastructure (NIST, 2017; Boutin, 2024).
- **ISO 31000**: While not mandatory, ISO 31000 may be considered by an international bank adopting ISO/IEC 27001, as it offers a broader enterprise risk management framework. ISO/IEC 27001 references ISO 31000 as a compatible approach, making it easier to implement ISO 27001 requirements and beneficial for integrating information security risk with other organisational risks (ISO, 2022; Barafort, Mesquida and Mas, 2018).

Not Chosen:

- **HITRUST CSF**: Healthcare-specific; not relevant to banking (Alder, 2024).
- **CIS Controls**: Too technical and narrow; lacks governance and audit depth needed in banking (CIS, 2021).
- **COSO**: More focused on enterprise risk and internal controls; COBIT is more IT-specific and widely adopted in finance.
- **FISMA/NERC CIP**: U.S. federal and energy sector-specific.

b. Large hospital.

Chosen Frameworks:

- **HITRUST CSF**: the HITRUST Common Security Framework (CSF) is primarily designed to address security, privacy, and regulatory compliance in the healthcare industry, and that it integrates requirements from HIPAA, HITECH, and other healthcare-related regulations (HITRUST Alliance, 2023; Alder, 2024).
- **ISO/IEC 27799**: Healthcare-specific extension of ISO 27001 (Kirvan and Granneman , 2023)
- **NIST CSF**: Addresses critical infrastructure like healthcare (Boutin, 2024).
- **ISO 31000**: Supports integrated risk management across clinical and IT domains.

Not Chosen:

- **COBIT**: Too focused on IT governance; lacks healthcare-specific controls.
- **PCI DSS**: Focuses on payment data; not central to hospital operations.
- **CIS Controls**: Technical focus; lacks healthcare compliance integration.
- **COSO**: Useful for enterprise risk but not tailored to healthcare IT.
- **FISMA/NERC CIP**: Not applicable unless hospital is a federal contractor or energy provider.

c. Large food manufacturing factory.

Chosen Frameworks:

- **ISO 9001**: Industry standard for quality management in manufacturing, widely adopted in manufacturing to ensure consistent product quality and continuous improvement (ISO, 2015).
- **ISO/IEC 27001**: It is particularly relevant for food manufacturers integrating digital systems and managing sensitive data, and can complement food safety standards like ISO 22000 (ISO, 2018).
- **NIST CSF**: Applicable due to the food supply chain being designated as part of critical infrastructure. (NIST, 2017).
- **ISO 31000**: ISO/IEC 27001 references ISO 31000 as a compatible approach, making it easier to implement ISO 27001 requirements and beneficial for integrating information security risk with other organisational risks (ISO, 2022; Barafort, Mesquida and Mas, 2018).

Not Chosen:

- **HITRUST CSF**: Primarily designed for healthcare organizations and HIPAA compliance (HITRUST Alliance, 2023; Alder, 2024).
- **COBIT**: While flexible, COBIT is optimized for IT governance in digital enterprises. Its complexity and IT-centric design make it less practical for traditional manufacturing environments without significant customization (De Haes et al., 2020).
- **GDPR**: Only applicable if the factory processes personal data of EU citizens. Otherwise, it does not directly impact manufacturing operations (EU, 2016).
- **CIS Controls**: Focused on technical cybersecurity controls; lacks integration with manufacturing-specific standards and operational processes.
- **FISMA/NERC CIP**: Not applicable unless involved in U.S. federal contracts or energy systems.

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

Tests and recommendations

a. International Bank

Tests

- Regulatory compliance audits against SOX, GDPR, PSD2, and PCI-DSS.
- ISO/IEC 27001 certification audit to ensure proper ISMS implementation.
- Penetration testing and red teaming to evaluate defences against cyberattacks targeting financial data.
- NIST CSF maturity assessments to measure progress against baseline controls and sector benchmarks.

Recommendations

- Establish an integrated governance framework aligning COBIT with ISO/IEC 27001 and NIST CSF(Prozorov, 2023).
- Strengthen third-party/vendor risk management programmes (aligned with ISO 31000).
- Conduct regular employee awareness training focused on phishing, social engineering, and insider threats.

b. Large Hospital

Tests

- HIPAA and HITRUST CSF readiness assessments to ensure compliance with healthcare privacy and security laws.
- ISO/IEC 27799 audits to verify patient data handling practices extend ISO 27001 into healthcare-specific processes.
- NIST CSF assessments to measure cyber resilience against ransomware and attacks on critical infrastructure.
- Disaster recovery and business continuity tests (e.g., restoring patient data from backups).
- Conduct regular employee awareness training focused on phishing, social engineering, and insider threats.
- Tabletop exercises simulating breaches of patient records or disruption to clinical systems.

Recommendations

- Adopt HITRUST CSF as the unifying compliance framework to integrate HIPAA, HITECH, GDPR, and ISO standards.
- Ensure all medical devices and IoT endpoints are included in the risk management scope.
- Establish strict access controls and multi-factor authentication for patient data systems.

- Conduct regular employee awareness training focused on phishing, social engineering, and insider threats.
- Develop a hospital-wide incident response plan and test it regularly with clinical staff included.

c. Large Food Manufacturing Factory

Tests

- ISO 9001 quality audits to ensure continuous improvement and consistent manufacturing processes.
- ISO 22000 food safety management tests (if handling food safety certification).
- ISO/IEC 27001 gap analysis and internal audits to check IT and OT (operational technology) integration.
- NIST CSF-based assessments to evaluate resilience of supply chain and critical infrastructure systems.
- Conduct regular employee awareness training focused on phishing, social engineering, and insider threats.
- Risk workshops (ISO 31000) to identify vulnerabilities in supply chain logistics and digital systems.

Recommendations

- Align ISO 9001 with ISO/IEC 27001 to integrate quality and information security into one management system.
- Secure operational technology (e.g., SCADA, IoT sensors) with network segmentation and regular patching.
- Monitor supply chain partners for cybersecurity compliance using NIST CSF.
- Conduct regular employee awareness training focused on phishing, social engineering, and insider threats.
- Establish a business continuity plan covering cyberattacks, food contamination, and supply disruptions.

References

Alder, S. (2024) ‘HIPAA vs HITRUST’, *The HIPAA Journal*. Available at: https://www.hipaajournal.com/hipaa-hitrust/ (Accessed: 26 August 2025).

Barafort, B., Mesquida, A.L. and Mas, A. (2018) ‘ISO 31000-based integrated risk management process assessment model for IT organizations’, *Journal of Software: Evolution and Process*, 31(1), e1984. Available at: https://doi.org/10.1002/smr.1984 (Accessed: 11 August 2025).

Boutin, C. (2024) NIST Releases Version 2.0 of Landmark Cybersecurity Framework. Available at: https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework (Accessed: 28 August 2025).

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations*. Springer.

EU (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, L 119, pp. 1–88. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Ewuga, S., Egieya, Z., Omotosho, A. and Adegbite, A. (2023) ‘ISO 27001 in banking: an evaluation of its implementation and effectiveness in enhancing information security’, *Finance & Accounting Research Journal*, 5(12), pp. 405–425. Available at: https://doi.org/10.51594/farj.v5i12.684 (Accessed: 28 August 2025).

HITRUST Alliance (2023) *HITRUST and HIPAA Compliance: How the HITRUST Approach Can Help Healthcare Organizations*. Available at: https://hitrustalliance.net/hubfs/Thought%20Leadership/HITRUST-and-HIPAA.pdf (Accessed 28 Aug. 2025).

ISO (2015) *ISO 9001:2015 – Quality management systems — Requirements*. 5th ed. Geneva: ISO. Available at: https://www.iso.org/standard/62085.html

ISO (2018) *ISO 22000 Food Safety Management*. Available at: https://www.iso.org/iso-22000-food-safety-management.html (Accessed: 28 August 2025).

ISO (2022) *ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements*. Geneva: International Organization for Standardization.

Kirvan, P. and Granneman, J. (2023) ‘Top 7 IT security frameworks and standards explained’, *SearchSecurity*. Available at: https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one (Accessed: 11 August 2025).

NIST (2017) ‘Financial Services Sector Specific Cybersecurity Profile’. Available at: https://www.nist.gov/system/files/documents/2017/05/18/financial_services_csf.pdf (Accessed: 28 August 2025).

Soares, B. (2023) ‘Improving Governance at a National Bank With COBIT’, ISACA, (3)2023. Available at: https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/improving-governance-at-a-national-bank-with-cobit (Accessed: 28 August 2025).

Prozorov, A. (2023) *How to integrate ISO 27001, COBIT and NIST.* Available at: https://www.linkedin.com/posts/andreyprozorov_how-to-integrate-iso-27001-cobit-and-nist-activity-7106578685121474561-vw3P (Accessed: 28 August 2025).

PwC (2016) Turnaround and transformation in cybersecurity- Key findings from The Global State of Information Security Survey 2016. Available at: https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf (Accessed: 28 August 2025).