

## Unit 5 wiki security frameworks project

Frameworks that may be applicable to the following organisations:

### International bank.

1. The International Organization for Standardization (ISO) 27001 Information Security Management System (ISMS) framework.
2. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).
3. The Payment Card Industry Data Security Standard (PCI DSS).
4. The COBIT framework for information and technology governance.
5. The Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT).

### Large hospital.

1. The Health Insurance Portability and Accountability Act (HIPAA) Security Rule.
2. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).
3. The International Organization for Standardization (ISO) 27001 Information Security Management System (ISMS) framework.
4. The COBIT framework for information and technology governance.
5. The Healthcare Information and Management Systems Society (HIMSS) Cybersecurity Framework
6. IEC 62443 standards for the industrial automation and control systems (IACS) sector

### Large food manufacturing factory.

1. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).
2. The COBIT framework for information and technology governance.
3. The Food Safety Modernization Act (FSMA) Preventive Controls for Human Food rule.
4. IEC 62443 standards for the industrial automation and control systems (IACS) sector

### Summary of three industries.

Tests and recommendations that I would make to the owners/managers for each of the businesses to help them use the frameworks and comply with industry standards.

#### International bank

To help an international bank use security frameworks and comply with industry standards, I would recommend conducting a thorough risk assessment to identify potential vulnerabilities and areas for improvement. Based on the findings of the risk assessment, I would recommend implementing appropriate security measures, such as implementing strong access controls and regularly backing up data. I would also suggest regularly testing and monitoring the effectiveness of these measures, and seeking certification or compliance with relevant industry standards, such as ISO 27001 and PCI DSS, to demonstrate the bank's commitment to security and best practices.

#### References

ISO (2022) ISO 27001 Information security management systems. Available from: <https://www.iso.org/isoiec-27001-information-security.html> [Accessed on 08 December 2022].

PCI\_DSS (2022) The PCI Security Standards Council. Available from: <https://www.pcisecuritystandards.org/> [Accessed on 09 December 2022].

#### Large Hospital

I would recommend implementing appropriate security measures based on the findings of the risk assessment, and regularly testing and monitoring the effectiveness of these measures. Additionally, I would suggest seeking certification or compliance with relevant industry standards, such as HIPAA and ISO 27001, to demonstrate the hospital's commitment to security and best practices while ensuring GDPR is enforced if compliance and regulation requires (Location and patient dependent)

#### References

HIPPA (2022) Health Insurance Portability and Accountability Act of 1996. Available from: <https://www.hhs.gov/hipaa/index.html> [Accessed on 07 December 2022].

ISO (2022) ISO 27001 Information security management systems. Available from: <https://www.iso.org/isoiec-27001-information-security.html> [Accessed on 08 December 2022].

### Large food manufacturing factory

To help a large food manufacturing factory use security frameworks and comply with industry standards, I would recommend conducting a thorough risk assessment to identify potential vulnerabilities and areas for improvement. I would then recommend implementing appropriate security measures based on the findings of the risk assessment, and regularly testing and monitoring the effectiveness of these measures. Additionally, I would suggest seeking certification or compliance with relevant industry standards, such as ISO 22000, ISO 27001 and FSMA, to demonstrate the factory's commitment to food safety and quality.

### References

FSMA (2022) Rules and Guidance for Industry related to the FDA Food Safety Modernization Act. Available from:

<https://www.fda.gov/food/food-safety-modernization-act-fsma/fsma-rules-guidance-industry> [Accessed on 09 December 2022].

ISO (2022) ISO 22000 Food safety management. Available from:

<https://www.iso.org/iso-22000-food-safety-management.html> [Accessed on 08 December 2022].

ISO (2022) ISO 27001 Information security management systems. Available from:

<https://www.iso.org/isoiec-27001-information-security.html> [Accessed on 08 December 2022].