Table of Contents

[Section 1: Frequently Asked Questions (FAQ) 1](#_Toc145936799)

[Section 2: Responses to Questions 2](#_Toc145936800)

[Q1. Which of the frameworks do you think would be applicable to the following organisations: 2](#_Toc145936801)

[A. International Bank 2](#_Toc145936802)

[B. Large Hospital 2](#_Toc145936803)

[C. Large Food Manufacturing Factory 2](#_Toc145936804)

[Q2. 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. 2](#_Toc145936805)

[A. International Bank 2](#_Toc145936806)

[B. Large Hospital 2](#_Toc145936807)

[C. Large Food Manufacturing Factory 2](#_Toc145936808)

# Section 1: Frequently Asked Questions (FAQ)

**Q1:** What's the key difference between the framework by Kirvan (2021) and Barafort et al. (2018)?

**Answer:** The key difference is in the focus areas and applications. Kirvan's framework is more suited for organizations that need a tailored approach to intricate regulatory and compliance needs. Barafort et al. focus on integration and adaptability of various ISO standards, making it versatile for different sectors.

**Q2:** How frequently should organizations review their compliance with these frameworks?

**Answer:** A periodic review is essential; most organizations opt for an annual review. However, high-risk industries like healthcare and banking may require more frequent assessments.

**Q3:** Can Barafort et al.'s framework be applied to smaller organizations or start-ups?

**Answer:** Yes, the framework is scalable and can be adapted to smaller organizations. However, due to its comprehensive nature, it might require a dedicated team for implementation and management.

**Q4:** How does Kirvan's framework specifically cater to financial institutions?

**Answer:** Although the specific details of Kirvan's framework were not provided, financial institutions often require specialized protocols for risk management, focusing on cyber-security, regulatory compliance, and data protection. Such frameworks often align closely with these specialized needs.

**Q5:** Are there any industry-specific standards that should be considered along with the general ISO standards in Barafort et al.'s framework?

**Answer:** Absolutely, depending on the industry, you might need to consider additional standards. For example, healthcare providers should also investigate HIPAA compliance in the U.S. or GDPR compliance in Europe.

# Section 2: Responses to Questions

# Q1. Which of the frameworks do you think would be applicable to the following organisations:

## A. International Bank

**Kirvan's 2021 Framework**: Given the sensitive nature of financial data and stringent regulatory requirements, a specialized framework like Kirvan's would be highly applicable.

**Barafort et al. 2018 Framework**: Also, applicable due to its strong focus on ISO standards which are globally recognized and often required in banking.

## B. Large Hospital

**Kirvan's 2021 Framework**: May not be as directly applicable given that it seems to cater more to financial and corporate governance.

**Barafort et al. 2018 Framework**: More suitable due to its adaptability and coverage of various ISO standards, including those relevant to healthcare.

## C. Large Food Manufacturing Factory

Kirvan's 2021 Framework: Less applicable as it seems more tailored to service sectors.

Barafort et al. 2018 Framework: Highly applicable due to its focus on ISO standards, including those that pertain to quality management and food safety.

# Q2. 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.

## A. International Bank

**Tests:** Regular penetration tests, compliance audits against applicable ISO standards, and financial audits.

**Recommendations:** Implement stringent data protection protocols and multi-factor authentication.

## B. Large Hospital

**Tests:** Regular HIPAA or equivalent audits, penetration tests for patient data security, and medical equipment safety checks.

**Recommendations:** Adopt a comprehensive risk management system and ensure all healthcare-related ISO standards are met.

## C. Large Food Manufacturing Factory

**Tests:** Regular food safety tests, ISO compliance checks, and machinery safety audits.

**Recommendations:** Develop a food safety management system in line with ISO standards and perform regular quality audits.

# References

1. Barafort, B., Mesquida, A. and Mas, A., 2018. ISO 31000-based integrated risk management process assessment model for IT organizations. Journal of Software: Evolution and Process, 31, e1984. doi:10.1002/smr.1984.