

# COMPARING THE ISO 27005:2022 & NIST SP 800-30 FRAMEWORKS

**Jordan Patterson 2024**

# Introduction

- ISO 27005:2022 is an international standard focused on information security risk management, providing organizations with a systematic approach to identify, assess, and manage information security risks.
- NIST SP 800-30 is a risk management guide published by the National Institute of Standards and Technology (NIST) in the United States, specifically targeting information technology systems. This framework is designed to help organizations identify, assess, and manage IT risks, ensuring the security of their systems.





# Scope and Applicability

## **ISO 27005:2022**

- Applicable to all types of organizations.
- Covers technology, people, and processes in risk assessment.
- Geared towards higher-level management practices.

## **NIST SP 800-30**

- Primarily focused on technology-related risk assessment.
- Most suited for US federal government agencies but can be applied to other organizations.

# Methodology and Approach

## **ISO 27005:2022**

- Flexible framework, customizable
- Process: context establishment, risk identification, analysis, evaluation, treatment
- Event-based and asset-based approaches

## **NIST SP 800-30**

- Structured, detailed methodology
- Process: preparation, assessment, communication, maintenance
- Techniques: questionnaires, interviews, document reviews



# **Risk Assessment Process**

## **ISO 27005:2022**

- Cyclical, continuous improvement
- Detailed documentation, ISO 27002 controls

## **NIST SP 800-30**

- Linear process, specific steps
- Security Requirements Checklists
- Detailed guidance on risk controls

# Risk Treatment

## **ISO 27005:2022**

- Four options: modification, retention, avoidance, sharing
- Refer to ISO 27001 for controls

## **NIST SP 800-30**

- Focus on risk mitigation strategies
- Detailed steps for control implementation



# Integration and Documentation

## **ISO 27005:2022**

- Integrates with ISO standards, especially ISO 27001
- Comprehensive documentation, ISO 27002 controls

## **NIST SP 800-30**

- Part of NIST SP 800 series
- Emphasizes detailed documentation and checklists

# From a Business Perspective

## ISO 27005:2022

### Pros:

- **Flexibility:** Tailorable framework for small businesses.
- **Comprehensive Scope:** Covers technology, people, and processes.
- **Integration with Other ISO Standards:** Seamless integration with ISO 27001 and others.

### Cons:

- **Complexity:** Can be overwhelming for small businesses with limited resources.
- **Implementation Cost:** High costs may not be feasible for all small businesses.

## NIST SP 800-30

### Pros:

- **Structured Methodology:** Easy-to-follow, detailed approach.
- **Focus on Technology Risks:** Relevant for tech-dependent small businesses.
- **Cost-Effective:** Practical and budget-friendly.
- **Readily Available Resources:** Extensive documentation and tools available.

### Cons:

- **US-Centric:** Primarily designed for US federal agencies.
- **Less Flexibility:** Less adaptable compared to ISO 27005:2022.



# Cost Comparison:

## ISO 27005:2022 vs. NIST SP 800-30

### ISO 27005:2022

- **Initial Assessment Costs:** Evaluation of current practices.
- **Consulting Fees:** External consultant assistance.
- **Training Costs:** Staff training on ISO 27005:2022.
- **Internal Resource Costs:** Internal staff time and effort.
- **Audit Fees:** Third-party certification audits.
- **Implementation Costs:** Changes to processes and systems.
- **Total Estimated Cost:** \$25,000 to \$100,000+ USD

### NIST SP 800-30

- **Initial Assessment Costs:** Initial risk assessment.
- **Consulting Fees:** External consultant assistance.
- **Training Costs:** Staff training on NIST SP 800-30.
- **Internal Resource Costs:** Internal staff time and effort.
- **Implementation Costs:** Changes to processes and systems.
- **Total Estimated Cost:** \$20,000 to \$75,000 USD

### Key Differences in Costs:

1. **Certification Audit Fees:** Required for ISO 27005:2022, not for NIST SP 800-30.
2. **Overall Cost Range:** ISO 27005:2022 is generally more expensive due to certification.



## Conclusion

When comparing ISO 27005:2022 and NIST SP 800-30 for information security risk management:

- **ISO 27005:2022:** Flexible and comprehensive, integrates with other ISO standards, suitable for diverse organizations, higher cost (\$25,000 to \$100,000+ USD).
- **NIST SP 800-30:** Structured and detailed, focused on technology risks, cost-effective (\$20,000 to \$75,000 USD), suitable for US-based organizations and small businesses.