

# ISO 27001:2022 Overview Outline

1. Explain the layout of the standard is identical to other management system standards (except ISO 13485: 2016) in a Clause 1-10 structure and naming convention. Add Slide 1 Review

**LESSON LEARNED:  
YOU NEED ISMS CONTROLS**

**Company 1:**  
had no control points - the “bad actors” were able to test the integrity of their information system and learned no ISO 27001 control points were in place.

**Company 2:**  
had the control points and implementation of the ISO 27001 ISMS - training, testing, improvement reviews, and countermeasures.

**PERRY JOHNSON  
CONSULTING, INC.**

December 2023 • Page 5

2. Introduction covers Sections 1-3: Informative and Non auditable
  - a) Scope Highlight: Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.
  - b) References: ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*
  - c) Terms and definitions: ISO Online browsing platform: available at [https:// www .iso .org/ obp](https://www.iso.org/obp) and IEC Electropedia: available at [https:// www .electropedia .org/](https://www.electropedia.org/)
3. Auditable sections: Clauses 4-10 in a Plan-Do-Check-Act progression
  - a) Plan (Clauses 4-7)
  - b) Do (Clause 8)
  - c) Check (Clause 9)
  - d) Act (Clause 10)
4. Clause 4 Context of the Organization
  - a) Understand your internal and external needs issue referencing Clause 5.4.1 of ISO 31000:2018
  - b) Interested parties
  - c) Scope and boundaries
  - d) Information security management system (ISMS) implementation

# ISO 27001:2022 Overview Outline

## 5. Clause 5 Leadership

- a) Commitment all the way to the top of the organization
- b) ISMS policy
- c) Roles, responsibilities and authorities

## 6. Clause 6 Planning (most significant and comprehensive clause of the entire standard)- see Slide 2

- a) Addressing risks and opportunities
- b) Information security risk assessment
- c) Information security risk treatment per 93 controls in the standard's [Annex A](#) in addition to a Statement of Applicability (if you exempt any controls as non-applicable, a justification for excluding them is required)
- d) Information security objectives
- e) Planning of changes

### Slide 2

**THREATS: REAL CASE SCENARIOS**

Information Security Management System (ISMS)- your control of theft and ransomware attacks

The tale of two companies:

**Company 1: Small family-owned business with limited Information Systems control**

- Ransomware attack at worst moment- “end of month” shipments/invoices
- Later reactive measures indicated several days of subtle surveillance
- Paid the ransom because company could not access ERP and do business

**Company 2: Recently certified ISO 27001 company with an ISMS**

- Ransomware attack detected on a weekend- control points implemented
- Full blown malware ransom attack by the following Monday
- Because of early warning, IT Department with support of outside process established an independent cloud-based server outside of their attacked platform
- Retrieved 90% of encrypted data- no ransom paid

 PERRY JOHNSON  
CONSULTING, INC.

December 2023 • Page 4

# ISO 27001:2022 Overview Outline


7. Clause 7 (similar to other management systems)
  - a) Resources
  - b) Competence
  - c) Awareness
  - d) Communication
  - e) Documented information
8. Clause 8 Operations (playing off Clause 6 ISMS risk assessment and risk treatment)
  - a) Operational planning and control implementing actions determined in Clause 6
  - b) Information security risk assessment per Clause 6 planning
  - c) Information security risk treatment- implement the 93 controls in the standard's [Annex A](#)
9. Clause 9 Performance evaluation (similar to other management systems)
  - a) Monitoring, measurement, analysis and evaluation
  - b) Internal audit
  - c) Management review
10. Improvement (similar to other management systems)- see Slide 3
  - a) Continual improvement
  - b) Nonconformity and corrective action

Slide 3

**LESSON LEARNED:  
YOU NEED ISMS CONTROLS**

**Company 1:**  
had no control points - the “bad actors” were able to test the integrity of their information system and learned no ISO 27001 control points were in place.

**Company 2:**  
had the control points and implementation of the ISO 27001 ISMS - training, testing, improvement reviews, and countermeasures.

 PERRY JOHNSON  
CONSULTING, INC.

December 2023 • Page 5