

# ISMS: A reality or a paper tiger?

Overview to ISO/IEC 27001: 2022

21 November 2024



Jatin Sehgal

Global Leader & Managing Partner | EY CertifyPoint

[Jatin.Sehgal@nl.ey.com](mailto:Jatin.Sehgal@nl.ey.com)

+31629084825



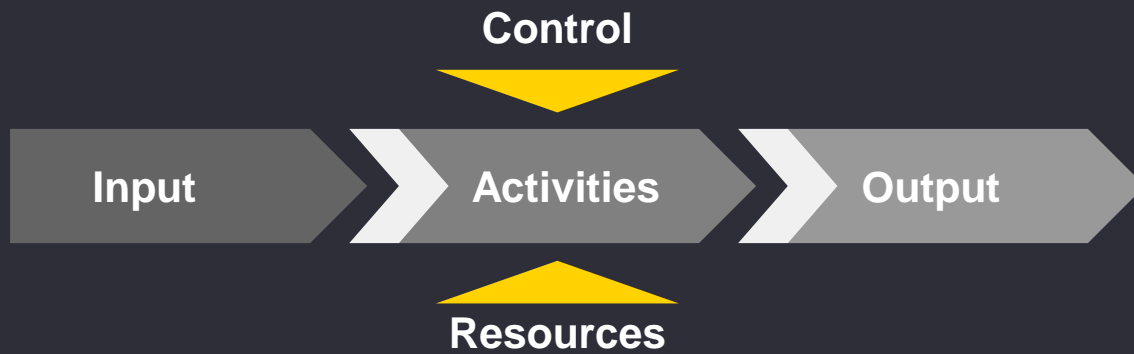
1. Scope
2. Normative references
3. Terms and definitions

4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement



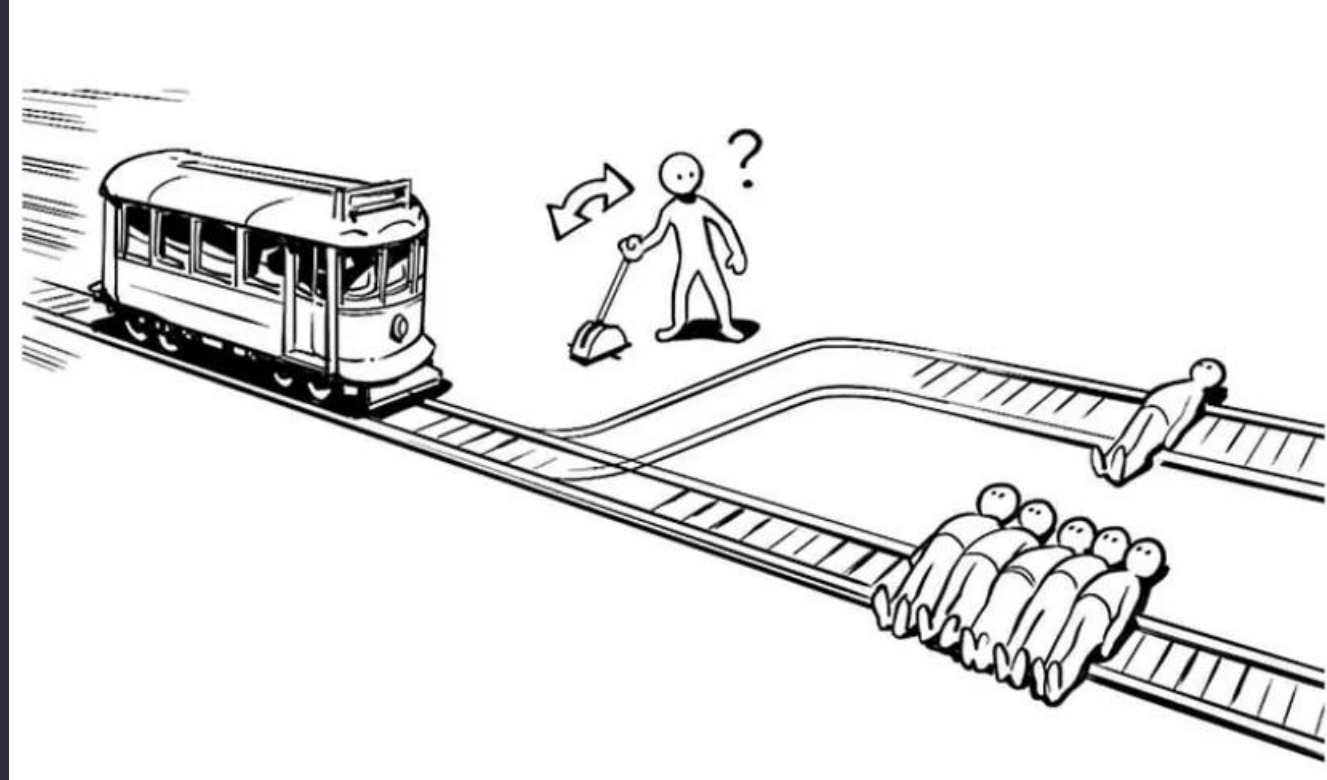
Annex A (normative) Reference control objectives and controls

Selection of Annex A Controls



# The Trolley Dilemma?

---



# Unlocking the full potential of ISO/IEC 27001: 2022

ISO/IEC 27001 is not just a compliance check box; it's a strategic asset.



OPTION 2

OPTION 1



1

Organisation NOT CERTIFIED with ISO/IEC 27001: 2022



2

Organisation CERTIFIED with ISO/IEC 27001: 2022

1

Enhances overall organizational security procedure

5

Proactively identifies & mitigates security risks

2

Builds customer and stakeholder trust

6

Provides a competitive advantage in the market

3

Helps organizations meet regulatory and legal requirements

7

Enhances ability to detect and respond to security incidents

4

Streamlines security processes and improves efficiency

8

Promotes security awareness and responsibility among staff

# Top Drivers Currently

---



## Geo-political Context:

- Increased cyber threats
  - Regulatory Compliance
  - Supply Chain Security
- 



## Looming Recession:

- helps organizations prioritize critical security measures even during budget cuts
  - Insider threats
  - Operational Continuity
- 



## AI Awareness:

- AI security Risks
- Data Privacy
- Training & Awareness

# Key Challenges Organizations face

## Challenges

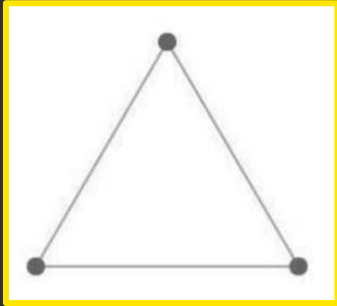
1. **ISMS may not address actual demands effectively** because of lack of understanding of the business
2. **Misaligned decisions and hindered alignment** with ISMS objectives are **caused by unclear or undocumented processes.**
3. Unclear accountability because of complex communication networks
4. **Overestimating an ISMS's capabilities** leads to poorly executed risk assessments -> **Failure to capture vulnerabilities**



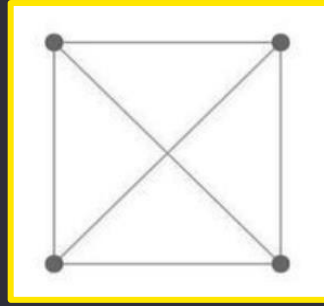
## Indicators

1. **A paper tiger exercise** for compliance instead of understanding how ISO/IEC 27001: 2022 is implemented.
2. **Lack of linkages** because of various actions taken.
3. Incomplete records for decision taken for key ISMS tasks.
4. The lack of documentation and inability of the organization to showcase key evidences.

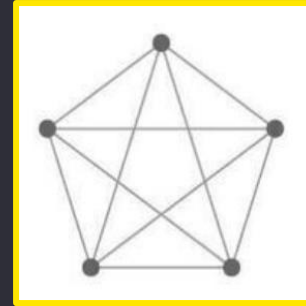
# Complexity of Communication Lines



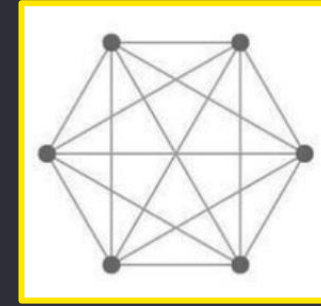
3 People, 3 lines



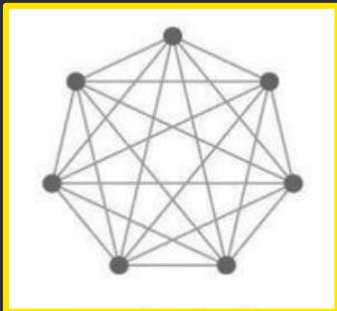
4 People, 6 lines



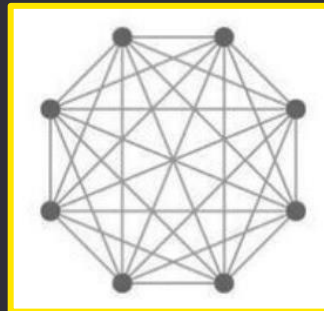
5 People, 10 lines



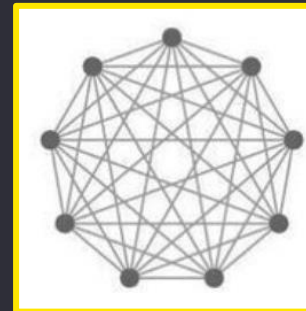
6 People, 15 lines



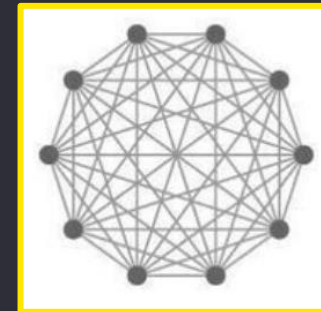
7 People, 21 lines



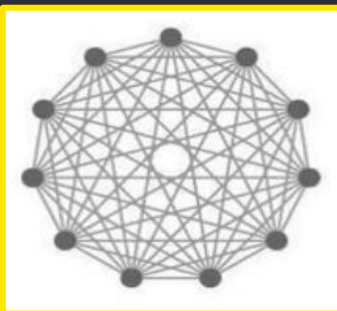
8 People, 28 lines



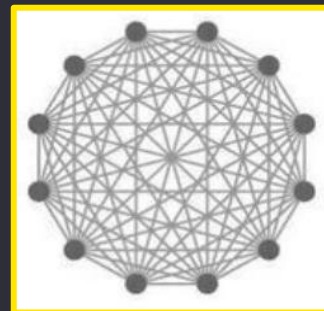
9 People, 36 lines



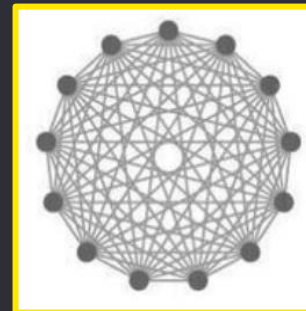
10 People, 45 lines



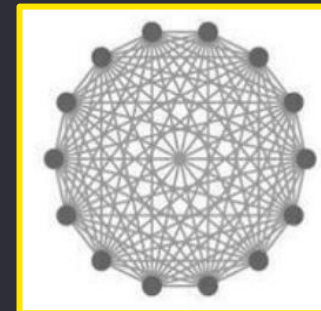
11 People, 55 lines



12 People, 66 lines



13 People, 78 lines



14 People, 91 lines

# Common Audit Findings: EYCP's auditors experience



Opportunity for improvement



Minor nonconformity



Major Nonconformity



Addressing these findings strengthen ISMS effectiveness and ensures certification success.



# Is ISMS a reality or a paper tiger?

## Strengths

- ▶ Provides a structured approach to protecting information assets
- ▶ Robust controls ensure effective risk assessment
- ▶ Promotes continuous improvement through regular maintenance and updates.

## Challenges

- ▶ Certification may be pursued as a checkbox exercise rather than real security
- ▶ Some auditors lack the expertise to assess the effectiveness of controls
- ▶ Blindly trusting certification can lead clients to rely on security measures that merely check boxes

A robust ISMS and ISO/IEC 27001 Certification form the cornerstone of an effective, multi-layered defense strategy.

- ▶ ISO/IEC 27001 is not a paper tiger, but its success depends on:



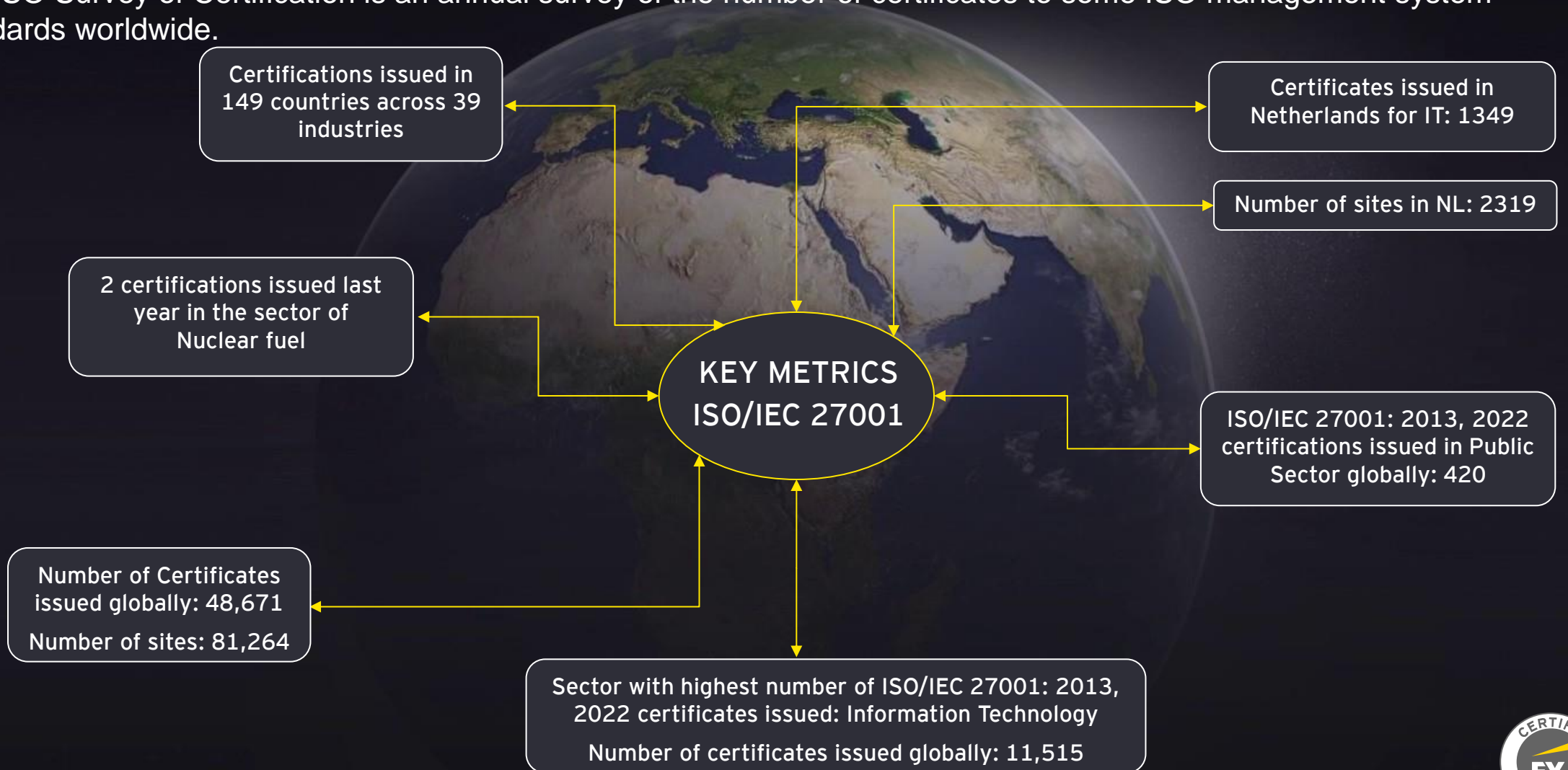
# ISO/IEC 27001: 2022 Certification

How to read an ISO Certificate



# ISO/IEC 27001:2013, 2022 Global Survey Results


The ISO Survey of Certification is an annual survey of the number of certificates to some ISO management system standards worldwide.



**ISMS: A reality or a paper tiger?**

**It Depends how you implement it**





**EY | Building a better working world**

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](https://ey.com/privacy). EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit [ey.com](https://ey.com).

[ey.com](https://ey.com)