How to make the transition from 2013 to 2022 revision of ISO 27001

Presenter:
Dejan Kosutic

Hosted by
Perry Johnson Registrars, Inc.

Advisera

Transition deadline is October 2025

For security officers, project managers

You’ll get a clear idea on how to proceed with the transition

Advisera

The transition effort will be 10% of your implementation effort if you plan for it carefully

Advisera

Agenda

- Main steps in the transition
- Documenting the transition
- How to merge controls?
- What will the certification auditor look for?
- Q&A

Main steps in the transition

Risk treatment → new control IDs

Statement of Applicability → new controls

Document new controls

Update references to controls

Advisera

Risk treatment – new controls and control IDs

Asset	Vulnerability	Threat	Old control	New control
Database	Lack of backup	Loss of data	A.12.3.1 Information backup	A.8.13 Information backup
Laptops	No rules for teleworking	Theft	A.11.2.6 Security of equipment and assets off-premises	A.7.9 Security of assets off-premises
E-commerce software	No rules on how to handle encryption	Compromising financial transactions	A.10.1.1 Policy on the use of cryptographic controls	A.8.24 Use of cryptography
E-commerce software	Encryption keys not adequately protected	Compromising financial transactions	A.10.1.2 Key management	A.8.24 Use of cryptography
Data center	Lack of monitoring of physical activities	Unauthorized activities	-	A.7.4 Physical security monitoring

Documenting the transition

Document examples:

- Risk Treatment Table
- Statement of Applicability
- Documenting new controls
- Updating references to controls

What to do with old 2013 documents and records?

- Documentation – use revisioning
- Example:
  - Access Control Policy ver. 3.2 (compliant with 2013 revision)
  - Access Control Policy ver. 4.0 (compliant with 2022 revision)
- Records – refer to valid controls at the moment of creation
- Example:
  - Backup logs were previously related to A.12.3.1
  - Now backup logs are related to A.8.13

How to merge controls

2013 revision:

- A.12.4.1 Event logging
- A.12.4.2 Protection of log information
- A.12.4.3 Administrator and operator logs

2022 revision:

- A.8.15 Logging

What will the certification auditor do?

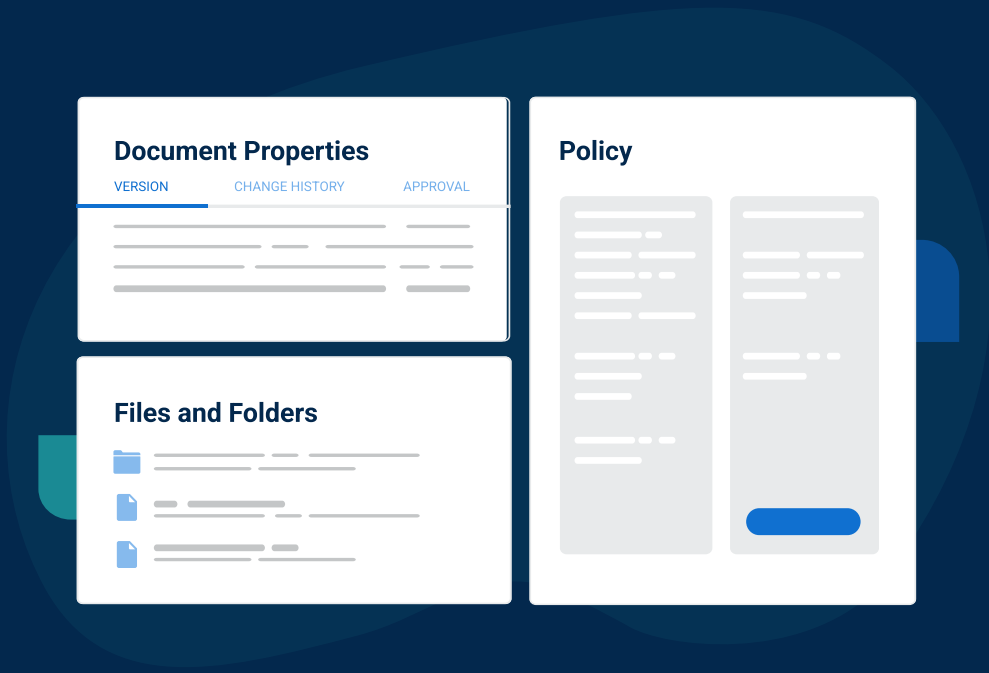
- During the surveillance audit or recertification audit
- Latest by October 2025
- The auditor will check all 4 things:
  - Risk treatment
  - SoA
  - Documenting new controls
  - Updates of existing documents

Conclusion

ISO 27001 changed only moderately – transition effort will also be moderate if approached systematically

ISO 27001 2022 Transition Toolkit

https://advisera.co/Transition-toolkit-27001



Advisera

Q&A

Advisera

Thank You