Navigating ISO/IEC 27001: Internal audits and management review

Presenter:
Dejan Kosutic

Hosted by
Perry Johnson Registrars, Inc.

Advisera

Internal audit and management review are a “health check” before the certification audit

Advisera

Agenda

- Last steps in ISO 27001 implementation
- Internal audit purpose and documents
- Internal audit process
- Example of internal audit checklist
- Management review purpose and documents
- Inputs for management review
- Outputs from management review

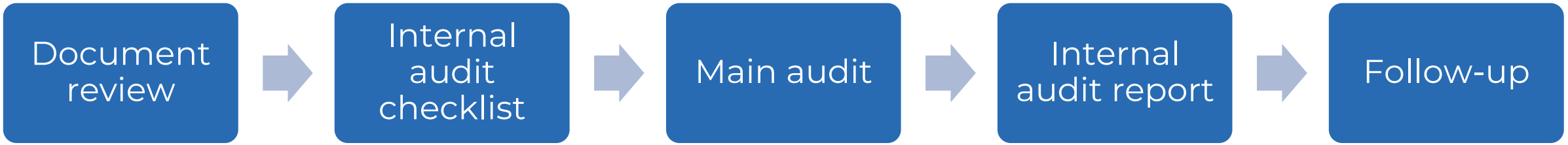
Last steps in ISO 27001 implementation

Advisera

Internal audit purpose and documents

- Purpose
- Mandatory documents
  - Internal audit program
  - Internal audit report
- Optional documents
  - Internal audit procedure
  - Internal audit plan
  - Internal audit checklist

Internal audit process



Advisera

Example of internal audit checklist

Clause	Requirement of the standard	Compliant Yes/No	Evidence
4.2	Did the organization determine interested parties?		
4.2	Does the list of all of interested parties' requirements exist?		
4.3	Is the scope documented with clearly defined boundaries and interfaces?		
5.1	Are the general ISMS objectives compatible with the strategic direction?		
5.1	Does management ensure that ISMS achieves its		

Management review purpose and documents

- Purpose
- (non-mandatory) Management review procedure
- (mandatory) Management review minutes

Inputs for management review

- Status from previous management review
- Changes in internal and external issues
- Feedback and trends on security performance
- Feedback from stakeholders
- Risk assessment, Risk treatment plan
- Continual improvement

Outputs from management review

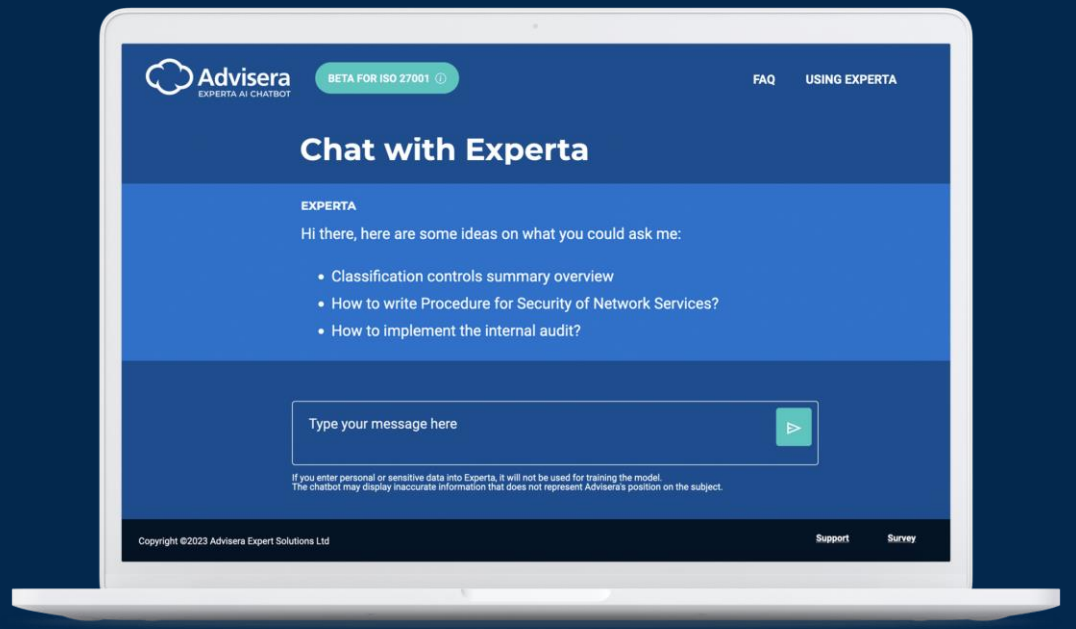
- Decisions about continual improvement
- Decisions about changes to the ISMS

Conclusion

Internal audit and management review are perfect “tools” to prepare for certification audit

Experta: AI-Powered ISO Knowledge Base

https://advisera.co/experta



Advisera

Q&A

Dejan
Kosutic

Advisera

Thank You

https://advisera.co/experta

Advisera