

How to Integrate ISO 27001 and ISO 42001?



Presenter:
Dejan Kosutic



Many ISO 27001-certified companies are now considering ISO 42001

How to integrate AIMS into an existing ISMS

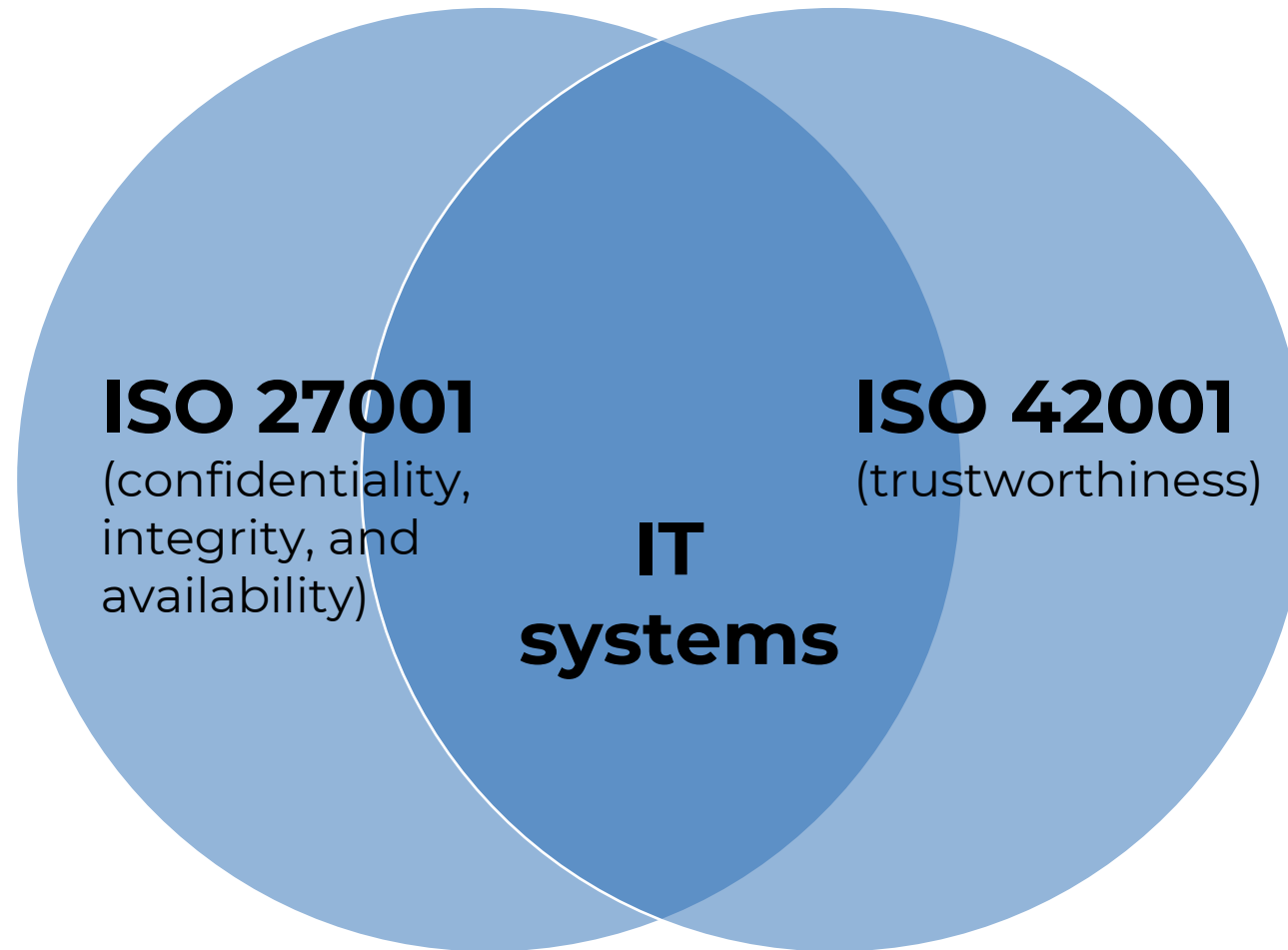
If you're in charge of ISO 27001 or ISO 42001 implementation

Despite strong similarities between ISO 27001 and 42001, some key elements must be handled separately

Agenda

- Why is ISO 42001 useful for ISO 27001?
- Similarities & differences between ISO 27001 and 42001
- Implementation process
- Roles
- Top management issues

ISO 27001 vs ISO 42001 purpose and scope



Why is ISO 42001 useful for ISO 27001?



- ISO 27001 wasn't designed with AI in mind
- AI is very often the source of security threats
- IT governance becomes much harder because of AI usage

Things that are the same



- PDCA Cycle
- Document control
- Internal audits
- Management review
- Corrective actions

Similar concepts



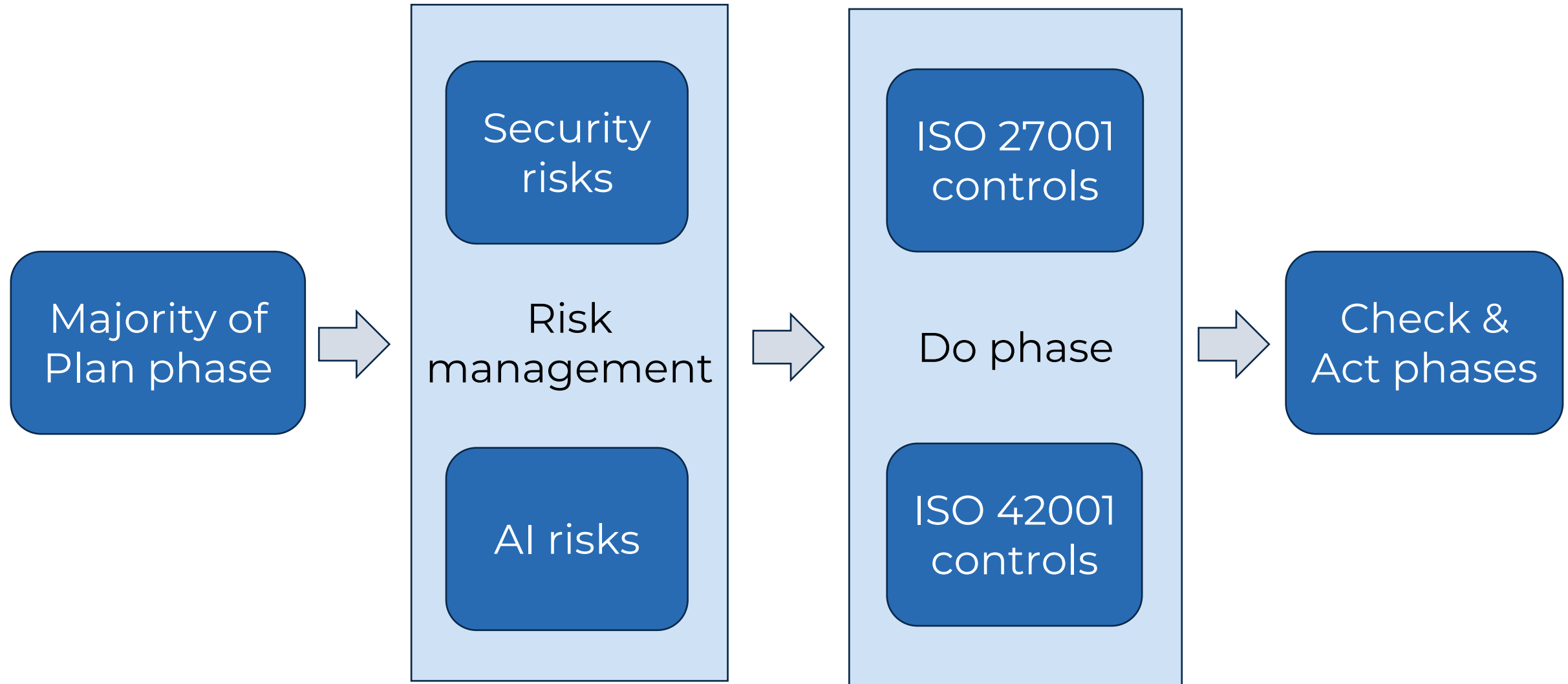
- Top-level policy
- The process of risk assessment and treatment
- Statement of Applicability
- Risk treatment plan
- Annex A purpose
- ISO 42001 Annex B purpose
- Training & awareness
- Setting the objectives and measuring

Differences



- Risk assessment
- Controls
- ISO 42001 AI system impact assessment

Implementation process



Roles

- Security officer / AI officer
- Project team
- Security / AI / IT committees
- Senior management / sponsor

Senior management perspective



- If ISO 27001 is already implemented, they will understand the benefits of ISO 42001 easier
- Management review for ISMS and AIMS can be done at the same time
- Setting objectives and measurement can be done at the same time
- Audits can be done at the same time

Biggest challenges with integration



- Shadow IT and Shadow AI
- Risk assessment and risk register
- Bring both standards together without creating duplicate processes or documentation
- Is the AI being governed responsibly and appropriately for its intended purpose?
- AI lifecycle integration process, do I need a manual?

Conclusion

Adding AIMS on top of ISMS will be relatively easy if you separate risk management

Advisera Courses

<https://advisera.co/Trainings-Advisera>





Q&A



**Dejan
Kosutic**



Thank You

<https://advisera.co/Trainings-Advisera>

