



AI Risk & Security Alignment Checklist that integrates ISO 42001 and ISO 27001. It's structured for clarity, impact, and practical use

AI Risk & Security Alignment Checklist

How ISO 42001 and ISO 27001 Work Together in Practice

As organizations deploy AI systems, aligning AI governance (ISO 42001) with information security (ISO 27001) is essential. This checklist helps compliance teams, risk managers, and IT leaders ensure that AI risks are addressed within a secure, auditable framework.

Governance & Leadership

Task	ISO 42001 Reference	ISO 27001 Reference
Define AI governance roles and responsibilities	Clause 5.3	Clause 5.3
Align leadership accountability across AI and ISMS	Clause 5.3	Clause 5.3
Establish cross-functional oversight	Clause 5.3	Clause 5.3

Risk Assessment & Treatment

Task	ISO 42001 Reference	ISO 27001 Reference
Conduct AI-specific risk assessments	Clause 6.1.2	Annex A.5.7, A.8.2
Integrate AI risks into ISMS methodology	Clause 6.1.2	Clause 6.1.2
Document shared risk treatment plans	Clause 6.1.2	Clause 6.1.3

Asset & Data Management

Please reach out to us at



info@deurainfosec.com



+1(707) 998 5164



Task	ISO 42001 Reference	ISO 27001 Reference
Identify AI system assets and data flows	Clause 6.1.3	Annex A.5.9, A.8.12
Apply ISMS controls to AI data	Clause 6.1.3	Annex A.8.12
Ensure traceability of training data	Clause 6.1.3	Annex A.5.10

AI System Lifecycle Controls

Task	ISO 42001 Reference	ISO 27001 Reference
Implement controls for AI design and deployment	Clause 8.1	Annex A.8.28
Apply secure development practices	Clause 8.1	Annex A.8.28
Monitor AI system behavior post-deployment	Clause 9.1	Annex A.5.25

Monitoring, Incident & Response

Task	ISO 42001 Reference	ISO 27001 Reference
Establish AI-specific monitoring	Clause 9.1	Annex A.5.25
Integrate with ISMS incident response	Clause 9.1	Annex A.5.24
Define escalation paths for AI-related events	Clause 9.1	Clause 6.1.2

Please reach out to us at



info@deurainfosec.com



+1(707) 998 5164

**Documentation & Continuous Improvement**

Task	ISO 42001 Reference	ISO 27001 Reference
Maintain AI risk logs and documentation	Clause 7.5	Clause 7.5
Align with ISMS audit trails	Clause 7.5	Clause 9.2
Review and improve AI-security alignment	Clause 10.2	Clause 10.2

Check out our earlier posts on AI-related topics: [AI topic](#)

[InfoSec services](#) | [InfoSec books](#) | [Follow our blog](#) | [DISC Ilc is listed on The vCISO Directory](#) | [ISO 27k Chat bot](#) | [Comprehensive vCISO Services](#) | [ISMS Services](#) | [Security Risk Assessment Services](#) | [Mergers and Acquisition Security](#)

<https://www.deurainfosec.com/>

Please reach out to us at



info@deurainfosec.com



+1(707) 998 5164