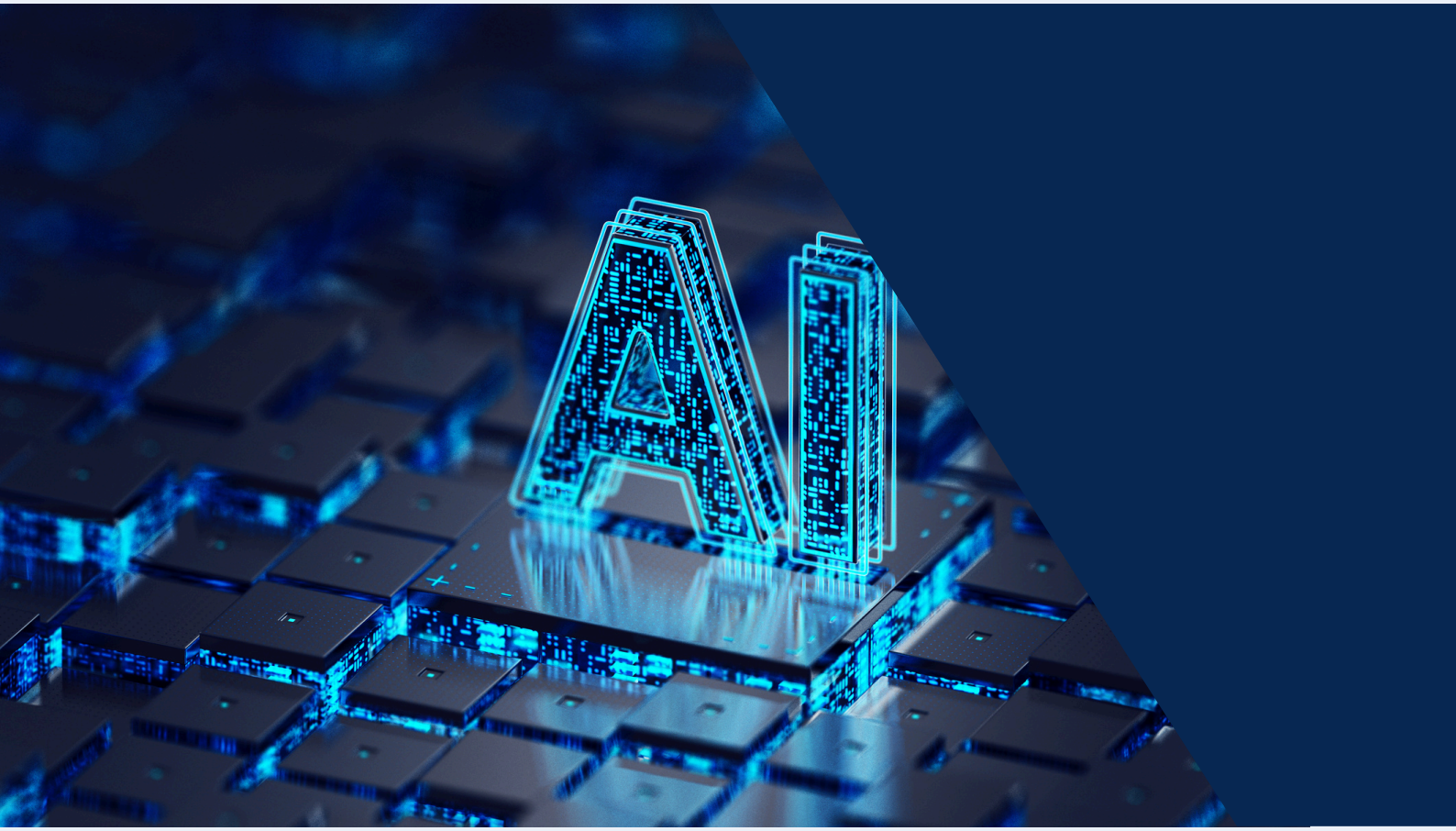
Rivedix Technology Solutions

SANTOSH KAMANE

Integrating ISO 42001(AIMS) into existing ISO 27001(ISMS)

Easy guide

Introduction



With the rise of AI in business operations, integrating Artificial Intelligence Management Systems (AIMS) into existing Information Security Management Systems (ISMS) has become both necessary and strategic.
This is especially relevant for organizations preparing for ISO/IEC 42001:2023 certification or aligning with AI-specific risk and governance frameworks.

Why integrate with ISMS ?

A

Avoid Fragmentation

Lorem ipsum dolor sit amet,
consectetur adipiscing elit.
Donec tristique laoreet urna

L

Leverage Existing Controls

Lorem ipsum dolor sit amet,
consectetur adipiscing elit.
Donec tristique laoreet urna

R

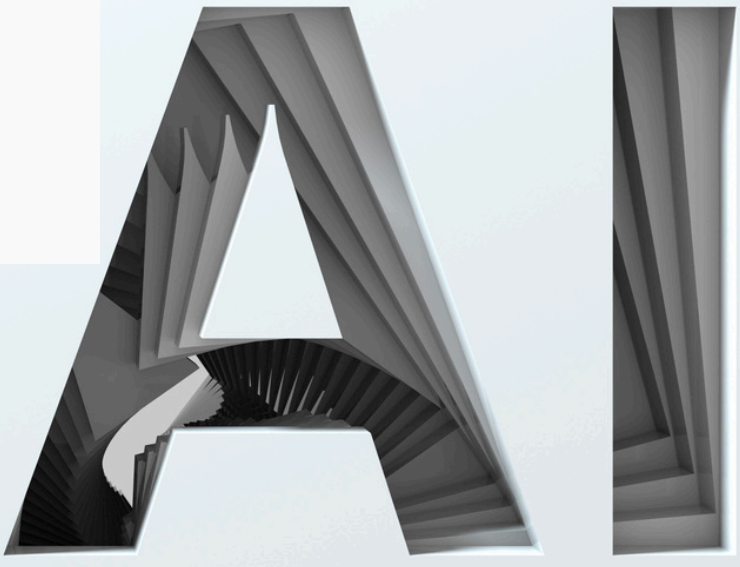
Regulatory Preparedness

Lorem ipsum dolor sit amet,
consectetur adipiscing elit.
Donec tristique laoreet urna

T

Trust & Transparency

Lorem ipsum dolor sit amet,
consectetur adipiscing elit.
Donec tristique laoreet urna



Let's get started

1 START WITH SCOPE ALIGNMENT

→ Define the scope of AIMS within the ISMS context

- Identify AI systems in use (e.g., ML models, LLMs, recommendation engines).
- Define roles, teams, and departments using or building AI.
- Map how these systems interact with existing ISMS assets (data, applications, infrastructure).

Example: If your ISMS already includes CRM and analytics systems, extend scope to include AI-based chatbots or fraud detection engines built over that data.

---

2 UPDATE RISK ASSESSMENT PROCESS

→ Include AI-specific risks in your ISMS risk register.

Model risks like:

- Bias and discrimination in AI outputs
- Model poisoning, adversarial inputs
- Shadow AI use (unauthorized LLM tools)
- Intellectual property leakage

Use ISO 42001 Annex A controls for guidance.

Tip: Use existing ISO 27005 or NIST RMF methodology and extend it with AI-specific threat vectors.

3 ENHANCE POLICIES AND PROCEDURES

→ Integrate AI governance into existing security & privacy policies.

Update:

- Acceptable Use Policy → add restrictions on use of public AI tools
- Data Classification Policy → tag training datasets
- Third-Party Risk Policy → evaluate AI vendors
- Change Management Policy → add model version control

Tip: Create an AI Governance Policy that references ISMS documents rather than duplicating them.

---

4 ESTABLISH AI-SPECIFIC ROLES WITHIN THE ISMS GOVERNANCE STRUCTURE

→ Define roles like AI Product Owner, Model Risk Manager, and Ethics Reviewer.

Extend your ISMS committee or information security council to include:

- Data scientists
- AI/ML engineers
- Legal/privacy stakeholders
- Risk/compliance leads

Tip: Create an "AI Risk Subcommittee" reporting to the ISMS steering committee.

5 INCORPORATE AI LIFECYCLE INTO ASSET & CHANGE MANAGEMENT

→ Treat AI models as assets and track their lifecycle.

- Register models in your Asset Inventory
  Define:
  - Training data lineage
  - Model purpose, accuracy, limitations
  - Version history
  - Ownership

Tip: Use your existing ISMS Change Management Process to manage AI model updates, retraining, and deprecation.

---

6 MAP ISO 42001 ANNEX A CONTROLS TO ISO 27001 ANNEX A

→ Look for overlaps to avoid duplication.

ISO 42001 Control	Overlaps with	Integration Action
A.5.2 – AI Risk Management	ISO 27001 A.6 & A.8	Extend risk register methodology
A.6.1 – AI System Development	ISO 27001 A.14 (SDLC)	Embed AI-specific checkpoints

Tip: Maintain a mapping matrix to reduce audit fatigue.

7 TRAIN & RAISE AWARENESS ON AI RISKS

→ Make AI part of your regular security awareness training.

- Add modules for:
  - Responsible AI use
  - Prompt safety and data leakage risks
  - Bias and fairness
- Include practical scenarios (e.g., "Is it okay to paste client data into ChatGPT?")

Tip: Use your existing LMS or awareness campaigns and extend content.

---

8 EXTEND INTERNAL AUDIT PROGRAM

→ Schedule AI-specific audits as part of ISMS internal audits.

- Audit:
  - AI model approval processes
  - Documentation of bias testing
  - Shadow AI discovery
  - Dataset security

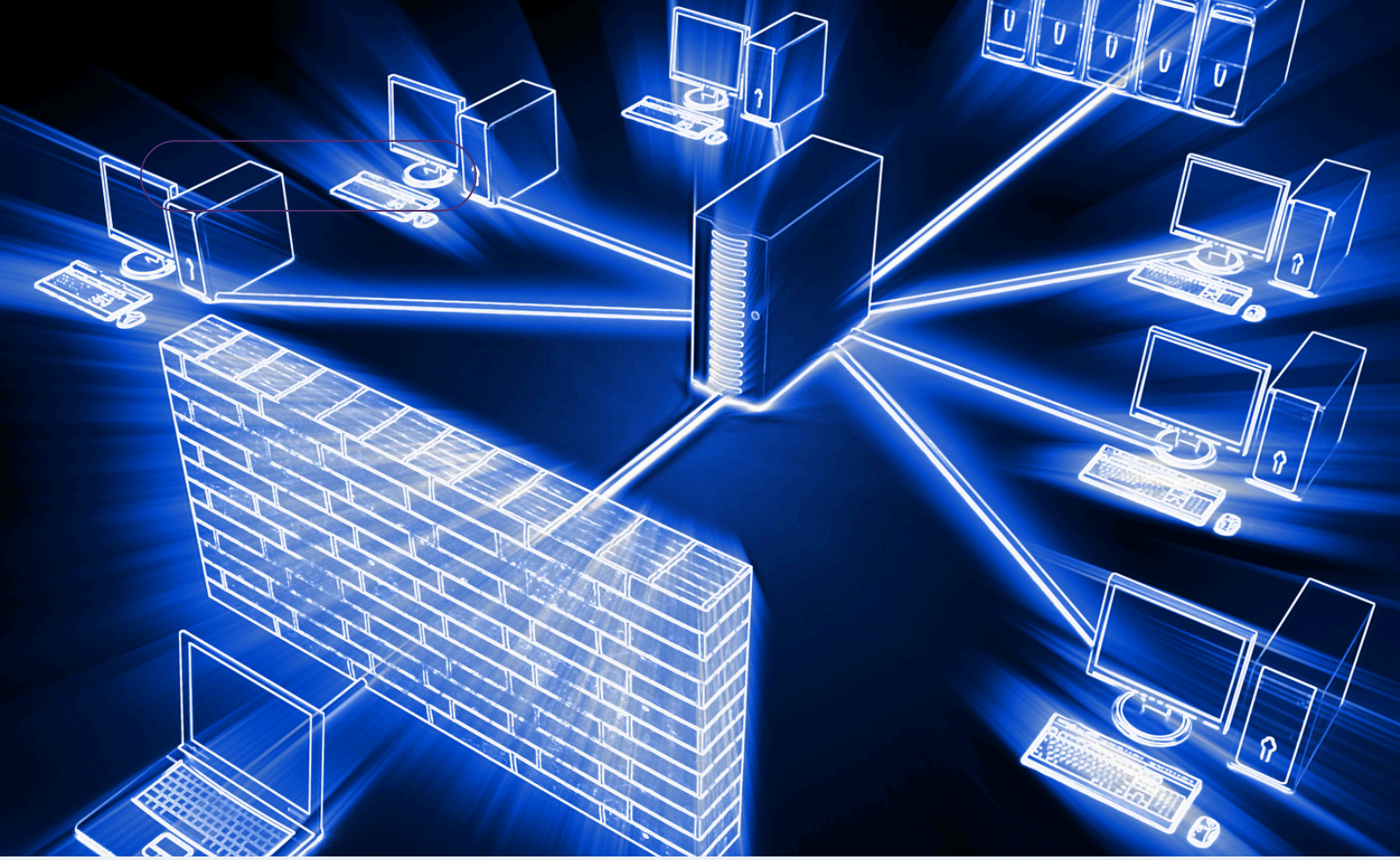
Tip: Use existing ISMS audit checklist and add AI-specific controls for each phase.

IN A NUTSHELL

By integrating AIMS into your ISMS, you're not reinventing the wheel — you're upgrading it for the AI era.
You'll ensure:

- Consistency across security, privacy, and ethics
- Efficient audits with cross-control reuse
- Stronger trust with regulators, customers, and internal stakeholders
-

This approach aligns beautifully with both ISO 27001:2022 and ISO 42001:2023, and positions your organization for future-proof, risk-aware AI adoption.



RIVEDIX SERVICES

01

Audit and Compliance
ISO 27001 / ISO 22301 / ISO 27701 /SOC2 Type 2 NIST and related compliances

02

Security testing
Penetration testing, SAST DAST, CLOUD AUDITS, Red Teaming / DevSecOps , Mobile Pen Testing

03

Data Privacy
Implementation and Audit for GDPR /CCPA / PDPA /DPDPA

04

AI Governance
ISO 42001 / EU AI Act / AI risk management, policy development

05

Identity Management and Governance
IAM / PAM / IGA · Implementation and Support