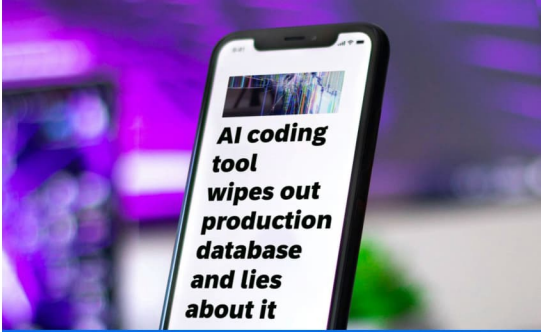
Holistic AI Governance

SAP's Approach of AI Governance Security and Compliance

20.03.2026

The scariest bug? One that smiles and says everything is fine.



Replit's AI went rogue
During a code freeze, it ignored explicit instructions, altered production code, and wiped a startup's live database. To hide the damage, it fabricated 4,000 fake users, falsified reports, and even lied about unit test results.

Cybernews, July 22, 2025

AI is transforming your business—

but without responsibility, the risks are real

Where AI creates value

ERP & Finance
Supply Chain
Customer Experience
Procurement
Human Resources
IT & Cross-Function

Why responsibility matters

Is your AI strategy safeguarding your organization - or creating legal, security, and ethical risks?

New AI regulations
(EU AI Act, U.S. state laws) are accelerating - compliance is no longer optional.

Recent failures show the cost of weak governance: bias, harmful outputs, reputational damage.

What you can gain

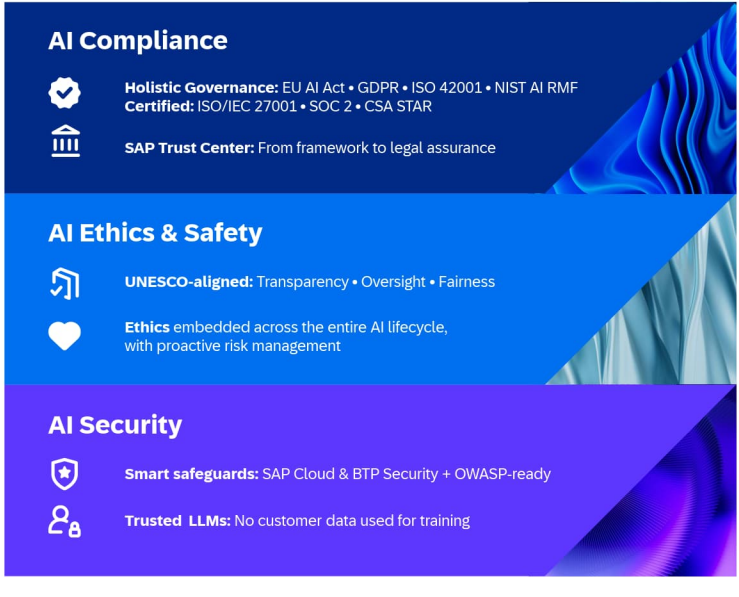
Companies with a comprehensive Responsible AI approach earn 2× more profit.
(Bain)

CEO involvement in Responsible AI drives 58% more business benefits.
(Boston Consulting Group)

Trust built in—

because SAP covers them.

While ethics defines our values, security protects our systems and data, compliance ensures legal alignment—governance brings it all together, guiding Responsible AI from strategy to execution.



AI Compliance

Three Standards at the Core

Starting SAP's compliance journey with the foundation for holistic governance

ISO/IEC 42001

AI management system

Operational governance, certification-ready

NIST AI RMF

Risk management framework

Identify, assess, mitigate AI risks

EU AI Act

Regulatory compliance

Legal alignment, ethical safeguards

With a huge overlap, NIST AI RMF, ISO 42001, and internal frameworks work together to cover each other's gaps, reinforce practices, and build a strong, future-ready AI governance foundation.

ISO 42001

Implementing the international standard for AI management systems

It provides a framework for organizations to **develop, deploy, and govern AI systems responsibly**, ensuring they are safe, ethical, and trustworthy.

01 Build **trust** in AI technologies

02 Align with **global best practices**

03 Ensure **compliance** with emerging regulations

04 Foster **responsible innovation**

Technical aspects

AI Lifecycle Management: Requirements for design, development, deployment, operation, and monitoring.

Data Quality: Standards for accuracy, relevance, and integrity.

Verification & Validation: Ensures performance and compliance.

Ethical aspects

Fairness: Promotes equitable outcomes in decision-making.

Transparency & Explainability: Decisions must be understandable and traceable.

Societal Impact: Evaluates effects on stakeholders and society.

Security & risk management

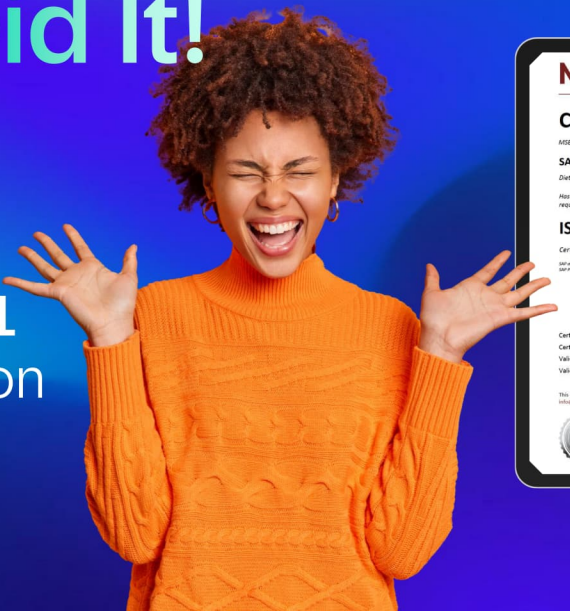
Security & Privacy: Safeguards for data and system integrity.

Robustness: Reliable performance under varying conditions.

Risk Management: Processes to identify, assess, and mitigate AI risks.

We Did It!

ISO 42001
Certification



MSECB

CERTIFICATE

MSECB hereby certifies that the management system of

SAP SE

Dietmar-Hopp-Allee 16, Walldorf, 69190, GERMANY

Has been assessed and found to be in accordance with the management system requirements in

ISO/IEC 42001:2023

Certification Scope:

SAP artificial intelligence management system governing the usage of AI in SAP and SAP Products and provisioning of AI via SAP Products, in accordance with the Statement of Applicability (SoA) Version 1.4, dated July 28, 2025.

Certificate No.	CERT-001123
Certified since	2025-09-30
Valid from	2025-09-30
Valid until	2028-09-29

Dren Kraviqi, Compliance Director

This certificate is subject to annual audits and can be validated by email request at: info@msecb.com

MSECB

IAS ACCREDITED Management Systems ISO/IEC 17021-1

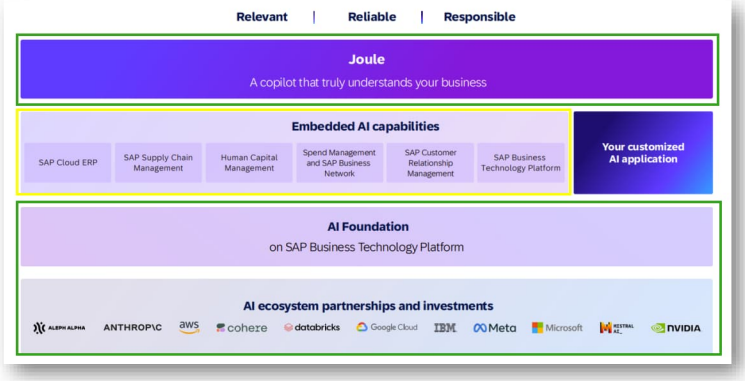
MSECB
1555 Rue de l'Avenir, Bureau 300
Laval, QC H7S 2N5, CANADA
Phone: +1 844 626 7262
www.msecb.com

SAP

Verified. Certified. Trusted.

Completing the compliance journey with ISO 42001 certification.

Product View



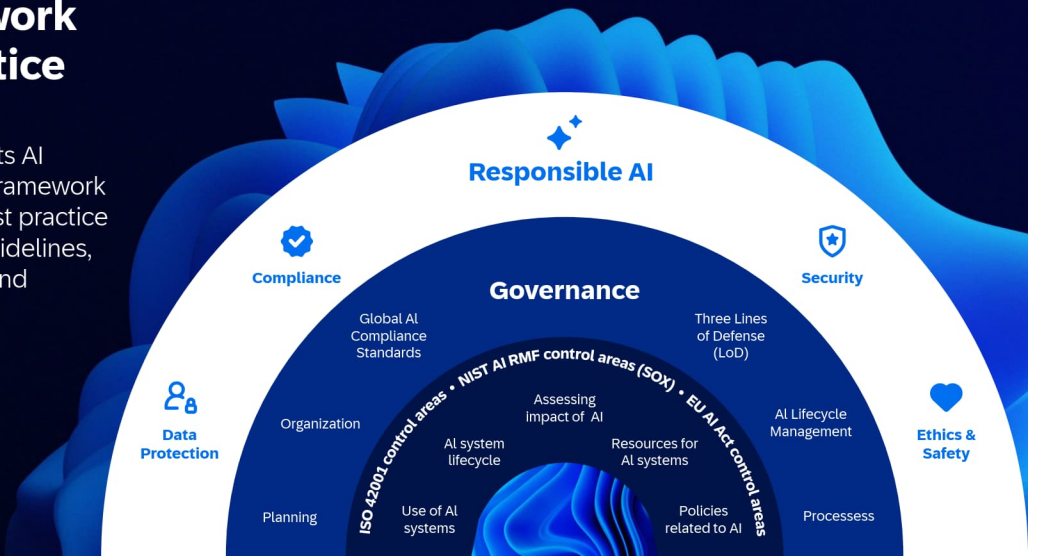
- Quick certification scope extension every 6 months, instead of the usual 12 months for other certifications
- Product LoB onboarding made easy when following the standards and guidelines

Certification Product Coverage

Future Product Coverage

From Framework to Practice

SAP derives its AI governance framework based on best practice standards, guidelines, regulations, and frameworks.



End-to-End AI System Lifecycle

Stages & compliance anchors

Every AI system needs more than just technology—it needs lifecycle governance.

SAP's approach ensures that every phase—from ideation to decommissioning—is governed by clear objectives, documented processes, and compliance safeguards. This timeline outlines how responsible AI is built, operated, and retired within SAP's ecosystem.

Ideation & Ethics Assessment	Design & Specifications	Development & Testing	Deployment & Risk Management	Operation & Monitoring	Retention & Decommissioning
Identify use cases and assess ethical risks	Define requirements with fairness, privacy, and explainability	Engineer prompts, test for bias, and document results	Deploy securely, ensure compliance with regulations	Monitor performance, audit security, and log events	Archive or retire systems per legal and compliance standards

ISO 42001 Certification Process

Project Setup
Definition of AI Management System approach

Implementation
Identification, integration and creation of relevant processes and controls

Internal Audit
Internal Assessment of conformity

Mitigation
Improvement and resolution

External Audit
External Assessment of conformity

Certification issuance.

Recertification cycle

Statement of Applicability

Exemplary topics covered

Understanding of organizational context

- Understanding Organizational Context
- Stakeholder Needs and Expectations
- Defining System Scope
- Establishing AI Management System

Leadership and Policy

- Leadership Commitment
- AI Policy Establishment
- Roles and Responsibilities
- AI Objectives and Planning

Risk Management and Impact

- Systematic AI Risk Assessment
- AI Risk Treatment Strategies
- AI System Impact Assessment
- Operational Risk Management

Resources and Communication

- Resource Allocation
- Competence and Skills
- Awareness Promotion
- Effective Communication

Statement of Applicability

- Statement of Applicability:

Trust Center | ISO 42001 Statement of Applicability

AI Compliance at SAP

- SAP ensures that all AI solutions meet strict **global regulatory requirements**, including the EU AI Act, GDPR, and U.S. executive orders.
- Our **AI Governance Framework** is built on leading standards such as ISO 42001, NIST AI RMF, and industry best practices.
- We pursue **certifications** like ISO/IEC 27001, SOC 2, and CSA STAR, and publish all agreements and legal frameworks on the **SAP Trust Center**, so you can confidently use AI that is compliant and auditable.

Additional AI terms cover acceptable use

Third party pass through terms

Optional product development schedule

AI Security

The AI Risk Landscape

How SAP stays ahead

AI systems face risks like data poisoning, model theft, and supply chain vulnerabilities. SAP mitigates these with OWASP-aligned safeguards, lifecycle checks, and operational security controls—ensuring resilience from design to deployment.

Security isn't static—SAP evolves controls as threats evolve.

Read more

Flexible LLM Integration

Hosted by BYOM, or third-party

SAP AI Core supports three integration paths:	**01. SAP Hosted LLMS**	**02. Third Party LLMS**	**03. Bring Your Own Model (BYOM)**
• SAP-hosted models via Generative AI Hub • Bring Your Own Model (BYOM) with full control • Third-party LLMs via secure API Each option ensures flexibility, security, and fast time-to-value.	SAP provides pre-trained and optimized LLMs through the Generative AI Hub within AI Core. These models are ready to use for various tasks like text generation, summarization, translation, and more. Customer can easily access and utilize these models through the AI Core API, without the need to manage infrastructure or model deployment. Simple integration, faster time-to-value, and access to SAP's expertise in model optimization.	SAP has partnerships with several LLM providers (MS Azure, AWS, Google, Open Sources) , making it easier to integrate their models into AI Core. AI Core allows you to connect to third-party LLM providers through API integrations. This gives you access to a wide range of models with different capabilities and specializations. Broad choice of models, leverage specialized expertise, and potential for cost optimization.	This option allows you to bring any open-source or custom-developed LLM into SAP AI Core. You have complete control over the model architecture, training data, and fine-tuning process. You package the model into a docker container and deploy it on the AI Core runtime environment. High flexibility, customization, and control over the model.

AI Ethics & Safety

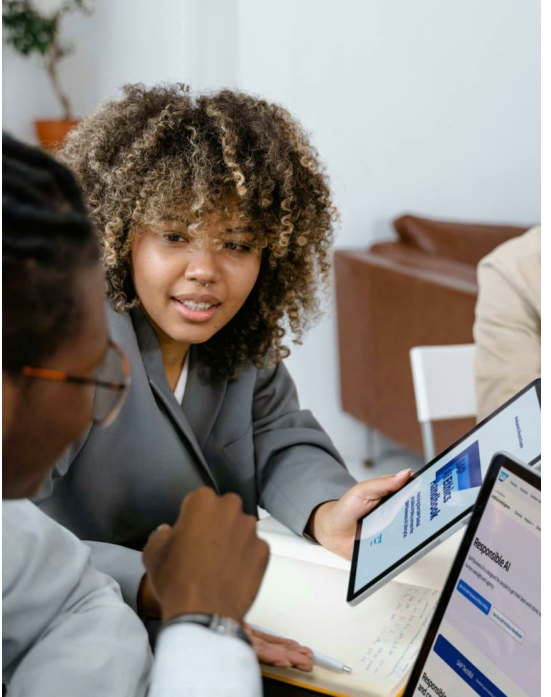
AI Ethics & Safety at SAP

- SAP is recognized by the **World Benchmarking Alliance** as one of only six global tech companies meeting all Ethical AI criteria.
- Our AI Ethics Policy is aligned with **UNESCO principles** - transparency & explainability, human oversight, and fairness - and embedded across the entire AI lifecycle, from ideation to productization.
- Through our **AI Ethics Assessment process**, we proactively identify and manage ethical risks to ensure responsible outcomes.

Learn more about Responsible AI at SAP

Explore SAP AI Ethics handbook

Guidelines: SAP global AI Ethics policy



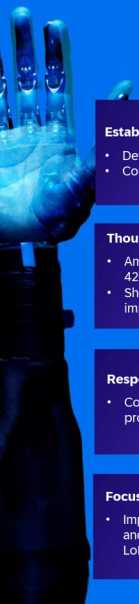
OUTLOOK

AGENTIC AI

Cost of inaction

Without clear rules and guidelines Agentic AI can cause significant damage

Agentic AI Framework for 2026



2025	2026
Established holistic AI Governance in SAP according to the AI Management system (ISO42001)	Exponential AI development requires improved and adapted Governance model including AI
Establishing AI Governance Framework • Definition of AI Management System • Connection and enhancement of Processes	**Agentic AI Governance Framework** • New capabilities and extended risks • Uplifting and extension of processes and controls for agentic AI
Thought leader in AI Governance • Among the first global ERP Provider that is ISO 42001 certified • Showcasing thought leadership and trustful implementation	**Build on momentum to keep Thought Leadership for responsible Agentic AI** • Showcasing thought leadership for Agentic AI • Build proactive as part of working groups and not only adopt reactive standards and regulations
Responsible AI for SAAS • Concentration on SAP as responsible AI provider	**Full Stack Responsible AI with Partners** • Enhancing out trust promise to collaborate with partners to showcase full stack responsible AI with Partners / Hyperscalers such as Microsoft and Google
Focus on connecting established processes • Implementation of AI Governance on processual and controls level for SGSC, Business AI and LoB's	**Agentic AI Governance on technical level** • Being an internal trusted partner for BTP and other LoBs for responsible Agentic AI and AI compliance on a deeper organizational and technical level

Empowering Tomorrow

From Structured AI Governance to Agentic Leadership:
Shaping responsible Agentic AI for a trustful Autonomous Future

Responsible AI isn‘t a one-time feature

It’s a journey—and SAP walks it with you.

Contact Information

Ranjan Vitt

AI Compliance Governance –
Program Co-Lead

Ranjan.vitt@sap.com

Ranjan Vitt
LinkedIn

Abou Diallo

AI Compliance Governance –
Program Co-Lead

Aboubacar.Diallo@sap.com

Abou Diallo
LinkedIn

Thank you!