



Methodology · 4 weeks · \$18,500

AI Governance Readiness: ISO/IEC 42001 and NIST AI RMF

Your AI workloads on Amazon Bedrock and Amazon SageMaker assessed against ISO/IEC 42001 Annex A and the NIST AI Risk Management Framework, producing a policy set, a GRC-ready control set, and a board briefing.

DURATION

4 weeks

STANDARDS

ISO 42001 + NIST AI RMF

OUTPUT

GRC-ready control set

INVESTMENT

\$18,500

Engagement phases

PHASE	TIMING	WHAT HAPPENS
Discovery	Week 1	Workshops with AI, engineering, security, and legal stakeholders to inventory AI use cases, data flows, model sources, and ownership. Shadow AI usage is surfaced here, not assumed away.
Environment review	Week 2	Read-only review of Amazon Bedrock, SageMaker, and related configuration: guardrails, model access boundaries, logging, and data handling.
Gap analysis	Weeks 2-3	Assessment against ISO/IEC 42001 Annex A controls and the NIST AI RMF Govern, Map, Measure, and Manage functions, scored with evidence notes.
Policy and control build	Week 3	AI governance policy set drafted and the control set formatted for import into your GRC platform.
Delivery	Week 4	Walkthrough with your team plus a board-ready briefing on AI risk posture.

Scope of review

AWS SERVICE OR AREA	WHAT IS EXAMINED
Amazon Bedrock	Model access, Bedrock Guardrails configuration, prompt and response logging, model evaluation practice
Amazon SageMaker AI	Model governance, model cards, model registry, training data lineage, endpoint protection
Amazon Q	Enterprise deployment patterns, data source connections, and access boundaries
AWS CloudTrail	Invocation logging, auditability, and retention for AI system activity
Amazon Macie, AWS KMS	Sensitivity classification of training and retrieval data; encryption of models, prompts, and outputs
AWS IAM	Model access boundaries, least privilege, and separation of duties for AI systems

What we need from you

- List of AI use cases in production, in pilot, and proposed
- Model sources: foundation models, fine-tuned models, and third-party AI services in use
- Any existing AI policy, acceptable use guidance, or customer AI commitments
- Customer or partner AI questionnaires you have received
- Read-only access to AWS accounts hosting AI workloads
- Access to AI, security, legal, and product stakeholders for workshops

Deliverables

- AI system inventory with owners, data flows, and risk classification
- ISO/IEC 42001 Annex A gap analysis, scored with evidence notes
- NIST AI RMF mapping across Govern, Map, Measure, and Manage
- AI governance policy set: acceptable use, model approval, data handling, human oversight, AI incident handling
- Control set formatted for import into your GRC platform
- Board-ready briefing on AI risk posture

Assumptions and exclusions

- This is a readiness assessment. ISO/IEC 42001 certification must be performed by an accredited certification body
- Model performance, bias, and fairness testing is a separate technical engagement
- Legal review of AI contractual terms is outside scope and should involve counsel
- Implementation of recommended controls is quoted separately

Support and service levels

Pre-purchase. Scoping conversations, AWS prerequisite confirmation, and a written statement of work before any private offer is issued. Inquiries answered within two business days.

During the engagement. A named engagement lead, Brian Govanlu, CISSP, as single point of contact. Support Monday to Friday, 9:00 AM to 6:00 PM US Eastern, by email and phone, with a response within one business day. Kickoff within five business days of offer acceptance, weekly written status updates, and a walkthrough of every deliverable.

After delivery. Thirty days of email support for questions about findings and recommendations. Refunds and disputes are handled directly with the engagement lead in accordance with the accepted private offer.

Available directly or through AWS Marketplace as a private offer. If you hold committed AWS spend, the engagement draws down against it and appears on your existing AWS bill. Any AWS infrastructure costs you incur remain your responsibility and are separate from the AWS Marketplace transaction.