

iapp



# AIGP Body of Knowledge and Exam Blueprint

Version 2.1.0

Effective date: 2 February 2026



# THE AIGP BODY OF KNOWLEDGE

## UNDERSTANDING THE AIGP BODY OF KNOWLEDGE

The main purpose of the AIGP BoK is to document the knowledge and skills that will be assessed on the AIGP certification exam. The domains reflect what the artificial intelligence governance professional should know and be able to do to show competency in this designation.

The BoK also includes the exam blueprint numbers, which show the minimum and maximum number of questions from each domain that will be found on the exam.

The BoK is developed and maintained by the subject matter experts that constitute each designation [exam development board](#).

Every year, the BoK is reviewed and, if necessary, updated. Changes are reflected in the annual exam updates and communicated to candidates at least 90 days before the new content appears in the exam.

## COMPETENCIES AND PERFORMANCE INDICATORS

The content in the BoK is represented as a series of competencies and connected performance indicators. Competencies represent broad knowledge domains in which qualified professionals should be conversant. Performance indicators are the discrete tasks and abilities that validate the professional's level of proficiency in the broader competence group. Exam questions assess an AI governance professional's proficiency on the performance indicators.

## WHAT TYPES OF QUESTIONS WILL BE ON THE EXAM?

The performance indicators are guides to the depth of knowledge required to demonstrate competency. The verbs that begin the skill and task statements (identify, evaluate, implement, define) signal the level of complexity of the exam questions. You can find their corollaries on Bloom's Taxonomy (see next page).

## OUR APPROACH TO AI CERTIFICATION

Our certification concentrates on AI governance. It builds a clear foundation in AI concepts and the principles, benefits, risks and responsibilities that underpin sound oversight. We distill global laws, frameworks and standards to their most widely accepted elements. Although some laws separate "developers" from "deployers" to assign liability, we use these labels only to describe distinct tasks. Many organizations will fill both roles. We continue to evolve content to cover rapidly changing governance requirements and the innovative applications of AI to which they apply, such as generative AI and agentic AI. Rather than covering every niche, this certification program delivers the core knowledge you need to govern AI effectively. Anyone responsible for adopting or managing AI in an organization will benefit. Because AI now touches every sector and role, a grasp of AI governance is essential to reduce risk and foster innovation.

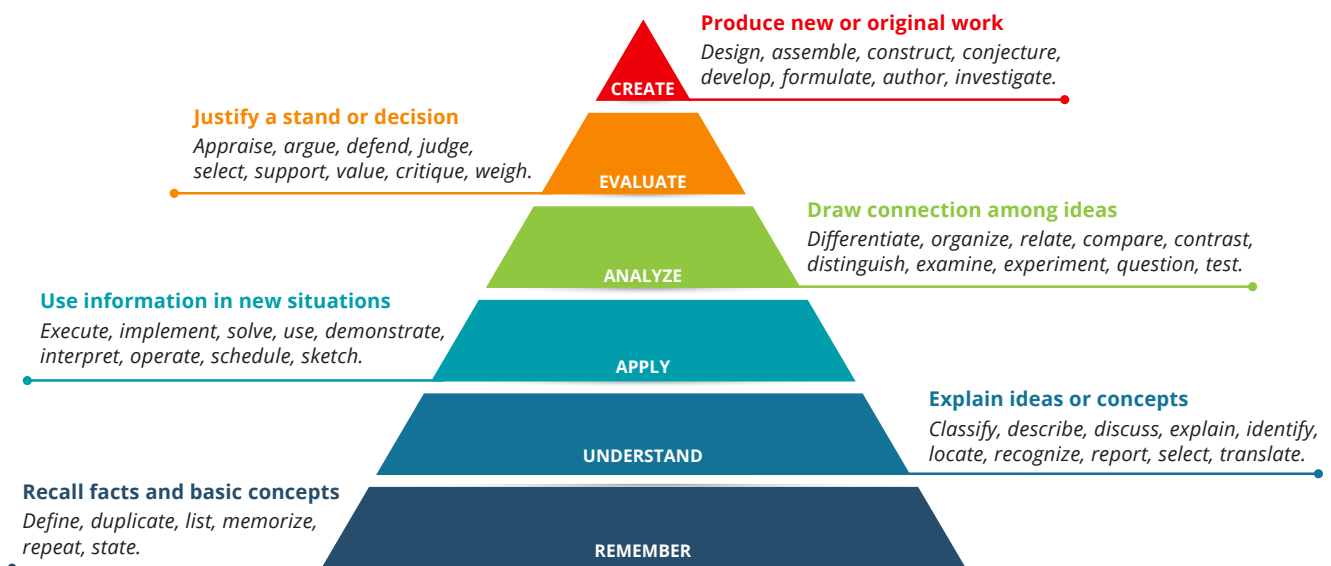
## SUMMARY

This edition reflects today's AI governance landscape and offers a broad curriculum for assessing candidates. We trust it will support your growth as an AI governance professional. For further resources, please visit the [IAPP AI Governance Center](#).

# THE AIGP BODY OF KNOWLEDGE

## BLOOM'S TAXONOMY

Bloom's Taxonomy (often represented as a pyramid) is a hierarchy of cognitive skills used to establish educational learning objectives. IAPP exam questions mostly focus on the remember/understand and apply/analyze levels.





# THE AIGP BODY OF KNOWLEDGE

MIN.	MAX.	Domain I – Understanding the foundations of AI governance	
16	20	<p><b>Domain I – Understanding the foundations of AI governance</b> focuses on what AI governance is, including the common principles and pillars to build an AI governance program. This domain covers best practices regardless of industry, sector or size.</p>	
		<b>COMPETENCIES</b>	<b>PERFORMANCE INDICATORS</b>
4	6	I.A	Understand what AI is and why it needs governance.
			Know the generally accepted definitions and types of AI.
			Identify the types of risks and harms posed by AI to individuals, groups, organizations and society (e.g., misalignment with objectives, ethics and bias risk, and complexity and scalability).
5	7	I.B	Identify the unique characteristics of AI that require a comprehensive approach to governance (e.g., complexity, opacity, autonomy, speed and scale, potential for harm or misuse, data dependency, and probabilistic versus deterministic outputs).
			Identify and apply the common principles of responsible AI (e.g., fairness, safety and reliability, privacy and security, transparency and explainability, accountability and human-centricity).
			Define roles and responsibilities for AI governance stakeholders.
			Establish cross-functional collaboration in the AI governance program (e.g., for efficacy and diversity of expertise and perspective).
			Create and deliver a training and awareness program to all stakeholders on AI terminology, strategy and governance.
6	8	I.C	Differentiate approaches to AI governance based upon company size, maturity, industry, products and services, objectives and risk tolerance.
			Identify differences among AI developers, providers, deployers and users from a governance perspective (e.g., with respect to responsibilities, opportunities and needs).
			Create and implement policies to ensure oversight and accountability across all AI life cycle stages (e.g., use case assessment, risk management, ethics by design, data acquisition and use, model and system development, training and testing, deployment and monitoring, documentation and reporting, and incident management).
			Establish policies and procedures to apply throughout the AI life cycle.
			Evaluate and update existing policies (e.g., data privacy, security, data governance and intellectual property) for AI.
			Create, update and implement policies, assessments and contracts to manage third-party risk (e.g., procurement, supply chain, human resources and acceptable use).



# THE AIGP BODY OF KNOWLEDGE

## MIN. MAX. Domain II – Understanding how laws, standards and frameworks apply to AI

**19 23** **Domain II – Understanding how laws, standards and frameworks apply to AI**  
 Understanding how laws, standards and frameworks apply to AI focuses on existing laws that apply to AI, as well as AI-specific laws, standards and frameworks. For the AI governance professional, this means an understanding of the major elements of current AI laws (e.g., the EU AI Act, the South Korean AI Basic Law, federal and state AI laws that apply to private sector organizations).

### COMPETENCIES

### PERFORMANCE INDICATORS

<b>4 6 II.A</b>	Understand how existing data privacy laws apply to AI.	Understand how transparency, choice, lawful basis and purpose limitation requirements apply to AI.
		Understand how data minimization and privacy by design requirements apply to AI.
		Understand how obligations on data controllers apply to AI (e.g., regarding privacy impact assessments, use of third-party processors, cross-border data transfers, data subject rights, automated decision making, incident management, breach notification and record keeping).
		Understand the requirements that apply to sensitive or special categories of data (e.g., biometrics).
<b>4 6 II.B</b>	Understand how other types of existing laws apply to AI.	Understand how intellectual property laws apply to AI (e.g., prohibiting or limiting use of data for AI training).
		Understand how nondiscrimination laws apply to AI (e.g., in the employment, credit, lending, housing and insurance contexts).
		Understand how consumer protection laws apply to AI (e.g., prohibiting unfair and deceptive acts or practices).
<b>6 8 II.C</b>	Understand the main elements of AI-specific laws.	Understand how product liability laws apply to AI (e.g., prohibiting design and manufacturing defects).
		Understand the risk classification framework for AI (e.g., prohibited/high/limited/minimal risk) and what systems/uses fall into each category.
		Understand the key requirements around risk management, data governance, technical documentation, conformity/impact assessments and record keeping.
		Understand the key requirements around human oversight, transparency and notification, and quality management.
		Understand the distinct requirements for general-purpose AI models.
		Understand the enforcement framework and penalties for noncompliance.
		Understand the differences in requirements based on organizational context (e.g., providers, deployers, importers and distributors).



# THE AIGP BODY OF KNOWLEDGE

## MIN. MAX. Domain II – Understanding how laws, standards and frameworks apply to AI

**19 23** **Domain II – Understanding how laws, standards and frameworks apply to AI**  
 Understanding how laws, standards and frameworks apply to AI focuses on existing laws that apply to AI, as well as AI-specific laws, standards and frameworks. For the AI governance professional, this means an understanding of the major elements of current AI laws (e.g., the EU AI Act, the South Korean AI Basic Law, federal and state AI laws that apply to private sector organizations).

### COMPETENCIES

### PERFORMANCE INDICATORS

**3 5 II.D** Understand the main industry standards and tools that apply to AI.

Understand the Organisation for Economic Co-operation and Development (OECD) principles, framework, policies and recommended practices for trustworthy AI.

Understand the NIST AI Risk Management Framework and Playbook (e.g., core functions, categories and subcategories).

Understand the core ISO AI standards (i.e., 22989, 42001 and 42005).



# THE AIGP BODY OF KNOWLEDGE

MIN. MAX. **Domain III – Understanding how to govern AI development**

**21 25** **Domain III – Understanding how to govern AI development** focuses on the responsibilities of AI governance professionals with respect to designing, building, training, testing and maintaining AI systems.

**COMPETENCIES**

**PERFORMANCE INDICATORS**

6	8	III.A	Govern the designing and building of the AI system.	Define the business context and use case of the AI system.
				Perform or review an impact assessment on the AI system.
				Apply the policies, procedures, best practices and ethical considerations to designing and building the AI system (e.g., purpose of AI, requirements gathering, architecture and model selection, human oversight, data analysis, metric and threshold evaluation, stakeholder engagement and feedback, and operational controls).
				Identify and manage the internal and external risks and contributing factors related to designing and building the AI model and system (e.g., using probability/severity harms matrix, using a risk mitigation hierarchy, stakeholder mapping, use-case evaluation, benchmarking, and pre-deployment pilots and testing).
				Document the designing and building process (e.g., to establish compliance and manage risks).
6	8	III.B	Govern the collection and use of data in training and testing the AI model and system.	Establish and follow the requirements for data governance (e.g., assess and document lawful rights to collect and use data, and assess data quality, quantity, integrity and fit-for-purpose).
				Establish and document data lineage and provenance.
				Plan and perform training and testing of the AI model and system (e.g., unit, integration, validation, performance, security, bias and interpretability).
				Identify and manage issues and risks during training and testing of an the AI model and system.
				Document the training and testing process (e.g., to validate results, establish compliance and manage risks).



# THE AIGP BODY OF KNOWLEDGE

MIN. MAX. **Domain III – Understanding how to govern AI development**

**21 25** **Domain III – Understanding how to govern AI development** focuses on the responsibilities of AI governance professionals with respect to designing, building, training, testing and maintaining AI systems.

**COMPETENCIES**

**PERFORMANCE INDICATORS**

<p><b>8 10 III.C</b></p> <p>Govern the release, monitoring and maintenance of the AI system.</p>	Assess readiness, and prepare for release into production (e.g., creating the model card and satisfying conformity requirements).
	Conduct continuous monitoring of the AI system, and establish a regular schedule for maintenance, updates and retraining.
	Conduct periodic activities to assess the AI system’s performance, reliability and safety (e.g., audits, red teaming, threat modeling and security testing).
	Manage and document incidents, issues and risks.
	Collaborate with cross-functional stakeholders to understand why incidents arise from AI systems (e.g., brittleness, lack of robustness, lack of quality data, insufficient testing, and model or data drift).
	Make public disclosures to meet transparency obligations (e.g., technical documentation, instructions for use to deployers and post-market monitoring plans).



# THE AIGP BODY OF KNOWLEDGE

## MIN. MAX. Domain IV – Understanding how to govern AI deployment and use

**21 25** **Domain IV – Understanding how to govern AI deployment and use** focuses on the responsibilities of AI governance professionals with respect to selecting an AI model, then deploying and using it responsibly through ongoing monitoring maintenance, and other key obligations. This domain applies in any deployment context, such as a company deploying its own proprietary model or one from a third party.

### COMPETENCIES

### PERFORMANCE INDICATORS

6	8	IV.A	Evaluate key factors and risks relevant to the decision to deploy the AI system.	Understand the context of the AI use case (e.g., business objectives, performance requirements, data availability, ethical considerations and workforce readiness).
				Understand the differences in AI model types (e.g., classic vs. generative, proprietary vs. open source, small vs. large, and language vs. multimodal capabilities).
				Understand the differences in AI deployment options (e.g., cloud vs. on-premise vs. edge, and using the AI model as is or with fine-tuning, retrieval augmented generation, agentic architectures, or other techniques to improve performance and fit).
5	7	IV.B	Perform key activities to assess the AI system.	Perform or review an impact assessment on the selected AI system.
				Identify and evaluate key terms and risks in the vendor or licensing agreement.
9	11	IV.C	Govern the deployment and use of the AI system.	Identify and understand the risks and opportunities that are unique to a company deploying its own proprietary AI model (e.g., increased obligations and higher potential liability).
				Apply the policies, procedures, best practices and ethical considerations to the deployment of an AI system (e.g., data governance, risk management, issue management, and user training).
				Conduct continuous monitoring of the AI model and system, and establish a regular schedule for maintenance, updates and retraining.
				Conduct periodic activities to assess the AI system's performance, reliability and safety (e.g., audits, red teaming, threat modeling and security testing).
				Document incidents, issues, risks and post-market monitoring plans.
				Forecast and reduce risks of secondary or unintended uses and downstream harms.
Establish external communication plans.				
				Create and implement a policy and controls to deactivate or localize an AI system as necessary (e.g., due to regulatory requirements or performance issues).