iapp

AIGP BODY OF KNOWLEDGE AND EXAM BLUEPRINT

VERSION 2.0.1

EFFECTIVE DATE: 3 February 2025

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 AI 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 FOCUS FOR VERSION 2

The focal points for this update to the BoK, include: (1) establish a more comprehensive foundation for understanding AI and the unique needs for, and approaches to, AI governance; (2) reflect the current laws, regulations and industry standards; (3) more clearly differentiate how governance is applied to AI development, deployment and use, and (4) focus on practical responsibilities, not theoretical questions, that AI governance professionals face on a daily basis.

While legislation has begun to create distinctions between developer and deployer to better understand where liability rests, we use these terms not as a binary classification of organizations, but to distinguish sets of tasks and abilities that are specific to deployment and development, fully understanding there will be situations where organizations play both roles.

LAWS, FRAMEWORKS AND STANDARDS

We did not include individual AI specific U.S. state laws at this time, not because they are unimportant, but because they are currently piecemeal and could easily overwhelm the rest of the exam content. We know that if your organization is subject to one of these laws, you will educate yourself on the requirements of that state law. There are many useful monitoring resources available, including the IAPP's AI Governance Center State Tracker.

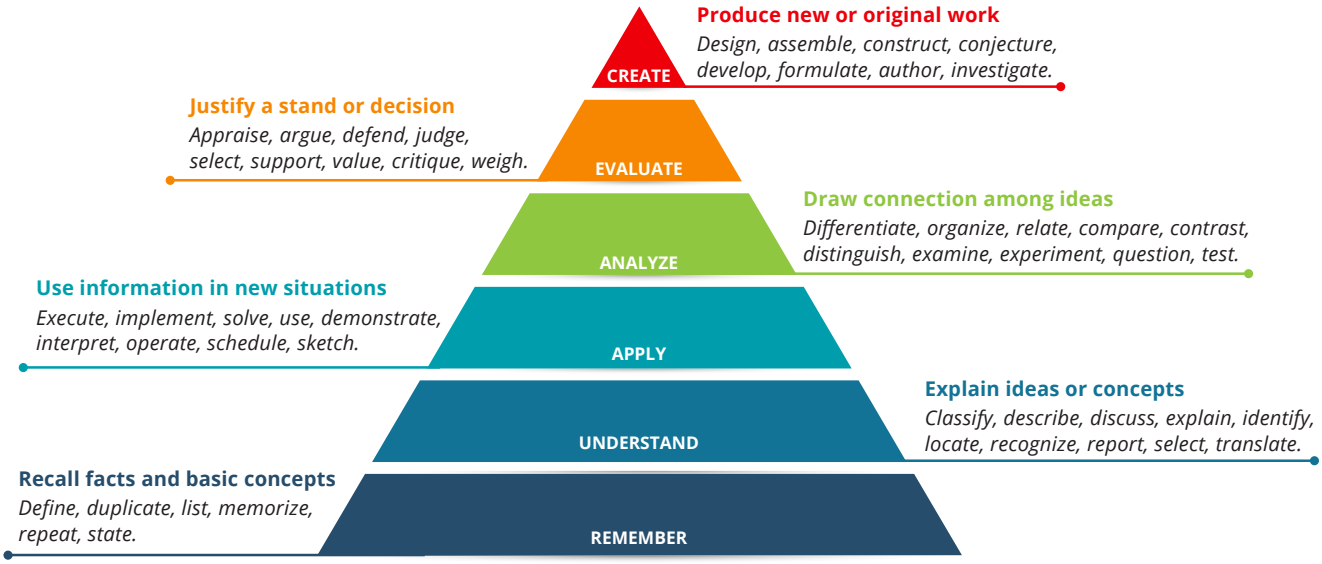
Similarly, we chose to simplify the approach to industry standards and frameworks. Many have emerged this past year to offer guidance to organizations, yet we chose to focus on those that have been globally accepted or serve as the foundation for new releases.

SUMMATION

We believe this version reflects the current state of the field for AI governance, and will offer a rich spectrum of topics to assess candidates. We hope you will find the changes we have made for this second version to be helpful in your journey as an AI governance professional. Please visit the IAPP AI Governance Center for links to the resources mentioned here and much more, including the IAPP AI Glossary, myriad reports and trackers from our research and publications teams.

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.



MIN	MAX		Domain I — Understanding the foundations of AI governance	
16	20		**Domain I — Understanding the foundations of AI governance** focuses on what AI governance is, including the common principles and pillars to build an AI governance program. This domain cover best practices regardless of industry, sector or size.	
			COMPETENCIES	**PERFORMANCE INDICATORS**
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).
				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).
5	**7**	**I.B**	Establish and communicate organizational expectations for AI governance.	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.
				Differentiate approaches to AI governance based upon company size, maturity, industry, products and services, objectives and risk tolerance.
				Identify differences among AI developers, deployers and users from a governance perspective (e.g., with respect to responsibilities, opportunities and needs).
6	**8**	**I.C**	Establish policies and procedures to apply throughout the AI life cycle.	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 development, training and testing, deployment and monitoring, documentation and reporting and incident management).
				Evaluate and update existing data privacy and security policies for AI.
				Create and implement policies to manage third-party risk (e.g., procurement, supply chain and human resources).

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** focuses on existing laws that apply to AI, as well as new AI-specific laws, standards and frameworks.		
			COMPETENCIES	**PERFORMANCE INDICATORS**
4	**6**	**II.A**	Understand how existing data privacy laws apply to AI.	Understand how notice, choice, consent, 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, incident management, breach notification and record keeping).
				Understand the requirements that apply to sensitive or special categories of data (e.g., biometrics).
4	**6**	**II.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 non-discrimination 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).
				Understand how product liability laws apply to AI (e.g., prohibiting design or manufacturing defects).
5	**7**	**II.C**	Understand the main elements of the EU AI Act.	Understand the risk classification framework for AI (i.e., prohibited AI, high-risk, limited-risk and minimal-risk) and what systems fall into each category.
				Understand the key requirements for high-risk, limited-risk and minimal-risk AI including risk management, data governance, technical documentation, conformity assessment, record keeping, human oversight, transparency and notification, quality management (as applicable).
				Understand the distinct requirements for general purpose AI models.
				Understand the enforcement framework and penalties for non-compliance.
				Understand the differences in requirements based on organizational context (e.g., providers, deployers, importers, and distributors).

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** focuses on existing laws that apply to AI, as well as new AI-specific laws, standards and frameworks.		
		COMPETENCIES		**PERFORMANCE INDICATORS**
4	**6**	**II.D**	Understand the main industry standards and tools that apply to AI.	Understand the OECD principles, framework, policies and recommended practices for trustworthy AI.
				Understand the NIST AI Risk Management Framework and Playbook (e.g., the core functions, categories and subcategories).
				Understand the NIST ARIA program for methodologies, tools, metrics and measurements on AI safety.
				Understand the core ISO AI standards (i.e., 22989 and 42001).

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 models.	
			COMPETENCIES	**PERFORMANCE INDICATORS**
6	**8**	**III.A**	Govern the designing and building of the AI model.	Define the business context and use case of the AI model.
				Perform or review an impact assessment on the AI model.
				Identify laws that apply to the AI model.
				Apply the policies, procedures, best practices and ethical considerations to designing and building the AI model (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 (e.g., using probability/severity harms matrix, using a risk mitigation hierarchy, stakeholder mapping, use case evaluation, benchmarking, 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.	Establish and follow the requirements for data governance (e.g., assess and document lawful rights to collect and use data, and to 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 (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.
				Document the training and testing process (e.g., to validate results, establish compliance and manage risks).

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 models.		
		COMPETENCIES		**PERFORMANCE INDICATORS**
8	**10**	**III.C**	Govern the release, monitoring and maintenance of the AI model.	Assess readiness and prepare for release into production (e.g., creating the model card and satisfying conformity requirements).
				Conduct continuous monitoring of the AI model and establish a regular schedule for maintenance, updates and retraining.
				Conduct periodic activities to assess the AI model'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 models (e.g., brittleness, lack of robustness, lack of quality data, insufficient testing, and model or data drift).
				Make public disclosures with to meet transparency obligations (e.g., technical documentation, instructions for use to deployers, and post-market monitoring plans).

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 on-going monitoring, maintenance, and other key obligations. This domain applies to any model type, 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 model.	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, or other techniques to improve performance and fit).
5	7	IV.B	Perform key activities to assess the AI model.	Perform or review an impact assessment on the selected AI model.
				Identify laws that apply to the AI model.
				Identify and evaluate key terms and risks in the vendor or open source agreement.
				Identify and understand issues that are unique to a company deploying its own proprietary AI model (e.g., increased obligations and higher potential liability).
9	11	IV.C	Govern the deployment and use of the AI model.	Apply the policies, procedures, best practices and ethical considerations to the deployment of an AI model (e.g., data governance, risk management, issue management, user training).
				Conduct continuous monitoring of the AI model and establish a regular schedule for maintenance, updates and retraining.
				Conduct periodic activities to assess the AI model'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 model as necessary (e.g., due to regulatory requirements or performance issues).