**Preparing for the AIGP Certification**

**Introduction and Module One**

# Overall differences between versions 1.0 and 2.0

There are significative changes between versions 1.0 and 2.0:

* Consolidation from six to four domains *[domains are treated as course modules].*
* New organization focuses on the life cycle of the AI systems.
* Reduced emphasis on technical and theoretical aspects.
* There is a significant leap in quality and relevance in version 2.0.

As a result, the information in the course is not directly in line with the competences of the current version. As suggested, we will add and update some materials.

The next table aims to present the differences in competences from both versions. The differences are more evident in the performance indicators that underpin the certification’s base of knowledge [BoK].

|  |  |
| --- | --- |
| **Base of Knowledge v 1.0** | **Base of Knowledge v 2.0** |
| **Domain I. Understanding the Foundations of Artificial Intelligence**  Competences:  I.A Understand the basic elements of AI and ML.  I.B Understand the differences among types of AI systems.  I.C Understand the AI technology stack.  I.D Understand the history of AI and the evolution of data science.  **Domain II. Understanding AI Impacts on People and Responsible AI Principles**  Competences:  II.A Understand the core risks and harms posed by AI systems.  II.B Understand the characteristics of trustworthy AI systems.  II.C Understand the similarities and differences among existing and emerging ethical guidance on AI. | **Domain I. Understanding the Foundations of AI Governance**  Competences:  I.A. Understand what Ai is and why it needs governance.  I.B. Establish and communicate organizational expectations for AI governance.  I.C. Establish policies and procedures to apply throughout the AI life cycle. |
| **Domain III. Understanding How Current Laws Apply to AI Systems**  Competences:  III.A Understand the existing laws that interact with AI use  III.B Understanding key GDPR intersections  III.C Understanding liability reform  **Domain IV. Understanding the Existing and Emerging AI Laws and Standards**  Competences:  IV.A Understanding the requirements of the EU IA Act.  IV.B Understand other emerging global laws.  IV.C Understand the similarities and differences among the major risks management frameworks and standards. | **Domain II. Understanding how laws, standards and frameworks apply to AI**  Competences:  II.A Understand how existing data privacy laws apply to AI.  II.B Understand how other types of existing laws apply to AI.  II.C Understand the main elements of the EU AI Act.  II.D. Understand the main industry standards and tools that apply to AI. |
| **Domain V. Understanding the AI Development Life Cycle**  Competences:  V.A Understand the key steps in the AI system planning phase.  V.B Understand the key steps in the AI system design phase.  V.C Understand the key steps in the AI system development phase.  V.C Understand the key steps in the AI system implementation phase. | **Domain III. Understanding how to govern AI development**  Competences:  III.A Govern the designing and building of the AI model.  III.B Govern the collection and use of data in training and testing the AI model.  III.C Govern the release, monitoring and maintenance of the AI model.  **Domain IV. Understanding how to govern AI deployment and use**  Competences:  IV.A Evaluate key factors and risks relevant to the decision to deploy the AI model.  IV.B Perform key activities to assess the AI model.  IV.C Govern the deployment and use of the AI model. |
| **Domain VI. Implementing Responsible AI Governance and Risk Management**  Competences:  VI.A Ensure interoperability of AI risk management with other operational risk strategies.  VI.B Integrate AI governance principles into the company.  VI.C Stablish an IA governance infrastructure.  VI.D Map, plan and scope the AI project.  VI.E Test and validate the AI system during development.  VI.F Manage and monitor AI systems after deployment  **Domain VII. Contemplating Ongoing Issues and Concerns**  Competences:  VII.A Awareness of legal issues  VII.B Awareness of user concerns  VII.C Awareness of AI auditing and accountability issues. |  |

Domain I >

**Understanding the foundations of AI governance**

This domain 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.

###### Competency I.A 4/6 questions

###### Understand what AI is and why it needs governance

### Performance Indicators

* 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).

### Some questions from the exam sample

Question 1: Ensuring AI Integrity and Data Accuracy

Examine the method ensuring AI integrity and data accuracy hinting at understanding different AI functionalities like tracking data linage.

A. Tracking data lineage.

B. Assuming the data is accurate.

C. Purchasing data from a vendor.

D. Reversioning the data internally.

Context: Focuses on methods to ensure that AI data is representative, accurate, and unbiased, relevant to knowing AI definitions and types​.

Question 12: Mitigating AI System Errors

Discusses considerations for mitigating AI system errors, directly linking to understanding the types of risks posed by AI, such as biases and errors related to data types​

A. Excluding a review of previous incidents.

B. Focusing exclusively on legal compliance.

C. Adopting a uniform approach for all errors.

D. Understanding the AI use case and the data type.

Context: Discusses the importance of understanding AI use cases and data types to mitigate risks and errors, linking directly to identifying risks and harms posed by AI​.

Question 21: Potential Group Harms Associated with AI Technologies

Highlights examples of potential group harms associated with AI technologies, directly addressing the types of risks and harms AI might pose​.

A. Safety and deep fakes.

B. Acceleration and reputational.

C. Mass surveillance and facial recognition.

D. Carbon dioxide emission and agricultural.

Context: Explores examples of group harms, addressing risks and harms AI poses to society, such as privacy violations or biased outcomes​.

**Question 9: Best Practice for Integrating AI into Operational Risk Monitoring**

Looks at integrating AI into operational risk monitoring without compromising data privacy, addressing the need for comprehensive AI governance due to AI's unique characteristics like complexity and data dependency​

A. Allow full access to the AI system for all employees.

B. Focus only on operational risks, ignoring privacy risks.

C. Apply data minimization and transparency principles in AI.

D. Delete all personal data from the system to avoid privacy risks.

Context: This question assesses best practices for integrating AI in a way that does not compromise data privacy, touching on the need for comprehensive AI governance due to AI's unique characteristics like complexity and data dependency​

Question 7: Interoperability of AI and Privacy Risk Management

Discusses steps to ensure interoperability of AI risk management with privacy risk management, which includes applying common principles of responsible AI such as transparency and accountability​.

A. Conduct regular simulations and tests.

B. Implement continuous audit protocols.

C. Create a specialized multidisciplinary team.

D. Develop ethical and transparent AI algorithms.

Context: Suggests steps for ensuring interoperability between AI risk management and privacy risk management,

embodying responsible AI principles​.

Question 13: AI Model's Impact Assessment Documentation

Covers what should be included in an AI model's impact assessment, touching on transparency, accountability, and stakeholder concerns, which are all principles of responsible AI​.

A. Marketing and sales budgets.

B. Stakeholder input and concerns.

C. User demographics and feedback.

D. Training algorithm and audit details.

Context: Focuses on what should be included in an AI model’s impact assessment, particularly elements like stakeholder concerns and audit details, relevant to responsible AI principles

###### Competency I.B 5/7 questions

###### Establish and communicate organizational expectations for AI governance.

### Performance Indicators

* 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).

### Some questions from the exam sample

Question 84: Establishing Roles and Responsibilities in AI Governance

What is a critical consideration when determining roles and responsibilities in AI governance?

A. Test and validate the AI system.

B. Establish priorities and allocate resources.

C. Compile feedback from impacted AI actors.

D. Establish appropriate roles and responsibilities.

Context: Focuses on the importance of defining clear roles and responsibilities for AI governance stakeholders.

Question 37: Cross-Functional Collaboration in AI Governance

What is a primary consideration for tailoring AI governance to the organization?

A. The availability and expertise of the organization’s IT team.

B. The organization’s budget constraints and financial resources.

C. The unique context, culture, and objectives of the organization.

D. Emerging trends and innovations in the broader industry landscape.

Context: Highlights the need for cross-functional collaboration by considering the unique context and objectives of the organization which impacts AI governance efficacy.

Question 7: Training and Awareness Programs

With this solution in sight, what initial step should AlphaTech take to ensure the interoperability of AI risk management with privacy risk management in its operations?

A. Conduct regular simulations and tests.

B. Implement continuous audit protocols.

C. Create a specialized multidisciplinary team.

D. Develop ethical and transparent AI algorithms.

Context: Discusses steps to integrate AI risk management with privacy risk management, essential for training stakeholders in AI governance.

Question 38: Differentiation in AI Governance Approaches

To strengthen the AI governance program early in its build-out, Tochi must do which of the following?

A. Block third-party AI solutions from being deployed in the organization.

B. Evaluate technology solutions different stakeholders can leverage in assessing AI solutions.

C. Create a new organization charter and hire AI experts to build new AI governance processes.

D. Understand the stakeholders involved and engage them early to identify areas of partnership.

Context: Emphasizes different governance approaches based on stakeholder engagement and partnership, crucial for organizations of varying sizes and industry sectors.

Question 52: Differences Among AI Developers, Deployers, and Users

A newly developed AI system in your organization is almost ready to deploy. The engineers who collaborated on the project are the most appropriate personnel to ensure which of the following is in place before the system is deployed?

A. A change management plan to support widespread internal adoption.

B. A new company policy to address AI developer, deployer, and user risks.

C. A method for continuous monitoring for issues that affect performance.

D. A set of documented roles and responsibilities for an AI governance program.

Context: Directly addresses the differences in roles and responsibilities among AI developers, deployers, and users from a governance perspective.

###### Competency I.C 6/8 questions

###### Establish policies and procedures to apply throughout the AI life cycle

### Performance Indicators

* 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)

### Some questions from the exam sample

Question 79: Policies to Ensure Oversight and Accountability Across All AI Lifecycle Stages

Which of the following is NOT a key component of AI governance policies to ensure oversight and accountability across all AI lifecycle stages?

A. Implementing a data privacy compliance program.

B. Establishing a centralized AI governance committee.

C. Promoting a culture of innovation and experimentation.

D. Developing comprehensive AI risk assessment frameworks.

Context: This question addresses the components necessary for robust AI governance across various stages of AI development and implementation.

Question 51: Evaluate and Update Existing Data Privacy and Security Policies for AI

As the privacy officer of a large commercial organization, which of the following will NOT require you to re-evaluate existing data privacy policies?

A. A jurisdiction in which you operate enacted a new law governing the use of AI in the private sector.

B. The privacy department has expanded from ten part-time employees to twelve full-time employees.

C. The finance department is planning to use a machine learning process to pre-approve financing for products.

D. Customer support is replacing some customer support team members with an AI-driven chatbot for customer inquiries.

Context: This question focuses on situations that may or may not trigger a re-evaluation of data privacy and security policies in the context of AI deployment.

Question 93: Policies to Manage Third-Party Risk

To understand third-party risk in the organization, it is necessary to identify all third-party tools that are integrated into the system. If there is an incident, the organization might need to notify the user of these third-party tools, as the incident might not only impact the tool owned by the organization. Which of the following options contains elements that should be considered when building an AI incident response plan?

A. The security incident plan, which covers all requirements needed, includes required incident actions so the security team can oversee AI incident management.

B. The third-party tools that are integrated into your system should be identified because, in the case of an incident, you might need to notify those third parties.

Context: This question evaluates the need to integrate third-party risk management into broader AI governance and incident response plans.

## Readings

**NOTE:** All the readings are in the folder ***Readings/Domain1***

### Materials from 2023 course

#### AI – general

1. Artificial Intelligence. OECD. <https://www.oecd.org/digital/artificial-intelligence>

Description: OECD website’ AI landing page.

Relevance: Diverse information. I found pertinent to skim:

* Mapping emerging critical risks (working paper) 12/16/2024. *In folder.*

This paper focuses on identifying and understanding new risks that could significantly shape the future. These risks span social, environmental, and technological challenges, including climate change, resource shortages, geopolitical tensions, and emerging threats like cyberattacks or the misuse of artificial intelligence. Drawing on expert input and innovative tools, the report examines how governments and societies can better anticipate and respond to these risks. Emerging risks often evolve quickly, with the potential to disrupt economies, societies, and global stability. By recognising these threats early, governments, businesses, and communities can take proactive steps to adapt, protect their interests, and strengthen resilience. This forward-looking approach is crucial in an increasingly interconnected and unpredictable world, where crises can escalate rapidly and affect multiple sectors. The findings are valuable for policymakers, risk analysts, and organisations striving to enhance preparedness and decision-making in the face of uncertainty. By fostering a deeper understanding of future challenges, the report aims to equip stakeholders with the insights needed to address risks before they become critical, ensuring a safer and more sustainable future for all.

* Using foresight to anticipate emerging critical risks (working paper) 12/16/2024. *In folder.*

This paper presents a methodology to help countries identify and characterise global emerging critical risks as part of the OECD’s Framework on the Management of Emerging Critical Risks. It supports experts and policymakers tasked with anticipating and preparing for uncertain and evolving threats that transcend traditional national boundaries. The approach begins with horizon scanning to capture weak signals and unconventional data sources, including patent analysis, crowd forecasting, and the use of generative AI. It then applies structured foresight techniques, such as futures wheels, cross-impact analysis, and scenario-based “Risk-Worlds,” to explore how risks might manifest and interact in multiple possible future contexts. The methodology emphasises understanding risks “at source,” focusing on vulnerabilities, interconnectedness, and possible management strategies. Rather than predicting a single future, it seeks to broaden the range of possibilities, encouraging proactive adaptation, building collective understanding, and ultimately strengthening government capacity to navigate and shape an increasingly complex and uncertain global risk landscape.

1. OECD Framework for the Classification of AI Systems: a tool for effective AI policies. <https://oecd.ai/en/classification>

Description: 2-page document. *In folder.*

Relevance: Initial guidelines to classify AI systems linking technical characteristics with the OECD AI Principles. It provides useful quiz-worthy information, although it is very basic and likely that the model has been superseded by more robust AI classification models developed.

A diagram of people and planet

Description automatically generated

1. “The Spectrum of Artificial Intelligence.” Future of Privacy Forum. <https://iapp.org/media/images/resource_center/fpf_infographic_the_spectrum_of_artificial_intelligence.jpg>
2. Turing, A.M. “Computing Machinery and Intelligence.” Mind 59, (1950): 433-460. <https://www.cs.ox.ac.uk/activities/ieg/e-library/sources/t_article.pdf>

### AI governance

1. “AI ethics & governance.” Accenture. <https://www.accenture.com/us-en/services/applied-intelligence/ai-ethics-governance>
2. AI Risk Management Framework. NIST. <https://www.nist.gov/itl/ai-risk-management-framework>
3. Baruch, Tang, Jain, Gong, Murchison, Adams and Harrington. “Our Responsible AI Principles in Practice.” LinkedIn Engineering blog, April 13, 2023. <https://www.linkedin.com/blog/engineering/responsible-ai/our-responsible-ai-principles-in-practice>
4. Casovan, Jones and Chaudhry. “AI Governance in Practice Report 2024.” IAPP and FTI Consulting, June 2024. <https://iapp.org/resources/article/ai-governance-in-practice-report>

1. “Empowering responsible AI practices.” Microsoft. <https://www.microsoft.com/en-us/ai/responsible-ai>
2. “The Ethical Norms for the New Generation Artificial Intelligence, China.” International Research Center for AI Ethics and Governance, September 27, 2021. https://ai-ethics-and-governance.institute/2021/09/27/the-ethical-norms-for-the-new-generation-artificial-intelligence-china.
3. “Ethics of Artificial Intelligence.” UNESCO. <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>

1. ISO/IEC TR 24028:2020 Information technology/Artificial intelligence/Overview of trustworthiness in artificial intelligence. ISO. May 2020. <https://www.iso.org/standard/77608.html>
2. OECD AI Principles overview. OECD, updated May 2024. <https://oecd.ai/en/ai-principles>
3. “Privacy and AI Governance Report.” IAPP and FTI Consulting, January 2023. <https://iapp.org/resources/article/ai-governance-report-summary>
4. Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments, Updated November 7, 2023. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
5. “Responsible AI from principles to practice.” Recorded January 31, 2022. Brookings. <https://www.brookings.edu/events/responsible-ai-from-principles-to-practice>

1. Responsible AI Practices. Google. <https://ai.google/responsibility/responsible-ai-practices>
2. Tools for trustworthy AI. OECD, June 28, 2021. <https://www.oecd.org/science/tools-for-trustworthy-ai-008232ec-en.htm>

### Cloud computing

1. “Artificial Intelligence in Cloud Computing.” Datacenters.com Cloud, May 25, 2023. <https://www.datacenters.com/news/artificial-intelligence-in-cloud-computing>
2. Mohmad, Parvin. “Top 5 Ways Artificial Intelligence Impacts Cloud Computing.” Analytics Insight, February 26, 2023. <https://www.analyticsinsight.net/top-5-ways-artificial-intelligence-impacts-cloud-computing/>
3. Uslu, Kivanc. “The Role of Cloud Computing in Artificial Intelligence.” Towards Data Science, April 12, 2021. https://towardsdatascience.com/the-role-of-cloud-computing-in-artificial-intelligence-507ffd68ca46.

## Additional Resources

#### Required Materials

AI language models. OECD, April 13, 2023. https://www.oecd-ilibrary.org/science-and-technology/ai-language

models\_13d38f92-en.

Berkeley Artificial Intelligence Research. https://bair.berkeley.edu/blog.

“Human-AI Interfaces and Robotics.” The Alan Turing Institute. https://www.turing.ac.uk/research/research

programmes/artificial-intelligence-ai/robotics.

©2024, International Association of Privacy Professionals, Inc. (IAPP). Not for reproduction, distribution or republication.

“Machine Learning vs Deep Learning vs LLMs vs GenAI: Explained and How are they Different from Each Other?”

3

Cloud 4C. May 3, 2024. https://www.cloud4c.com/blogs/genai-vs-machine-learning-vs-deep-learning-vs-llms.

Rouse, Margaret. "ChatGPT." Techopedia, updated March 14, 2024.

https://www.techopedia.com/definition/34933/chatgpt.

"Topic: What is deep learning?" IBM. https://www.ibm.com/topics/deep-learning.

"Topic: What is generative AI?" IBM. https://research.ibm.com/blog/what-is-generative-AI.

"Topic: What is machine learning?" IBM. https://www.ibm.com/topics/machine-learning.

"Topic: What is Natural Language Processing (NLP)?" AWS. https://aws.amazon.com/what-is/nlp.

MODULE 1: Lesson 3

Cloudflare Resource Hub. Cloudflare. https://www.cloudflare.com/resource-hub.

IBM Technology AI Fundamentals. (YouTube playlist).

https://www.youtube.com/playlist?list=PLOspHqNVtKADfxkuDuHduUkDExBpEt3DF.

“The Internet of Things (IOT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions.”

Future of Privacy Forum, January 2019. https://fpf.org/wp-content/uploads/2019/01/2019\_01\_29

The\_Internet\_of\_Things\_and\_Persons\_with\_Disabilities\_For\_Print\_FINAL.pdf.

M

Welcome to