



AI Governance, the Short Version

A plain-English map of the AIGP syllabus: all 58 topics and 79 lessons, a few sentences each.

Danilo Stojkovic

PeritumAI | October 2026

Unofficial study material. Not affiliated with, endorsed by or produced by the IAPP. AIGP is a trademark of the International Association of Privacy Professionals.

Before you start

What this book is

This is a map, not the territory.

AI governance sounds big and scary. It's actually a set of fairly simple ideas: know what AI you have, know what can go wrong, decide who is responsible, follow the rules that apply, and keep an eye on things once the AI is running.

This book walks through every topic on the official AIGP syllabus (the IAPP's Artificial Intelligence Governance Professional certification) in a few sentences each. Read it in an evening. Afterwards you'll know what the whole field covers, which parts you already understand, and which parts need real study.

It's also the outline of a free, full course I'm building: workbook, videos and a practice trainer. Every heading here becomes a lesson there.

The short version of AI governance: AI makes guesses, at speed and at scale, from data. Governance is the set of rules, people and checks that makes sure those guesses help more than they hurt, and that someone is accountable when they don't.

How the syllabus is built

The IAPP publishes the syllabus as a "Body of Knowledge" (version 2.1, used for exams from 2 February 2026). It has three layers:

- **4 domains:** the big parts. Foundations, Laws, Development, Deployment.
- **13 competencies:** topic groups inside each domain, coded I.A, I.B and so on.
- **58 performance indicators:** the specific things you should know or be able to do, coded I.A.1, I.A.2 and so on.

In this book, every module starts with a grey box called "What the syllabus asks". It lists those 58 topics in plain words, with their codes. Then come the lessons that teach them.

The exam in one table

Item	Detail
Questions	100 in total. 85 count toward your score, 15 are unscored trial questions you can't tell apart.
Time	3 hours, per the IAPP's 2026 study guide.
Question types	Multiple choice, multi-select ("pick 3 of 5", no partial credit) and case studies, where one story has several questions.
Passing score	300 on a scale of 100 to 500.
Where	Pearson VUE test center, or online from home with a remote proctor.
Weight by domain	I Foundations 16 to 20 questions. II Laws 19 to 23. III Development 21 to 25. IV Deployment 21 to 25.

Notice the weights. More than half the exam is about the AI life cycle (Domains III and IV), not law. Many people over-study the law and under-study the practical parts.

A note on dates. The syllabus (version 2.1) was written before the 2026 changes. Since then, the EU changed the AI Act (Regulation (EU) 2026/1744), mainly by moving the high-risk deadlines later. Where it matters, this book tells you both: what the syllabus was written against, and the law as of October 2026.

Contents

Part 0. Start here	3 lessons
Part 1. Foundations of AI governance (Domain I)	14 lessons
Part 2. Laws, standards and frameworks (Domain II)	24 lessons
Part 3. Governing AI development (Domain III)	17 lessons
Part 4. Governing AI deployment and use (Domain IV)	12 lessons
Part 5. Exam preparation	9 lessons
Glossary, sources and what's next	

This is general education, not legal advice. Laws change and details vary by country and situation. Check with a qualified professional before you act. Current as of 25 October 2026.

PART 0

Start here

Three short lessons on what the AIGP is and how to study for it. No exam weight, but they save you time.

0.1 What the AIGP is, and who it's for

The AIGP is the IAPP's certification for people who govern AI: privacy and compliance people, risk managers, lawyers, product owners and career changers like me. It tests whether you understand AI well enough to manage its risks, not whether you can build it. You don't need to code.

0.2 The exam: format, scoring, booking

You buy one exam attempt, then book it within a year. Case studies are long, so practise reading fast. Multi-select questions give no partial credit, so one wrong pick means the whole question is wrong. You get your result on screen straight away.

0.3 How to study

Use the official syllabus as your checklist and tick off each of the 58 topics. The IAPP suggests at least 30 hours. Without a privacy or GRC background (GRC means governance, risk and compliance), plan for more, roughly 60 to 90. Mix reading with practice questions from the start, not only at the end.

Foundations of AI governance

What AI is, what can go wrong, who is responsible, and which policies hold it all together. This works the same way whatever your industry or company size.

16 to 20 exam questions

Module 1A. What AI is and why it needs governance

What the syllabus asks (I.A, 4 to 6 questions)

- I.A.1** Know the accepted definitions and types of AI.
- I.A.2** Spot the risks and harms AI can cause to people, groups, organizations and society.
- I.A.3** Explain what makes AI different enough to need its own governance.
- I.A.4** Know and apply the common principles of responsible AI.

1.1 What counts as AI

There's no single definition, but the big ones agree. The OECD (Organisation for Economic Co-operation and Development, a club of mostly rich countries) describes an AI system as a machine-based system that, for explicit or implicit goals, infers from its input how to produce outputs like predictions, content, recommendations or decisions. The EU AI Act (Article 3) uses almost the same words. ISO 22989 is the official vocabulary standard, and it's free.

The key word is "infers". A calculator follows fixed rules. An AI system works out its answer from patterns.

Syllabus: I.A.1

1.2 AI for non-engineers (1): how machine learning works

Machine learning means the system learns from examples instead of being told the rules. You feed it data (training), it adjusts millions of internal settings (parameters), and the result is a model. Using the model on new data is called inference.

Learning styles you should recognize: supervised (examples come with the right answers), unsupervised (the system finds groups on its own) and reinforcement learning (it learns by trial, reward and penalty).

Syllabus: I.A.1 (also supports Domains III and IV)

1.3 AI for non-engineers (2): generative AI and agents

Generative AI creates new content: text, images, audio, code. Large language models (LLMs) like ChatGPT or Claude predict the next word, very well, based on huge amounts of training text. That's why they sound confident even when they're wrong. A wrong but confident answer is called a hallucination.

Foundation models are big general models that others build on. Agents go one step further: they don't just answer, they take actions using tools, like sending an email or updating a database.

Syllabus: I.A.1 (also supports IV.A)

1.4 Risks and harms

Think in four circles. Individuals can be denied a job or a loan unfairly, or have their privacy invaded. Groups can be systematically disadvantaged, for example by a hiring model that learned old biases. Organizations face lawsuits, fines, security breaches and lost trust. Society faces misinformation, damage to democracy, environmental cost and job disruption.

The syllabus names three risk sources to remember: the AI doesn't do what you intended (misalignment), ethics and bias problems, and complexity and scale.

Syllabus: I.A.2

1.5 Why AI is different from normal software

Normal software does exactly what it's coded to do. AI is different in ways that make old controls not enough:

- **Opacity:** it's often hard to see why it gave an answer (the "black box").
- **Autonomy:** it can act with little human input.
- **Speed and scale:** one mistake repeats a million times.
- **Data dependency:** bad data in, bad decisions out.
- **Probabilistic outputs:** ask the same question twice and you may get two different answers.

Add complexity and the potential for misuse, and you have the case for dedicated AI governance.

Syllabus: I.A.3

1.6 Principles of responsible AI

Every major framework lists similar principles. The syllabus uses six: fairness, safety and reliability, privacy and security, transparency and explainability, accountability, and human-centricity (AI should serve people, not the other way round).

You'll see versions of these in the OECD AI Principles, the EU's 2019 Ethics Guidelines for Trustworthy AI (seven requirements) and UNESCO's 2021 Recommendation. "Explainable" in exam language means a human can understand the system's inputs, outputs and how it works.

Syllabus: I.A.4

Module 1B. Setting organizational expectations

What the syllabus asks (I.B, 5 to 7 questions)

- I.B.1** Define roles and responsibilities for AI governance.
- I.B.2** Build cross-functional collaboration into the program.
- I.B.3** Create and deliver AI training and awareness for everyone involved.
- I.B.4** Tailor the approach to company size, maturity, industry and risk tolerance.
- I.B.5** Tell developers, providers, deployers and users apart.

1.7 Who does what

Good governance means every AI system has a named owner. Typical setup: the board sets how much risk is acceptable, a senior executive owns the program, an AI governance committee approves risky use cases, system owners run the day-to-day, and internal audit checks it all works. Many companies borrow the "three lines" model: the business manages the risk, risk and compliance teams oversee, audit checks independently.

Syllabus: I.B.1

1.8 Cross-functional by design

No single team can govern AI alone. Legal knows the rules, privacy knows the data, security knows the threats, data scientists know the models, HR knows the people impact, and the business knows the goal. Bring them together early. Different backgrounds also catch different blind spots, which is the point.

Syllabus: I.B.2

1.9 Training and AI literacy

People can't follow rules they don't understand. Training should fit the audience: basic awareness for all staff, deeper training for builders and reviewers, risk and strategy for leaders.

In the EU this is now law. The AI Act (Article 4) has required AI literacy measures since February 2025. Since the 2026 amendment, providers and deployers must take measures to support the AI literacy of their staff and others using AI on their behalf. It doesn't require a specific level or certificate.

Syllabus: I.B.3

1.10 One size doesn't fit all

A 15-person startup and a global bank both need AI governance, but not the same kind. Size, maturity, industry, products, goals and risk tolerance shape how formal it gets. A small firm might have one accountable person, a short AI use policy and a simple register. A bank will have committees, model risk teams and regulators asking questions. The exam likes questions where you pick the approach that fits the company described.

Syllabus: I.B.4

1.11 Developers, providers, deployers, users

A developer builds the AI. A provider puts it on the market under its own name. A deployer uses it in its own business. A user is the person actually interacting with it. One company can play several roles at once.

The difference matters because duties follow the role. Under the EU AI Act, providers carry most of the heavy duties. Most companies are deployers. The IAPP uses these labels to describe tasks, not to assign blame.

Syllabus: I.B.5

Module 1C. Policies across the AI life cycle

What the syllabus asks (I.C, 6 to 8 questions)

I.C.1 Create policies for oversight and accountability at every life cycle stage.

I.C.2 Update existing policies (privacy, security, data governance, IP) for AI.

I.C.3 Manage third-party risk with policies, assessments and contracts.

1.12 Policies for the whole life cycle

The AI life cycle runs from idea to retirement: use case review, risk management, ethics by design, getting and using data, building, training and testing, deployment and monitoring, documentation and reporting, and incident handling. Each stage needs a rule that says what must happen and who signs off. Without that, decisions get made by whoever happens to be in the room.

Syllabus: I.C.1

1.13 Update what you already have

You don't start from zero. Your privacy, security, data governance and intellectual property policies already exist. They just weren't written with AI in mind. Ask of each: does it cover data used for training? Staff pasting company data into chatbots? Who owns AI-generated content? Usually a few added clauses do more than a brand-new policy.

Syllabus: I.C.2

1.14 Third-party AI risk

Most AI you use comes from someone else, so their risk becomes yours. Cover it in four places: procurement (ask vendors the right questions before buying), the supply chain (models, data and services underneath the product), HR (AI in hiring, and staff using AI tools) and an acceptable use policy that tells staff which AI tools are allowed and what they may put into them. That last one tackles "shadow AI": tools people use without anyone approving them.

Syllabus: I.C.3

Laws, standards and frameworks

The rules that already apply to AI (privacy, IP, discrimination, consumer protection, product liability), the new AI-specific laws, and the voluntary frameworks most programs are built on.

19 to 23 exam questions

Remember: AI isn't a legal vacuum. Long before AI laws arrived, privacy, anti-discrimination and consumer protection laws already applied to it. Most AI enforcement so far has come from these older laws.

Module 2A. Privacy law applied to AI

What the syllabus asks (II.A, 4 to 6 questions)

II.A.1 Apply transparency, choice, lawful basis and purpose limitation to AI.

II.A.2 Apply data minimization and privacy by design to AI.

II.A.3 Apply controller duties: impact assessments, processors, transfers, data subject rights, automated decisions, incidents, breach notice, records.

II.A.4 Handle sensitive data, such as biometrics.

2.1 Transparency, choice, lawful basis, purpose

People must be told when their personal data feeds an AI system and why (transparency). Where the law requires it, they get a say (choice). Under the GDPR, the EU's privacy law, every use of personal data needs a legal reason, such as consent or "legitimate interest" (Article 6). Data collected for one purpose can't just be reused to train a model for another (purpose limitation). The EDPB, the group of EU privacy regulators, explained how this works for AI models in Opinion 28/2024.

Syllabus: II.A.1

2.2 Data minimization and privacy by design

AI wants as much data as possible. Privacy law says use only what you need. Those two pull against each other, and governance is where you settle it. Privacy by design (GDPR Article 25) means building protection in from the start: removing names, using fake but realistic (synthetic) data, limiting access, and deleting data when you no longer need it.

Syllabus: II.A.2

2.3 Controller duties (1): assessments, vendors, transfers, records

The controller is whoever decides why and how personal data is used. Their AI-related duties include a DPIA (data protection impact assessment) for high-risk processing (GDPR Article 35), which AI often triggers; a proper contract with every processor, including AI vendors (Article 28); safeguards when data leaves the EU, such as standard contractual clauses; and records of processing (Article 30).

Syllabus: II.A.3

2.4 Controller duties (2): rights, automated decisions, breaches

People can ask to see, correct or delete their data. With a trained model that's genuinely hard, and the exam knows it. GDPR Article 22 gives people the right not to be subject to decisions made solely by automation that have legal or similarly significant effects, like an automatic loan refusal, with some exceptions and safeguards. California's privacy regulator has adopted its own rules on automated decision-making technology. Breaches must usually be reported to the regulator within 72 hours (GDPR Article 33).

Syllabus: II.A.3

2.5 Sensitive data and biometrics

Some data gets extra protection: health, ethnicity, religion, sexual orientation, and biometrics such as face and fingerprint data (GDPR Article 9 calls these "special categories"). AI can also infer sensitive facts from harmless-looking data, which counts too. In the US, Illinois' biometric privacy law (BIPA) has led to large lawsuits. The EU AI Act bans some biometric uses outright.

Syllabus: II.A.4

Module 2B. Other laws that already apply

What the syllabus asks (II.B, 4 to 6 questions)

- II.B.1 Intellectual property law and AI, such as limits on training data.
- II.B.2 Nondiscrimination law in jobs, credit, lending, housing and insurance.
- II.B.3 Consumer protection law, such as bans on unfair and deceptive practices.
- II.B.4 Product liability law, such as design and manufacturing defects.

2.6 Intellectual property

Three questions keep coming up. Can you train on copyrighted material? In the EU, text and data mining is allowed unless the rights holder has opted out (DSM Copyright Directive, Article 4), and the AI Act requires general-purpose model providers to have a policy that respects those opt-outs. Who owns AI output? The US Copyright Office says copyright needs human authorship. And watch for trade secrets leaking into prompts.

Syllabus: II.B.1

2.7 Nondiscrimination

If a human couldn't legally make a decision based on race, sex or age, neither can an AI. Existing anti-discrimination laws cover employment, credit, lending, housing and insurance. In US credit, lenders must give specific reasons when they deny someone, even if a complex model made the call. New York City's Local Law 144 requires bias audits of automated hiring tools.

Syllabus: II.B.2

2.8 Consumer protection

Laws against unfair and deceptive practices apply to AI products and to AI claims. In the US, the FTC (Federal Trade Commission) uses Section 5 of the FTC Act to go after companies that exaggerate what their AI can do ("AI washing") or use AI in harmful ways. The EU's Unfair Commercial Practices Directive plays a similar role. Simple rule: don't promise what the AI can't do.

Syllabus: II.B.3

2.9 Product liability

If a product is defective and hurts someone, the maker can be liable. The question is whether AI counts as a product. In the EU, the new Product Liability Directive (2024/2853) says yes: software, including AI, is covered. Defects can come from design, manufacturing, or failing to warn. The EU dropped a separate AI Liability Directive proposal in 2025, so the general rules carry the load.

Syllabus: II.B.4

Module 2C. AI-specific laws

What the syllabus asks (II.C, 6 to 8 questions)

- II.C.1** The risk classes (prohibited, high, limited, minimal) and what falls into each.
- II.C.2** Key duties: risk management, data governance, technical documentation, conformity and impact assessments, record keeping.
- II.C.3** Key duties: human oversight, transparency and notices, quality management.
- II.C.4** The separate rules for general-purpose AI models.
- II.C.5** Enforcement and penalties.
- II.C.6** How duties differ for providers, deployers, importers and distributors.

2.10 The EU AI Act in one page

The EU AI Act (Regulation (EU) 2024/1689) is the world's first broad AI law. It entered into force on 1 August 2024. It regulates by risk: the more harm an AI use can cause, the more rules apply. It also reaches companies outside the EU if their AI is sold or used in the EU.

Date	What applies (law as of October 2026)
2 Feb 2025	Banned practices and the AI literacy duty
2 Aug 2025	General-purpose AI model rules, governance bodies, penalties
2 Aug 2026	Most of the rest, including transparency duties (Article 50)
2 Dec 2026	New bans added in 2026 (sexual deepfakes of real people without consent, AI-generated child sexual abuse material)
2 Dec 2027	High-risk rules for Annex III uses (jobs, credit, education and others)
2 Aug 2028	High-risk rules for AI inside regulated products (Annex I)

The syllabus was written before the 2026 amendment. In the original Act, the high-risk dates were 2 August 2026 (Annex III) and 2 August 2027 (Annex I). Know both.

Syllabus: II.C (all)

2.11 The risk classes

Prohibited (Article 5): uses too harmful to allow, such as social scoring, manipulative techniques that cause harm, exploiting vulnerable people, emotion recognition at work or school, untargeted scraping of faces, and most real-time facial recognition by police in public.

High-risk (Article 6): AI that is a safety part of regulated products (Annex I), and AI used in sensitive areas (Annex III) such as hiring, credit, education, essential services, law enforcement, migration and justice. Some Annex III systems escape if they only do narrow, low-impact tasks.

Limited risk (Article 50): transparency duties, like telling people they're talking to a chatbot and marking AI-generated content. **Minimal risk**: everything else, like spam filters. No new duties.

Syllabus: II.C.1

2.12 High-risk duties (1): risk, data, documents, logs

Providers of high-risk AI need a risk management system that runs for the system's whole life (Article 9), good data governance for training and testing data (Article 10), detailed technical documentation (Article 11 and Annex IV), and automatic logs so events can be traced later (Article 12).

Syllabus: II.C.2

2.13 High-risk duties (2): checks, oversight, quality

Before going to market, a high-risk system needs a conformity assessment, which is a check that it meets the rules (Article 43). For most Annex III systems, the provider does this itself. Then come the CE mark and registration in an EU database. The system must allow human oversight (Article 14), come with clear instructions for use (Article 13), be accurate, robust and secure (Article 15), and sit inside a quality management system (Article 17). Some deployers, such as public bodies and those scoring credit or pricing life and health insurance, must do a fundamental rights impact assessment (FRIA) first (Article 27).

Syllabus: II.C.2, II.C.3

2.14 General-purpose AI models

General-purpose AI (GPAI) models, like the big LLMs, have their own chapter. All GPAI providers must keep technical documentation, give information to companies building on their model, have a copyright policy, and publish a summary of their training content (Article 53). Models with "systemic risk", presumed for the very largest training runs, must also run evaluations and adversarial testing, report serious incidents and keep strong cybersecurity (Article 55). A voluntary Code of Practice, published in July 2025, shows one way to comply.

Syllabus: II.C.4

2.15 Who carries which duties

Providers carry the most (Article 16). Deployers must use the system as instructed, assign competent human oversight, monitor it and keep its logs (Article 26). Importers and distributors check that the paperwork and CE mark are in place before passing it on (Articles 23 and 24).

The trap: you become a provider if you put your name on someone else's high-risk system, change it substantially, or use it for a high-risk purpose it wasn't meant for (Article 25).

Syllabus: II.C.6

2.16 Enforcement and penalties

National market surveillance authorities enforce most of the Act. The EU's AI Office supervises general-purpose AI models. Maximum fines (Article 99):

- Banned practices: up to EUR 35 million or 7% of worldwide yearly turnover, whichever is higher.
- Most other duties: up to EUR 15 million or 3%.
- Misleading information to authorities: up to EUR 7.5 million or 1%.

For small and medium companies, the lower of the two amounts applies. Since the 2026 amendment, small mid-cap companies also get the lower amount for the EUR 15 million and EUR 7.5 million tiers. These are maximums. Real fines depend on how serious the breach was.

Syllabus: II.C.5

2.17 South Korea's AI Basic Act

South Korea's AI Basic Act took effect on 22 January 2026, making it the second broad national AI law after the EU's. It focuses on "high-impact" AI in areas like health, energy, hiring and lending, with duties such as risk management, explanations and human oversight. It also requires notice and labelling for generative AI, and larger foreign companies must appoint a local representative. Reported penalties are far smaller than the EU's.

Syllabus: II.C (all)

2.18 The United States: a patchwork

The US has no broad federal AI law. At federal level, policy comes through executive orders and agencies enforcing existing laws. The real action is in the states: Colorado's AI law on automated "consequential decisions" (the original 2024 AI Act was repealed and replaced in May 2026 by a narrower law, SB 26-189, which takes effect on 1 January 2027), Texas' Responsible AI Governance Act, Utah's AI disclosure rules, California's frontier-model law (SB 53) and its rules on automated decisions, Illinois' rules on AI in hiring, and New York City's Local Law 144.

US AI law changes month to month, and federal moves to override state laws are part of the picture. Check the current status before relying on any date here.

Syllabus: II.C (all)

2.19 Comparing the laws

The EU is broad and detailed, with high fines. South Korea is a lighter framework law. The US is sector-by-sector and state-by-state. Underneath, they share the same ideas: sort AI by risk, do more where harm is likely, be transparent, keep humans in control, and document what you did. Learn the shared core and you can read any new AI law quickly.

Syllabus: II.C (all)

Module 2D. Standards and frameworks

What the syllabus asks (II.D, 3 to 5 questions)

II.D.1 The OECD principles and recommendations for trustworthy AI.

II.D.2 The NIST AI Risk Management Framework and Playbook.

II.D.3 The core ISO AI standards: 22989, 42001 and 42005.

2.20 The OECD AI Principles

Adopted in 2019 and updated in 2024, these were the first intergovernmental AI principles, and many laws borrow from them. Five principles for trustworthy AI: inclusive growth and well-being; respect for the rule of law, human rights and democratic values, including fairness and privacy; transparency and explainability; robustness, security and safety; and accountability. Five recommendations for governments: invest in research, build an inclusive AI ecosystem, create enabling and interoperable policy, build skills and prepare for job changes, and cooperate internationally.

Syllabus: II.D.1

2.21 NIST AI RMF (1): trustworthy AI, Govern and Map

The NIST AI Risk Management Framework (AI RMF 1.0, January 2023) is a free, voluntary US framework used worldwide. It describes seven characteristics of trustworthy AI: valid and reliable; safe; secure and resilient; accountable and transparent; explainable and interpretable; privacy-enhanced; and fair, with harmful bias managed.

Its core has four functions. **Govern** runs through everything: culture, policies, roles. **Map** sets the context: what the system is for, who it affects, what could go wrong.

Syllabus: II.D.2

2.22 NIST AI RMF (2): Measure, Manage, Playbook, GenAI profile

Measure tests and tracks the risks with metrics. **Manage** decides what to do about them: prioritize, respond, monitor, handle third parties. Each function splits into categories and subcategories.

The Playbook gives suggested actions for each subcategory. It's not a checklist. The Generative AI Profile (NIST AI 600-1, July 2024) applies the framework to generative AI and lists 12 risks, including confabulation (NIST's word for hallucination), harmful bias, data privacy, information security, intellectual property and dangerous content.

Syllabus: II.D.2

2.23 ISO 22989 and ISO 42001

ISO 22989 is the dictionary: shared AI terms and concepts, so everyone means the same thing. ISO 42001 (published December 2023) is the AI management system standard, and companies can be certified against it. If you know ISO 27001 for security, the shape is familiar: the same main clauses (context, leadership, planning, support, operation, performance evaluation, improvement) plus an annex of AI-specific controls. It also asks for AI system impact assessments.

Syllabus: II.D.3

2.24 ISO 42005 and how it all fits

ISO 42005 (2025) is guidance on how to do an AI system impact assessment: who and what to consider, and how to document it. How they fit together: laws like the AI Act say what you must achieve, ISO 42001 gives you a certifiable system to manage it, NIST gives you a practical risk process, and OECD gives you the shared values underneath. Many programs use all four.

Syllabus: II.D.3

Governing AI development

What governance looks like while an AI system is designed, built, trained, tested and maintained. You don't need to code. You need to know which questions to ask at each step, and what evidence to expect.

21 to 25 exam questions

Module 3A. Design and build

What the syllabus asks (III.A, 6 to 8 questions)

- III.A.1 Define the business context and use case.
- III.A.2 Perform or review an impact assessment.
- III.A.3 Apply policies and ethics to design choices.
- III.A.4 Identify and manage design and build risks.
- III.A.5 Document the design and build process.

3.1 Start with the use case

Before anyone builds, answer the basics. What problem are we solving? Why AI, and not a simpler tool? What does success look like? Who will it affect? A short intake form plus a quick risk triage at this stage stops bad ideas cheaply, and sends the risky ones to deeper review.

Syllabus: III.A.1

3.2 AI impact assessments

An impact assessment asks one main question: what are the possible benefits and harms of this system, and to whom? Do it before building, and update it when the system changes. It's broader than a DPIA, which covers privacy only, and different from the EU's FRIA, which is a legal duty for certain deployers. Free templates and examples: Canada's Algorithmic Impact Assessment tool and the EU's ALTAI checklist.

Syllabus: III.A.2

3.3 Governance in design choices

Design is where most risk gets decided. Key choices: the exact purpose and requirements; architecture and model choice, where a simpler, more explainable model is sometimes the better one; how humans stay in control, either approving each decision ("in the loop") or supervising and able to step in ("on the loop"); which metrics and thresholds count as good enough, set before you see the results; feedback from affected stakeholders; and operational controls.

Syllabus: III.A.3

3.4 Risk tools

Common tools from the syllabus:

- **Probability and severity matrix:** how likely is the harm, and how bad would it be?
- **Mitigation hierarchy:** avoid the risk first, then reduce it, and only then accept or transfer what's left.
- **Stakeholder mapping:** who is affected, and how much say do they get?
- **Benchmarking, pilots and pre-deployment testing:** try it small before going big.

"Don't build it" is always an option.

Syllabus: III.A.4

3.5 Document as you go

If it isn't written down, it didn't happen, at least as far as a regulator or auditor is concerned. Record decisions, the options you rejected and why, risk assessments and sign-offs. For high-risk AI under the EU AI Act, Annex IV lists what the technical documentation must contain.

Syllabus: III.A.5

Module 3B. Data, training and testing

What the syllabus asks (III.B, 6 to 8 questions)

- III.B.1** Set and follow data governance requirements: rights to use the data, quality, quantity, integrity, fit for purpose.
- III.B.2** Establish and document data lineage and provenance.
- III.B.3** Plan and run training and testing (unit, integration, validation, performance, security, bias, interpretability).
- III.B.4** Manage issues and risks during training and testing.
- III.B.5** Document training and testing.

3.6 Data governance for AI

First: do we have the right to use this data for this purpose? Check consent, licences and website terms. Then: is it good enough? That means accurate, complete, representative of the people the system will affect, big enough, unchanged since collection (integrity), and actually suited to the task. The EU AI Act sets data quality duties for high-risk systems in Article 10.

Syllabus: III.B.1

3.7 Lineage and provenance

Provenance is where data came from. Lineage is everything that happened to it on the way: cleaning, merging, labelling. Together they let you answer "why did the model learn this?" and prove you had the right to use the data. A well-known format is the "datasheet for datasets": a short standard description of a dataset's origin, contents and limits.

Syllabus: III.B.2

3.8 Types of testing

- **Unit and integration tests:** do the parts work, alone and together?
- **Validation:** does the model work on data it never saw in training?
- **Performance:** how accurate is it, measured the right way for the task?
- **Security:** can attackers fool it, poison it or extract data from it?
- **Bias:** does it treat groups fairly?
- **Interpretability:** can we tell which factors drove a result?

Syllabus: III.B.3

3.9 Bias and fairness testing

Bias usually comes from the data: history (past unfair decisions), sampling (some groups missing) or measurement (the wrong thing measured). It can hide behind proxies. A postcode can stand in for ethnicity. There are several mathematical definitions of fairness, and you usually can't satisfy all of them at once. So pick the definition that fits the context, and write down why.

Syllabus: III.B.3, III.B.4

3.10 What goes wrong in training and testing

Common problems: overfitting (the model memorizes training data and fails in real life), data leakage (test answers sneak into training, so results look better than they are), poisoning (someone corrupts the training data on purpose), imbalanced data (too few examples of some cases), bad labels, and for generative AI, hallucinations. Governance makes sure someone looks for these before release, not after.

Syllabus: III.B.4

3.11 Documenting training and testing

Write down the test plan, the data used, the results, known limits and who approved going ahead. The aim is that someone else could repeat the tests and get the same results. This record is your evidence for audits, conformity assessments and any later dispute.

Syllabus: III.B.5

Module 3C. Release, monitoring and maintenance

What the syllabus asks (III.C, 8 to 10 questions)

- III.C.1** Check readiness for release (model card, conformity).
- III.C.2** Monitor continuously and schedule maintenance, updates and retraining.
- III.C.3** Run periodic checks: audits, red teaming, threat modeling, security testing.
- III.C.4** Manage and document incidents, issues and risks.
- III.C.5** Work out with others why AI incidents happen.
- III.C.6** Make public disclosures to meet transparency duties.

3.12 Ready for release?

Agree on go/no-go criteria before testing ends, so nobody moves the goalposts. A model card is a short fact sheet for a model: what it's for, how well it performs across different groups, and its known limits. For high-risk AI in the EU, release also means a finished conformity assessment. Release in stages where possible.

Syllabus: III.C.1

3.13 Monitoring and maintenance

AI can get worse without anyone touching it. Data drift: the inputs change, like new customer types. Concept drift: the world changes, so old patterns stop being true. Monitor performance, data quality, drift, speed (latency) and computing cost. Set a schedule for updates and retraining, and test again after every change.

Syllabus: III.C.2 (also IV.C.2)

3.14 Audits, red teaming and security testing

Audits check the system against rules and policy. Red teaming means people deliberately trying to break it or make it misbehave. Threat modeling maps how an attacker might go after it. Good free references: the OWASP Top 10 for LLM applications (including prompt injection, where hidden instructions trick the model) and MITRE ATLAS, a catalogue of real attacks on AI.

Syllabus: III.C.3 (also IV.C.3)

3.15 Incidents and issues

Decide in advance what counts as an AI incident, who gets told, and how fast. Then: contain it, investigate, fix it, learn from it, and record everything. Under the EU AI Act, providers of high-risk AI must report serious incidents to authorities (Article 73). Deadlines are tight: usually within 15 days, and much shorter in the most serious cases.

Syllabus: III.C.4

3.16 Why AI incidents happen

Typical root causes from the syllabus: brittleness (the system fails on slightly unusual input), lack of robustness, poor-quality data, testing that wasn't thorough enough, and model or data drift. Finding the real cause takes several teams, because the data people, the model people and the business people each see part of the picture.

Syllabus: III.C.5

3.17 Public disclosures

Transparency doesn't end at launch. Providers share technical documentation with authorities, give deployers clear instructions for use, and keep a post-market monitoring plan: a plan for watching how the system behaves in real use (EU AI Act Articles 13 and 72). Some high-risk systems must also be registered in a public EU database.

Syllabus: III.C.6

Governing AI deployment and use

Choosing an AI system, assessing it, putting it to work and keeping it under control. This applies whether you built the model yourself or bought it. Most companies live here.

21 to 25 exam questions

Module 4A. Deciding to deploy

What the syllabus asks (IV.A, 6 to 8 questions)

IV.A.1 Understand the use case context: goals, performance, data, ethics, workforce readiness.

IV.A.2 Understand the differences between AI model types.

IV.A.3 Understand the deployment options and techniques.

4.1 The use case context

Before deploying, check five things. The business goal. The performance you actually need. Whether you have the right data. The ethical questions. And whether your people are ready, which is the one most often forgotten. Do they have the skills, will the AI change their jobs, and will they trust it too much or too little?

Syllabus: IV.A.1

4.2 Model types

- **Classic vs generative:** classic AI predicts or sorts (fraud yes/no). Generative AI creates content.
- **Proprietary vs open:** closed models you rent through a vendor, or open models you can download and run yourself. Open gives you control, but more responsibility.
- **Small vs large:** small models are cheaper, faster and can run on a device. Large ones are more capable but cost more.
- **Language vs multimodal:** text only, or also images, audio and video.

Syllabus: IV.A.2

4.3 Deployment options

Where it runs: in the cloud, on your own servers (on-premise), or on the device itself (edge). Each trades control, cost and data exposure differently. How you adapt it: use it as is; fine-tune it on your data; use RAG (retrieval augmented generation), where the model looks things up in your documents before answering; or build agents that take actions. Agents need the most care: limited permissions, human approval for important steps, and full logs.

Syllabus: IV.A.3

Module 4B. Assessing the system

What the syllabus asks (IV.B, 5 to 7 questions)

- IV.B.1** Perform or review an impact assessment on the chosen system.
- IV.B.2** Identify and evaluate key terms and risks in vendor and licensing agreements.
- IV.B.3** Understand the extra risks and opportunities of deploying your own model.

4.4 Assessing a system you bought

Buying AI doesn't mean buying away the risk. The vendor's assessment covers their product in general. Yours covers your use: your data, your users, your context. Ask the vendor for documentation, test results and limits, then assess the impact in your own setting. Some EU deployers also need a FRIA.

Syllabus: IV.B.1

4.5 Vendor and licence agreements

Read the contract for the AI-specific points. Will they train on your data? Who owns the outputs, and will they defend you if someone claims your output infringes their rights (indemnity)? Are their liability caps realistic? Do you get performance commitments, audit rights, documentation and incident notices? Will they tell you before they change the model? What happens to your data when you leave? The EU has published model contract clauses for buying AI that help here.

Syllabus: IV.B.2

4.6 Running your own model

Building or hosting your own model gives you control over data, cost and features, and can set you apart from competitors. But you take on the duties a vendor would carry. Under the EU AI Act you may become a provider, with a heavier legal load and more liability. You also need the skills to run it. Pick this path on purpose, not by accident.

Syllabus: IV.B.3

Module 4C. Governing deployment and use

What the syllabus asks (IV.C, 9 to 11 questions, the biggest group)

- IV.C.1** Apply policies and ethics to deployment: data governance, risk and issue management, user training.
- IV.C.2** Monitor continuously and schedule maintenance, updates and retraining.
- IV.C.3** Run periodic checks: audits, red teaming, threat modeling, security testing.
- IV.C.4** Document incidents, issues, risks and post-market monitoring plans.
- IV.C.5** Predict and reduce secondary uses and downstream harms.
- IV.C.6** Set up external communication plans.
- IV.C.7** Create a policy and controls to switch off or limit an AI system when needed.

4.7 Policies in daily use

Deployment is where policy meets real people. Set what data users may put into the system, how risks and issues get reported and handled, and what training users need before they start. Clear, short rules beat long documents nobody reads.

Syllabus: IV.C.1

4.8 Monitoring after go-live

The same ideas as 3.13 and 3.14, seen from the user's side. Watch outputs and user complaints. Notice when a vendor update changes how the system behaves. Run periodic reviews. EU deployers of high-risk AI must monitor the system and keep its logs, generally for at least six months (Article 26).

Syllabus: IV.C.2, IV.C.3

4.9 Incidents and post-market monitoring

Keep an issue and incident register. When something goes wrong, deployers usually tell the provider, and in serious cases the authorities. A post-market monitoring plan sets out what you watch, how often, and what triggers action. Documented, so you can show it.

Syllabus: IV.C.4

4.10 Secondary uses and downstream harms

AI tends to get used for things it wasn't approved for. That's called function creep. Say a tool bought to summarize meetings starts being used to rate employees. That's a new and riskier use. Predict likely misuse, set purpose limits, control access, and review uses regularly. Also think about harm further down the line, to people who never touch the system.

Syllabus: IV.C.5

4.11 Talking to the outside world

Plan in advance what you say, to whom, and when. Customers need to know when they're dealing with AI. Regulators may need reports. When something goes wrong, the media and the public need a clear, honest message, prepared before the crisis rather than during it.

Syllabus: IV.C.6

4.12 The off switch

Every AI system needs a way to stop it. Decide in advance who can switch it off, under what conditions, and what happens next: a backup manual process, a rollback to an earlier version, or limiting it to certain countries ("localizing"), for example when one country's law changes. Test that it works before you need it.

Syllabus: IV.C.7

Exam preparation

Turning knowledge into points. No new topics here, just practice and strategy.

5.1 Reading case studies and multi-select questions

Case studies are long stories with several questions attached. Read the question first, then go back to the story for the facts it needs. Look for role words (provider or deployer?), location (EU, US state, Korea?) and risk signals (hiring, credit, children). For multi-select, check each option on its own: no partial credit means one wrong pick costs the whole question.

5.2 to 5.6 Five worked case studies

One worked example per common scenario: an AI hiring tool, a credit decision model, a customer service chatbot built on generative AI, an AI tool in healthcare, and an AI agent that takes actions on its own. Each one walks through roles, applicable laws, risks, controls and what to document.

5.7 and 5.8 Two full mock exams

100 questions each, timed, in the real format, with a review of every answer. Treat the first one as a diagnosis and the second as a dress rehearsal. Your weak areas by competency tell you what to revisit.

5.9 The last week

Stop learning new things. Revisit your weakest competencies, reread your notes on the EU AI Act roles and the NIST functions, sleep properly, and check your setup if you're testing from home. You've done the work.

Glossary

The terms you'll meet most often, in plain words.

AI system

A machine-based system that works out from its input how to produce outputs like predictions, content, recommendations or decisions.

AI governance

The rules, roles and checks that keep AI useful, lawful and safe, with someone accountable.

Agent (agentic AI)

AI that takes actions using tools, not just answers questions.

Bias (harmful)

Systematically unfair results for some people or groups.

Conformity assessment

The check that a high-risk AI system meets the EU AI Act before it goes on the market.

Controller / processor

Privacy law roles. The controller decides why and how data is used. The processor handles data on the controller's behalf.

Deployer

An organization using an AI system in its own work (EU AI Act).

DPIA

Data protection impact assessment: a privacy risk check required for high-risk processing.

Drift

When real-world data or patterns change, so the model gets worse over time.

Explainability

Humans can understand a system's inputs, outputs and how it works.

Fine-tuning

Extra training of an existing model on your own data.

Foundation model / GPAI model

A large general model that many applications are built on.

FRIA

Fundamental rights impact assessment: required by the EU AI Act for certain deployers of high-risk AI.

Hallucination (confabulation)

A confident answer that is false.

High-risk AI

AI in sensitive uses or safety components that carries the strictest EU AI Act duties.

Human oversight

Competent people who can understand, check and stop an AI system.

Impact assessment

A structured look at the likely benefits and harms of an AI system, and to whom.

Inference

A trained model producing an answer from new input.

LLM

Large language model: generative AI trained on huge amounts of text.

Model card

A short fact sheet on a model's purpose, performance and limits.

Post-market monitoring

Watching how an AI system behaves in real use after release.

Prompt injection

Hidden instructions that trick a model into doing something it shouldn't.

Provider

An organization that puts an AI system or model on the market under its own name (EU AI Act).

RAG

Retrieval augmented generation: the model looks things up in your documents before answering.

Red teaming

Deliberately trying to break or misuse a system to find weaknesses first.

Shadow AI

AI tools staff use without approval.

Training data

The examples a model learns from.

Sources

Official sources first. All accessed October 2026.

- IAPP, AIGP Body of Knowledge and Exam Blueprint, version 2.1, effective 2 February 2026. iapp.org/certify/aigp
- IAPP, AIGP Study Guide, effective February 2026.
- Regulation (EU) 2024/1689 (EU AI Act), consolidated text of 27 July 2026, including Regulation (EU) 2026/1744. eur-lex.europa.eu
- Regulation (EU) 2016/679 (GDPR). eur-lex.europa.eu
- Directive (EU) 2019/790 (DSM Copyright Directive) and Directive (EU) 2024/2853 (Product Liability Directive). eur-lex.europa.eu
- OECD, Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449), revised 3 May 2024, and Explanatory memorandum on the updated OECD definition of an AI system (2024).
- NIST AI 100-1, AI Risk Management Framework 1.0 (2023); NIST AI RMF Playbook; NIST AI 600-1, Generative AI Profile (2024).
- EU High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI (2019) and ALTAI (2020).
- UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).
- ISO/IEC 22989:2022, ISO/IEC 42001:2023, ISO/IEC 42005:2025 (official ISO summaries).
- EDPB Opinion 28/2024 on AI models; New York City Local Law 144 of 2021; California CCPA and CPPA regulations.
- South Korea, Framework Act on AI (AI Basic Act), effective 22 January 2026 (English translation by Georgetown CSET).

What's next

This book is the map. The full course is the journey.

I'm building a free, complete AIGP prep course at PeritumAI: a lesson for every heading in this book, with a workbook page, a short video and practice questions in a free web trainer, including case studies and multi-select questions in the real exam format.

If you want it when it launches, find me on LinkedIn (Danilo Stojkovic) or at peritumai.com.

Unofficial study material. Not affiliated with, endorsed by or produced by the IAPP. AIGP is a trademark of the International Association of Privacy Professionals. This is general education, not legal advice. Current as of 25 October 2026.