1. Record Nr. UNINA9911058126103321

Autore	Gregory Peter H
Titolo	IAPP AIGP Artificial Intelligence Governance Professional Study Guide
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2026 ©2026
ISBN	1-394-36395-8 1-394-36397-4 1-394-36396-6
Edizione	[1st ed.]
Descrizione fisica	1 online resource (481 pages)
Collana	Sybex Study Guide Series
Soggetti	Artificial intelligence - Examinations Artificial intelligence - Law and legislation Computer security - Examinations Study guides
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Half Title Page -- Title Page -- Copyright -- Acknowledgments -- About the Author -- About the Technical Editor -- Contents at a Glance -- Contents -- Introduction -- Assessment Test -- Answers to Assessment Test -- Part I: Foundations of AI and Governance -- Chapter 1: AI and AI Governance -- The Types of AI -- Definition of AI -- AI Capabilities -- AI Functionalities -- AI Techniques -- Risks and Harms Posed by AI -- Risks and Harms to Individuals -- Risks and Harms to Groups -- Risks and Harms to Organizations -- Risks and Harms to Society -- Characteristics of AI Requiring Governance -- Complexity -- Opacity -- Autonomy -- Speed and Scale -- Potential for Harm and Misuse -- Data Dependency -- Privacy -- Intellectual Property -- Probabilistic vs. Deterministic Outputs -- Principles of Responsible AI -- Ethics -- Challenges with Ethics -- Applications of Ethics -- Fairness -- Challenges with Fairness -- Applications of Fairness -- Safety and Reliability -- Challenges with Safety -- Applications of Safety and Reliability -- Privacy -- Challenges with Privacy -- Applications of Privacy -- Security -- Challenges with Security -- Applications of Security -- Transparency and Explainability

-- Challenges with Transparency and Explainability -- Applications of Transparency and Explainability -- Accountability -- Challenges with Accountability -- Applications of Accountability -- Human-centricity -- Challenges with Human-centricity -- Applications of Human-centricity -- Summary -- Exam Essentials -- Review Questions -- Chapter 2: Organizational Readiness -- Roles and Responsibilities for AI Governance Stakeholders -- The Strategic Importance of Defined Governance Roles -- Stakeholder Categories and Their Governance Roles -- Executive Leadership -- AI Governance Board or Council -- Legal, Ethics, and Compliance Teams.
Technical and Engineering Teams -- Cybersecurity and Risk Management Teams -- Product and Business Unit Leaders -- End Users and Frontline Staff -- External Parties -- Assigning Responsibilities Across the AI Lifecycle -- Implementation Tools and Techniques -- Cross-functional Collaboration in the AI Governance Program -- Why Cross-functional Collaboration Is Critical -- Principles of Effective Cross-functional Governance -- Building the Collaborative Structure -- Working Groups and Advisory Boards -- Establish Cross-functional Use Case Reviews -- Collaboration Templates and Artifacts -- Fostering a Collaborative Culture -- External and Cross-organizational Collaboration -- Sustaining Collaboration Over Time -- Training and Awareness Program on AI Terminology, Strategy, and Governance -- Why Training and Awareness Are Foundational -- The Scope of the Training Program -- Curriculum Structure -- Example Structure and Content Areas -- Example Module Titles -- Delivering the Training -- Blended Learning -- Mandatory vs. Elective Content -- Regional and Cultural Considerations -- Maintaining Training Records -- Building Awareness Beyond Formal Training -- Tracking and Measuring Success -- Common Pitfalls and How to Avoid Them -- Sustaining the Program Over Time -- Tailoring AI Governance to Organizational Context -- Company Size: Scaling Governance to Organizational Footprint -- Small Companies and Startups (1-200 Employees) -- Mid-sized Organizations (200-5,000 Employees) -- Large Enterprises (5,000+ Employees) -- Organizational Maturity and AI Governance -- Maturity Models -- Low Maturity -- Moderate Maturity -- High Maturity -- Industry Sector-specific Governance Imperatives -- Regulated Industries -- Business- and Consumer-facing Technology -- Industrial and Manufacturing -- Public Sector and Nonprofits.
Products and Services: Governance Based on Use Case Impact -- Internal Use AI -- Decision Support AI -- Automated Decision-making -- Real-time/High-stakes AI -- Risk Tolerance: Calibrating Governance Based on Appetite for Uncertainty -- Low Risk Tolerance -- Medium Risk Tolerance -- High Risk Tolerance -- Business Alignment -- Innovation-driven Organizations -- Reputation-focused Organizations -- Cost-reduction or Efficiency-oriented Organizations -- Developers, Deployers, and Users in AI Governance -- Definitions and Role Boundaries -- AI Developers -- AI Deployers -- AI Users -- Responsibilities Across the AI Lifecycle -- Opportunities and Leverage Points -- Resource Needs and Expectations -- AI Developer -- AI Deployer -- AI User -- Governance Conflicts and Misalignments -- Developers vs. Users -- Developers vs. Deployers -- Users vs. Deployers -- Role-based Governance Controls -- Controls for Developers -- Controls for Deployers -- Controls for Users -- Role Coordination and Integration -- Summary -- Exam Essentials -- Review Questions -- Chapter 3: Updating Policies for AI -- Oversight in the Age of Autonomous Decision-making -- The Lifecycle Policy Model -- Why Lifecycle Oversight Matters -- Core Features of a Lifecycle-oriented Policy -- Use Case Assessment: Aligning Purpose and Risk --

Should AI Be Used at All? -- Risk Rating Frameworks -- Risk Management Tailored for AI -- Ethics by Design: From Principle to Practice -- Operationalizing AI Ethics -- Building Ethics into Technical Design -- Data Acquisition and Use -- Data Lineage and Documentation -- Consent, Privacy, and Synthetic Data -- Model Development: Guardrails for Creation -- Enforcing Reproducibility and Accountability -- Safe and Interpretable Model Architectures -- Training and Testing: Preparing for the Real World -- Rigorous Validation Standards.
Red Teaming and Adversarial Testing -- Test Results Are a Vital Gate -- Deployment and Monitoring: Guarding the Gate -- Pre-deployment Controls -- Post-deployment Monitoring -- Documentation and Reporting: Building Institutional Memory -- Living Documentation -- Internal and External Reporting -- Incident Management: Planning for Failure -- Defining and Escalating Incidents -- AI Playbooks Are Needed -- Root Cause and Remediation -- Evaluate and Update Existing Data Privacy and Security Policies for AI -- Why AI Disrupts Traditional Data Governance -- AI Is Data-hungry by Design -- Inference and Reidentification Risks -- Privacy Policy Gaps and AI-specific Threats -- Common Policy Shortfalls -- AI-specific Privacy Threats -- Key Policy Areas to Evaluate and Update -- Purpose Limitation in Dynamic Pipelines -- Enhanced Anonymization and Pseudonymization Standards -- Lifecycle-based Data Retention Controls -- Data Subject Rights in AI Contexts -- Right to Explanation and Access -- Right to Be Forgotten (Data Deletion) -- Security Policy Updates for AI Systems -- Expanding the Threat Model -- Securing the AI Supply Chain -- Practical Steps for Policy Revision -- Conduct a Gap Assessment -- Build Cross-functional Review Teams -- Policy Compliance Artifacts -- Policies to Manage Third-party Risk -- Why AI Multiplies Third-party Risk -- Beyond the Traditional Vendor Model -- Hidden Dependencies and Sub-tier Risks -- Core Policy Objectives for Third-party AI Risk Management -- Procurement Policy Controls for AI-enabled Solutions -- AI Risk Flagging at Procurement Intake -- AI-specific Due Diligence -- Vendor Risk Tiers -- Contracting and Legal Safeguards -- AI-specific Contractual Clauses -- Liability and Incident Handling -- AI Supply Chain Governance -- Mapping the AI Supply Chain -- Open-source AI Risk Policies -- Other Third-party AI Issues.
Contracting with Human Annotators and AI Workers -- Employee Use of Generative AI Tools -- Monitoring and Reviewing Third-party AI Risk -- Ongoing Vendor Oversight -- Triggers for Reassessment -- Summary -- Exam Essentials -- Review Questions -- Part II: Legal and Regulatory Obligations -- Chapter 4: Privacy and Data Protection Law -- Notice, Choice, Consent, and Purpose Limitation in AI -- Notice -- Unique Challenges in AI -- Choice and Consent -- Defining Consent and Its Variants -- Obstacles to Meaningful Consent in AI -- Purpose Limitation -- Purpose Creep and Reuse -- AI-specific Purpose Challenges -- Data Minimization and Privacy by Design in AI -- Data Minimization -- Data Minimization Across the AI Lifecycle -- Balancing Utility and Minimization -- Privacy by Design (PbD) -- Seven Foundational Principles of Privacy by Design -- Implementing Privacy by Design in AI Development -- Aligning Privacy by Design with Organizational Roles -- Practical Tools and Frameworks -- Practical Implications and Governance -- Operationalizing Privacy Principles in AI -- Governance Touchpoints Across the AI Lifecycle -- Privacy Roles and Responsibilities -- Documentation and Auditability -- Scaling Governance -- Data Controller Obligations in the AI Context -- Privacy Impact Assessments and Risk Management -- The Role of DPIAs in AI Development -- DPIA Lifecycle in AI Projects -- Common Pitfalls in AI

	DPIAs -- Aligning with Emerging Frameworks -- Using Third-party Processors in AI Projects -- Controller vs. Processor in the AI Context -- Contractual Requirements -- Processor Drift and Compliance Gaps -- Cross-border Data Transfers -- Global Data Flows in AI Systems -- AI-specific Data Transfer Challenges -- Transfer Impact Assessments (TIAs) -- Data Subject Rights and AI -- AI-specific Implementation Challenges -- Practical Solutions. Incident Management and Breach Notification.
Sommario/riassunto	An accurate and up-to-date guide to success on the AIGP certification exam and an essential resource for technology and business professionals with an interest in artificial intelligence governance In the IAPP AIGP Artificial Intelligence Governance Professional Study Guide , tech educator and author of more than 50 cybersecurity and technology.