AIIM CIP 2027 Exam Blueprint

The CIP exam is based on the following domains and topics. Individual questions all carry the same weight; the number of questions in each domain reflects the relative weight of that domain.

Domain	Exam Weight
Domain 1: The Value of Information in the Age of AI	12%
Domain 2: Capturing and Preparing Information for People and Machines	23%
Domain 3: Using and Sharing Information and AI Outputs	18%
Domain 4: Governing, Protecting and Retaining Information	25%
Domain 5: Improving Information Management	22%

Domain 1: The Value of Information in the Age of AI	Topics (9)
Includes the following topics: ❑ Why information management matters ❑ Artificial intelligence ❑ AI governance and risk management **Exam weight:** 12%	a. Explain why records are managed and distinguish records from non-records. b. Explain how good and poor information management affect an organization, and align information management outputs (e.g., retention schedules, taxonomies, AI-ready content) with the business outcomes they should deliver (e.g., reduced risk, faster decisions, improved customer service). c. Match AI use cases to information work (e.g., categorization, entity extraction, data loss prevention). d. Evaluate what large language models can and can't reliably do with organizational information. e. Distinguish the main types of AI solutions and their capabilities and explain what each means for information management. f. Explain the benefits of intelligent information management and its effect on how people work. g. Weigh the business value of AI from internal and stakeholder perspectives. h. Identify AI and analytics risks (e.g., poor training data, bias, black-box models, hallucination). i. Assess reputational risks and opportunities from information and AI decisions.

Domain 2: Capturing and Preparing Information for People and Machines	Topics (19)
Includes the following topics: ❑ Document capture and intelligent processing ❑ Preparing information for AI ❑ Organizing information, metadata and taxonomy ❑ Knowledge management, search and discovery **Exam weight:** 23%	a. Explain the stages of records, document, content, and data lifecycles, and identify the points where information moves from one to another (e.g., a draft becomes a record, a record is copied into a dataset or AI index) so the right controls apply. b. Determine the best capture point and process entry for each information type. c. Design a capture process covering what to capture, approvals, and audits. d. Assess completeness, accuracy, and validity at capture, before information reaches downstream systems. e. Choose a digitization strategy and file formats that preserve long-term access. f. Address information from sources the organization doesn't control (e.g., personal devices, social platforms). g. Select methods for extracting information from structured applications and scanned images and explain the benefits of automating extraction. h. Apply attribution, provenance, and transparency requirements to AI-generated content, e.g., labeling content as human-written, AI-assisted, or AI-generated. i. Protect the authenticity and integrity of records (e.g., audit trails, chain of custody) and verify the provenance of content before people or AI systems rely on it. j. Prepare content for AI use by breaking it down, summarizing, and normalizing it while preserving source links, version, meaning, and qualifications. Check transformed content for omissions and errors. k. Identify and remediate redundant, obsolete, and trivial (ROT) content and improve the quality of existing information before people or AI systems rely on it. l. Identify and reduce data exposure risks in prompts and AI-generated outputs, e.g., removing personal data before content reaches an AI system. m. Connect organizational content to AI systems through retrieval (RAG) and context management. n. Define and apply a metadata strategy that gives both human readers and AI systems the context they need (e.g., consistency, maintenance, automation, quality of values). o. Develop and maintain taxonomies, controlled vocabularies, and ontologies (e.g., naming conventions, picklists, knowledge graphs, and engage stakeholders in classification schemes). p. Design information architecture that links related content and supports AI systems. q. Apply reference data, data standards, and interoperability practices so information and its metadata can be shared and reused across systems and data domains. r. Work with the business, IT, and security to define who should have access to what information based on its classification, sensitivity, and business need, and to apply those rules to people and AI tools. s. Compare classification, search, and navigation approaches, including application and enterprise search, and make recommendations on the approach or combination of approaches that best improves findability for people and AI systems.

Domain 3: Using and Sharing Information and AI Outputs	**Topics (13)**
Includes the following topics: ❑ Document and content management ❑ Collaboration and information sharing ❑ AI governance and risk management (AI outputs) ❑ Managing prompts and improving AI practices **Exam weight:** 18%	a. Apply check-in/check-out, version control, workflow, and access controls to support collaboration. b. Understand and recommend change control for critical documents (e.g., policies, procedures, regulated documents), ensuring only the current approved version is in use and superseded versions are withdrawn. c. Govern information sharing across departments, partners, and customers, including collaboration environments. d. Manage email, chat, and meeting content (including AI-generated recaps) as information assets: identify records, apply retention, and control what AI tools can surface. e. Design and advocate for human oversight for automated information processes and AI agents, including bounded permissions and action authority, risk-based approval, escalation, exception handling, quality sampling, an accountable owner, and the ability to stop and recover. f. Recognize when AI output needs human review. g. Set up review and approval workflows for AI outputs before organizational use. h. Apply output validation frameworks and quality indicators to AI-generated content (e.g., citations back to source). i. Maintain documentation and audit trails for AI-related decisions. j. Manage prompts with templates, standards, and version control. k. Build and maintain prompt libraries as organizational information assets. l. Establish quality metrics and monitoring for AI-related information practices. m. Run continuous improvement so corrections feed back into AI information practices.

Domain 4: Governing, Protecting and Retaining Information	Topics (22)
Includes the following topics: ❑ Information governance ❑ Privacy, security and compliance ❑ AI governance and risk management (ethics) ❑ Records management, retention and eDiscovery ❑ Digital preservation and archiving **Exam weight:** 25%	a. Define stewardship and compare governance roles and responsibilities. b. Evaluate an existing governance strategy, processes, documents, and tools. c. Develop, implement, and maintain information management and AI use policies and procedures (e.g., when AI outputs become records), and monitor compliance through information audits. d. Work with IT, security, privacy, and legal, and report on information management to leadership. e. Run day-to-day information management operations, including monitoring dashboards and metrics and responding to everyday enquiries. f. Maintain inventories of systems and repositories that hold records and information. g. Define personal and sensitive data and apply protection strategies. h. Apply Privacy by Design and conduct privacy assessments. i. Apply consent management and privacy impact assessments to AI data use. j. Use redaction, encryption, and rights management effectively. k. Address data sovereignty and respond to a data breach. l. Capture, classify, prioritize, and resolve information incidents, and reduce repeat incidents. m. Identify vital records and plan for business continuity and disaster recovery of records and information. n. Apply fairness and ethical considerations to AI data practices. o. Detect and mitigate bias in AI data practices. p. Set retention and disposition for different content types, including retention schedule elements. q. Apply automation, including AI, to records management tasks such as classification, retention, and disposition, and explain its benefits and risks. r. Select secure disposition methods suited to the information's type, sensitivity, and media, and document disposition. s. Apply legal holds and respond to litigation, audit, and regulatory requests. t. Determine when AI prompts and outputs (e.g., meeting summaries, chat transcripts, generated drafts) are records, and apply records and retention requirements to them and to AI training data. u. Develop a digital preservation strategy that addresses format and media risks. v. Determine whether archived and legacy information can be used, including for AI training, taking privacy, consent, copyright and licensing, and other legal restrictions into account.

Domain 5: Improving Information Management	Topics (21)
Includes the following topics: ❑ Information strategy and digital transformation ❑ Process and workflow automation ❑ Technology/vendor selection and management ❑ Change management and adoption **Exam weight:** 22%	a. Develop an information management strategy with vision, KPIs, and success measures. b. Conduct baseline organizational and technical readiness assessments. c. Diagnose information management problems by tracing symptoms (e.g., information that can't be found, conflicting versions, missed retention, unreliable AI answers) to root causes in people, process, information, or technology. d. Build a program roadmap and business case. e. Identify the system of record for each type of information so people and AI tools rely on the authoritative source. f. Set up governance to prioritize, plan, and measure improvement, and engage stakeholders in it. g. Map a process using standard methods. h. Determine whether a process can be automated and whether AI is suitable. i. Identify reasons for process change and which processes suit it. j. Estimate the expected benefits of automating a process and identify the metrics to capture about it. k. Select process technologies (e.g., workflow, BPM, RPA, and case management). l. Design workflows that maintain audit trails and governance controls. m. Gather business and system requirements for an information management solution. n. Compare content management solution types and select the right fit. o. Evaluate, select, and manage technology vendors, service providers, and AI tools against business, risk, and compliance requirements, including where and how they store and process the organization's data. p. Plan content migrations and address legacy content issues. q. Plan and manage the implementation of an information management solution, including key steps, one-time and ongoing costs, testing, and project management. r. Develop a change plan covering communications, training, AI literacy, and resistance. s. Deliver ongoing education and awareness that builds information and AI literacy among staff, stewards, and owners, including explaining information management to non-technical audiences. t. Define the roles and responsibilities an implementation program needs. u. Define success metrics and conduct post-implementation reviews and benefits measurement.

Appendix: Reference Standards

A CIP should recognize these standards and frameworks and know when to consult them for guidance or compliance. Exam items may test that recognition in context but won't test recall of standard numbers or clause details. The CIP Commission confirms current editions and reviews the list periodically.

Area	Standards and frameworks
Records management	ISO 15489-1 (records management concepts and principles); ISO 16175 (records functionality in business systems); ISO 30301 (management systems for records)
Metadata	ISO 23081 (metadata for records); ISO/IEC 11179 (metadata registries); ISO 15836 (Dublin Core)
Digital preservation	ISO 14721 (Open Archival Information System, OAIS); ISO 19005 (PDF/A); PREMIS (preservation metadata)
Information security and privacy	ISO/IEC 27001 (information security management); ISO/IEC 27701 (privacy information management)
Risk	ISO 31000 (risk management)
Artificial intelligence	ISO/IEC 42001 (AI management systems); ISO/IEC 23894 (AI risk management); NIST AI Risk Management Framework