Information Officers Association

CPIO®

Certified Personal Information Officer

Candidate's Guide

Revised July 2020

Table of Contents

PAGE

1. Introduction

The Certified Personal Information Officer certification program is developed specifically for those persons who are responsible for compliance and encouraging compliance with the conditions for the lawful processing of personal information, dealing with requests made regarding the processing of personal information, working with the Information Regulator and undertaking the obligations set forth in the Regulations.

The CPIO® certification is for all individuals who design, manage and oversee an enterprise's use of personal information. While its central focus is the lawful processing of personal information, it will be of value to anyone with responsibility for the protection of information. This certification promotes best practices and provides executive management with assurance that those with the designation CPIO® are knowledgeable about the requirements for lawfully processing personal information.

The CPIO® Exam

2. Development/Description of the CPIO® Exam

The CPIO® exam has been developed to ensure it is relevant and its content is current. Questions for the CPIO® exam are developed through a comprehensive process designed to ensure the ultimate quality of the exam.

Job practice statements serve as the basis for the exam and are the knowledge and skill requirements to earn the CPIO® certification. These job practice statements are periodically updated and consist of six domains. The domains and the accompanying tasks and knowledge statements were the result of extensive research and feedback from subject matter experts.

The tasks and knowledge statements describe the tasks performed by CPIO®s and the knowledge required to perform these tasks. Exam candidates will be tested based on their practical knowledge associated with performing these tasks.

The current job practice analysis contains the following domains and percentages:

- Legislation for the protection of personal information (10%)
- Privacy rights of data subjects (10%)
- Conditions for the lawful processing of personal information (30%)
- Data protection risk management (10%)
- Generally accepted data protection measures, practices and procedures (25%)
- Data protection compliance management frameworks and standards (15%)

Note: The percentages listed with the domains indicate the percentage of questions that will appear on the exam from each domain. For a description of each domain's task and knowledge statements, please refer to pages 9-12.

The CPIO® exam consists of 100 multiple-choice questions and is administered during one two-hour session.

3. Preparing for the CPIO® Exam

Passing the CPIO® exam can be achieved through the study of the Protection of Personal Information Act, its regulations, related legislation, standards, best practices and information related to its application and interpretation. To assist individuals with their studies, study aids and training courses are available to exam candidates. See www.cpio.co.za to view the study aids that can help you prepare for the exam.

A list of references recommended for future study in preparation for the exam will be found at www.cpio.co.za. A more comprehensive list will be in the CPIO® Examination Review Manual that is currently under development.

No representation, warranties or assurances regarding a candidates' ability to pass the exam are made in connection with these or other publications, courses and/or other study materials.

4. Administration of the CPIO® Exam

Testing, administration and scoring of the CPIO® is undertaken online.

4.1. Exam Admission

Candidates are able to register for the CPIO® exam online. Exam admission confirmation will indicate the date and examination time for the CPIO® exam.

Please Note: In order to receive an exam admission confirmation, all fees must be paid and candidates must have provided a current e-mail address. Only candidates with an admission confirmation will be permitted to take the exam. If a candidate's e-mail address changes, he/she should update his/her profile with the exam administrator.

Candidates must note the specific exam times on their admission confirmation. An admission confirmation can only be used for the designated examination time and on the specified examination date.

4.2. Special Arrangements

Upon request, reasonable accommodations in the exam procedures will be made for candidates with documented disabilities or religious requirements. These candidates may request consideration for reasonable alternatives in the arrangements. No food or drinks are allowed during the period the exam is taken. Request for consideration must be submitted in writing, accompanied by appropriate documentation, no later than two months before the exam date.

4.3. Exam Admission and Authentication

Every candidate's exam admission will take place before the start of the exam. The candidate must be confirmed for a specific date and time at least three days in advance. The candidate's identity must be authenticated by scanning the candidate's identity document before commencement of the exam.

Candidates can only use their admission confirmation for the exam on the designated date and time. Candidates will be admitted to the exam only if they possess a valid admission confirmation and an acceptable form of identification. An acceptable identification document (ID) is a current and original official government-issued ID that contains the candidate's name, as it appears on the admission confirmation, and the candidate's photograph. Examples include, but are not limited to a passport, driver's license and national ID. Any candidate who does not provide an acceptable form of ID will not be allowed to sit for the exam and will forfeit his/her registration fee.

4.4. Computer used to take the exam

- Candidates must supply their own computer and they must check that it is compatible with requirements for the exam prior to the commencement time for the exam.
- Only the computer used to take the exam can be in the room where the exam will be taken. No other devices are allowed in the room at the time f the exam.
- The candidate's computer must not have more than one display or monitor. For example, if you usually use a laptop with a monitor connected, disconnect your monitor and use only the laptop screen.
- The candidate must close all other programs or windows on the computer before commencing the exam.
- The candidate must not use the following tools.
    a. Programs such as Excel, Word, or PowerPoint.
    b. Communication programs such as Skype.
    c. Any website page other than the exam window in your course.

4.5. Exam Rules

- Candidates must not allow anyone else to substitute for them.
- Visitors are not permitted in the room during the exam.
- Candidates must dress as though they are in a public setting.
- Candidates will only be admitted to an exam on the designated date and time.
- Candidates must present an acceptable government issued photo-ID for identification before the commencement of the exam.
- Candidates are not allowed to bring reference materials or blank paper into the exam room.
- Candidates are not allowed to bring or use a calculator during the exam.
- Candidates are not allowed to bring any type of communication device (i.e., cell phones, PDAs, tablets) into the exam room.
- Candidates must not use headphones, ear buds, or any other type of listening equipment.
- Candidates must not communicate with any other person by any means.
- Candidates must not leave the room during the exam for any reason.

- No food or beverages are allowed in the exam room.

4.6. Exam Questions and the Online exam

- Before a candidate begins the exam, the candidate must read all instructions. The candidate's identification document must be captured correctly before the exam commences.
- Candidates who skip over the directions or read them too quickly could miss important information and possibly fail to answer questions correctly.
- A candidate is required to read each exam question carefully and understand it before attempting to answer the questions.
- All answers are to be indicated in the appropriate field of the online exam. Candidates must be careful to select the correct answer. If an answer needs to be changed, a candidate can do so.
- All questions should be answered. There are no penalties for incorrect answers. Grades are based solely on the number of questions answered correctly.
- After completion, candidates will receive their test scores. Successful candidates will receive an electronic certificate of their success.
- An examine proctor will monitor the exam session remotely.
- Candidates must complete the exam within the time limit specified.

4.7. Exam Duration and Time Allocation

- The CPIO®exam is two hours in length. This is strictly controlled by the system. This allows for approximately one minute per question, with a few minutes for revision. Candidates are advised to pace themselves to complete the entire exam. Candidates must therefre complete an average of 50 questions per hour.
- Candidates are urged to immediately record their answers. **No additional time will be allowed after the exam time has elapsed.**

4.8. Conduct

- The CPIO® certification body reserves the right to disqualify any candidate who is discovered engaging in any kind of misconduct, such as giving or receiving help; using notes, papers or other aids; attempting to take the exam for someone else; or copying or otherwise recording the exam materials. The examine proctor will provide the CPIO certification committee with reports regarding any irregularities for its review and final decision.

4.9. Reasons for Dismissal

The CPIO® examine proctor may dismiss a candidate for any of the following reasons:

- Unauthorized admission to the exam.
- Candidate creates a disturbance or receives help.
- Candidate attempts to record test materials or makes notes.
- Candidate impersonates another candidate.
- Candidate brings items into the exam room that are not permitted.

5. Scoring the CPIO® Exam

The CPIO® exam consists of consists of 100 multiple-choice items. A candidate must score 75% of the questions correctly to pass the exam. A score of 75% represents the minimum standard of knowledge as established by the CPIO certification committee. A candidate receiving a passing score may then apply for certification.

The official exam result will be available immediately on completion of the exam to candidates. Additionally, with the candidate's consent, an e-mail message containing the candidate's pass/fail status and score will be sent to the candidate. This e-mail notification will only be sent to the email address listed in the candidate's profile at the time of the initial release of the results. To ensure the confidentiality of scores, exam results will not be reported by telephone or fax.

Successful candidates will receive, along with a score report, an application for CPIO certification.

Unsuccessful candidates should note that the total score is determined by calculating a simple average of the recorded scores.

Candidates receiving a failing score on the exam may not request a re-score of their answer sheets but they can register to take the exam again.

6. Types of Questions on the CPIO® Exam

CPIO® exam questions are developed with the intent of measuring and testing practical knowledge and the application of general concepts and standards. All questions are multiple choice and are designed with one best answer.

Every CPIO® exam question has a stem (question) and four options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement. In some instances, a scenario or description problem may be included.

These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided. The candidate is cautioned to read each question carefully. A CPIO exam question may require the candidate to choose the appropriate answer based on a qualifier, such as MOST likely or BEST. In every case, the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible.

7. Application for CPIO® Certification

Passing the exam means a candidate is a CPIO®. Once certified, the new CPIO® will receive a certificate and the CPIO® continuing professional education (CPE) policy requirements. Individuals must request that their CPIO® status be placed in the public domain.

8. Requirements for Initial CPIO® Certification

Certification is granted initially to individuals who have successfully completed the CPIO® exam.

9. Requirements for Maintaining CPIO® Certification

CPIO®s must comply with the following requirements to retain certification:

- Attain and report an annual minimum of 20 CPE hours. The CPIO® continuing professional education policy requires the attainment of 20 CPE hours over an annual reporting period.
- Submit annual CPE maintenance fees in full.
- Respond and submit required documentation of CPE activities to support the hours reported if selected for an annual audit.
- Comply with the CPIO® Professional Code of Ethics.

Failure to comply with these general requirements will result in the revocation of an individual's CPIO designation.

10. CPIO® Code of Ethics

A Code of Ethics guides the professional and personal conduct of individuals who hold the CPIO® certification.

Holders of the CPIO® certification shall:

1. Support the implementation of, and encourage compliance with, legislation for protection of personal information, appropriate related national and international standards, procedures and controls.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with related professional standards and best practices
3. Serve in the interest of stakeholders (including data subjects and responsible parties) in a lawful and honest manner, while maintaining high standards of conduct and character, and not behave or engage in unethical activities
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties

5. Maintain competency in the necessary fields and agree to undertake only those activities that they can reasonably expect to complete with the required competence
6. Inform appropriate parties of the results of work performed, revealing all significant facts known to them
7. Support the education of stakeholders in enhancing their understanding of the conditions for the processing of personal information, information systems security and control
8. Failure to comply with this Code of Ethics can result in an investigation into the certification holder's conduct and, ultimately, in disciplinary measures.

11. Revocation of CPIO® Certification

The CPIO® certification committee may, at its discretion after due and thorough consideration, revoke an individual's CPIO® certification for any of the following reasons:

- Failing to comply with the CPIO® CPE policy
- Violating any provision of the CPIO Code of Ethics
- Falsifying or deliberately failing to provide relevant information
- Intentionally misstating a material fact
- Engaging or assisting others in dishonest, unauthorized or inappropriate behaviour at any time in connection with the CPIO exam or the certification process.

12. CPIO® EXAM DOMAIN CONTENT

1. **Legislation for the Protection of Personal Information —** Demonstrate an understanding of the laws and regulations applicable to the protection of personal information.

Task Statements

1.1. Understand a data subject's constitutional right to privacy

1.2. Understand the balance between the right to privacy and other rights, particularly the right of access to information, protecting important interests and the free flow of information.

1.3. Identify current and potential legal and regulatory requirements affecting the processing of personal information.

1.4. Define the roles and responsibilities for the protection of personal information throughout the organization.

1.5. Interpret and apply the Protection of Personal Information Act and its regulations.

1.6. Interpret and apply the Promotion of Access to Information Act.

1.7. Interpret and apply other legislation that impacts the processing of personal information.

1.8. Understand how to translate legal obligations into data protection objectives and practices.

1.9. Maintain a process for notifying relevant stakeholders of privacy compromises.

1.10. Understand the process for issuing codes of conduct.

1.11. Understand the rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories and automated decision-making.

1.12. Understand the legal requirements for the transfer of personal information outside the Republic.

1.13. Understand the procedures used by the Information Regulator to enforce the rights of data subjects, and the process to appeal this enforcement.

1.14. Understand the offences, penalties and administrative fines that may result from unlawful acts relating to the processing of personal information.

Knowledge Statements

1.1. Knowledge of the relationship between data protection and information security.

1.2. Knowledge of the scope of legislation governing the processing of personal information.

1.3. Knowledge of regulatory requirements and their potential business impact from a privacy standpoint.

1.4. Knowledge of the legal definition for "personal information" and other definitions associated with the processing of personal information.

1.5. Knowledge of the legal responsibilities of Responsible Parties, Information Officers, Operators and other key roles.

1.6. Knowledge of the conditions that prescribe the minimum threshold requirements for the lawful processing of personal information.

1.7. Knowledge of the Companies Act and other South African legislation that impact the processing of personal information.

1.8. Knowledge of the rights of data subjects and their remedies to protect their personal information from processing when it is not in accordance with the Protection of Personal Information Act.

1.9. Knowledge of the technical and organisational measures that give effect to data subjects' rights.

1.10. Knowledge of data protection compliance frameworks.

2. Privacy rights of Data Subjects - Identify and manage the measures that give effect to the conditions for the lawful processing of personal information.

Task Statements

2.1. Understand the potential harm to data subjects

2.2. Implement the privacy rights of data subjects

2.3. Define processes to give effect to the privacy rights of data subjects

2.4. Minimise the use of personal information

2.5. Use techniques to reduce linkability of personal information

2.6. Maintain transparency through privacy notices and the PAIA manual

2.7. Control the quality of information

2.8. Protect the integrity of personal information

2.9. Protect the confidentiality of personal information

2.10. Ensure the availability of personal information

2.11. Define the purpose of processing

2.12. Provide notification of processing

2.13. Provide notification personal information is being collected

2.14. Notify data subjects of unauthorised access

2.15. Manage records

2.16. Develop procedures to destroy personal information.

Knowledge Statements

2.1. Knowledge of the rights of data subjects.

2.2. Knowledge of the legal basis for processing personal information.

2.3. Knowledge of the right to be informed of right to object

2.4. Knowledge of the right to be informed of right to withdraw consent

2.5. Knowledge of the right to be informed of right to lodge a complaint

2.6. Knowledge of the right to receive documentation

2.7. Knowledge of the right to be informed about interferences

2.8. Knowledge of the right to have their data minimised

2.9. Knowledge of the right to have reduced linkability

2.10. Knowledge of the right to be have disputed accuracy notifications sent out

2.11. Knowledge of the right to have notifications sent when information is changed

2.12. Knowledge of the right to hsvr data exported.

3. Conditions for the lawful Processing of Personal Information - Identify and manage the measures that give effect to the conditions for the lawful processing of personal information.

Task Statements

3.1. Comply with the conditions and all the measures that give effect to the conditions set out in the Protection of Personal Information Act.

3.2. Determine scope and set policy for the protection of personal information.

3.3. Establish accountability for the processing of personal information.

3.4. Identify personal information.

3.5. Document the processing of personal information.

3.6. Conduct personal information impact assessments

3.7. Process personal information lawfully and in a reasonable manner.

3.8. Prepare privacy notices and statements.

3.9. Process personal information in a manner that is not excessive.

3.10. Understand how data minimisation can be achieved.

3.11. Collect personal data only for specific purposes.

3.12. Request consent to process personal information from data subjects.

3.13. Limit further processing of personal information.

3.14. Retain and destroy records of personal information no longer required.

3.15. Take reasonably practical steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

3.16. Maintain the measures that give effect to the protection of personal information.

3.17. Secure the integrity and confidentiality of personal information.

3.18. Enable data subject participation.

3.19. Prohibit the processing of special personal information.

3.20. Process sensitive personal information only if a general authorisation applies.

3.21. Request and exemption from the conditions for processing of personal information when appropriate.

Knowledge Statements

3.1. Knowledge of the conditions for the lawful processing of personal information.

3.2. Knowledge of the legal bases for processing personal information

3.3. Knowledge of the powers, duties and functions of the Information Regulator.

3.4. Knowledge of the duties and responsibilities of the Information Officer and any deputy information officers.

3.5. Knowledge of third-party relationships and their impact on information security (e.g., in cases of mergers and acquisitions).

3.6. Knowledge of methods to maintain and manage a systematic record of personal data processing activities

4. Data Protection Risk Management - Identify and manage the risks related to the processing of personal information.

Task Statements

4.1. Implement a systematic and structured risk assessment process.

4.2. Identify all reasonably foreseeable internal and external risks to personal information.

4.3. Establish a process for information asset classification and ownership.

4.4. Implement a systematic and structured data protection risk assessment process.

4.5. Identify legal, organisational and technical vulnerabilities.

4.6. Ensure that personal information impact assessments are conducted periodically.

4.7. Ensure that threat and vulnerability evaluations are performed on an on-going basis.

4.8. Identify suitable risk treatment options for internal and outsourced processing.

4.9. Understand how to implement privacy by design and by default.

4.10. Identify and periodically evaluate information security controls and countermeasures to mitigate risks to data subjects.

4.11. Integrate risk, threat and vulnerability identification and management into life cycle processes (e.g., development, procurement and employment life cycles).

4.12. Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven.

Knowledge Statements

4.1. Knowledge of the business goals and objectives.

4.2. Knowledge of the potential reputational damage.

4.3. Knowledge of data protection reference architectures.

4.4. Knowledge of data protection risk management policies and objectives

4.5. Knowledge of data protection risk management methodologies and processes.

4.6. Knowledge of the threats to the processing of personal information.

4.7. Knowledge of information security concepts and safeguards.

5. Generally Accepted Data Protection Measures, Practices and Procedures - Identify and manage data protection safeguards to secure the integrity and confidentiality of personal information.

Task Statements

5.1. Establish a process for information asset classification and ownership.

5.2. Establish and maintain appropriate safeguards to secure the integrity and confidentiality of personal information.

5.3. Verify the effectiveness of information security safeguards

5.4. Maintain a data protection incident handling procedure.

5.5. Periodically test and refine data protection incident response plans.

5.6. Establish a capability to investigate data protection and information security incidents (e.g. forensics, evidence collection and preservation, log analysis and interviewing).

Knowledge Statements

5.1. Knowledge of information security and data protection concepts.

5.2. Knowledge of the components that comprise an information security and data protection strategy.

5.3. Knowledge of how to specify the target information security and data protection architecture.

5.4. Knowledge of the relationship between information security and the protection of personal information.

5.5. Knowledge of the organisational and technical arrangements for the protection of personal information.

5.6. Knowledge of methods of testing the effectiveness and applicability of information security controls (e.g. penetration testing, password cracking, social engineering, assessment tools).

5.7. Knowledge of the procedures for information separation, blocking, deletion & destruction of all generations of copies, backups and archives for structured and unstructured data

5.8. Knowledge of how to restore the integrity of the responsible party's information systems.

5.9. Knowledge of the contents of a written contract between the responsible party and the operator.

5.10. Knowledge of how to verify that operators which process personal information for the responsible party has established and maintains the required security measures.

5.11. Knowledge of information security management roles, responsibilities and general organizational structures.

5.12. Knowledge of generally accepted international standards for information security management.

5.13. Knowledge of notification and escalation processes for effective security management.

5.14. Knowledge of internal and external reporting requirements.

5.15. Knowledge of methods for establishing reporting and communication channels throughout an organization.

6. Data Protection Compliance Management Framework and Standards - Identify and manage the protection of personal information in a formally structured manner.

Task Statements

6.1. Establish a framework for managing the protection of personal information.

6.2. Implement a systematic and structured personal information management processes.

6.3. Establish governance structures for the protection of personal information.

6.4. Develop policies for the protection of personal information.

6.5. Establish senior management accountability for the management of personal information.

6.6. Implement data protection management practices.

6.7. Maintain a record of data protection policies, practices and changes thereto.

Knowledge Statements

6.1 Establish a framework for managing the protection of personal information.

6.2 Knowledge of the goals, policy, strategy, benefits and other expected outcomes from data protection management.

6.3 Knowledge of building capability in data protection management practices.

6.4 Knowledge of proactive design methods for data protection, as the default, embedded, fully functional, end-to-end, visible and transparent, with respect for end user privacy.

6.5 Knowledge of data protection enhancing technologies.

6.6 Knowledge of the specification for a data protection management system.

6.7 Knowledge of techniques for quantifying damages, costs and other business impacts arising from data protection incidents.

6.8 Knowledge of post-incident data protection review practices and investigative methods to identify causes and determine corrective actions.