DIRECTORATE FOR REGISTRATION AND RECOGNITION

EVALUATION REPORT FOR THE RECOGNITION OF PROFESSIONAL BODIES AND REGISTRATION OF PROFESSIONAL DESIGNATIONS

Name of Professional Body	Information Systems Audit and Control Association South Africa Chapter NPC (ISACA SA)
Statutory or Non-Statutory Body	Non-Statutory
Sector	IT audit
Physical Address	Unit 7 Roodebloem Office Park, 20 Bella Rosa Street, Rosenpark, Bellville, Cape Town, South Africa
Application Approved by Board/Council	Yes
Application Signed by CEO / Registrar/ Board Chairperson	Yes
Number of Designations Applied for	2
Date of Site Visit	19 June 2020
Date of Gazette Notice	13 November 2020

PROFESSIONAL BODY RECOGNITION AND PROFESSIONAL DESIGNATION REGISTRATION

EVALUATION REPORT

NAME OF BODY: Information Systems Audit and Control Association South Africa Chapter NPC (ISACA SA)

1. PROFESSIONAL BODY BACKGROUND

1.1. ISACA SA applied to SAQA for recognition as a professional body and the registration of two (2) professional designations on the NQF in terms of the NQF Act, Act 67 of 2008.

1.2. ISACA was founded in 1967 when a small group of individuals with similar professions - auditing controls in the computer systems that were becoming increasingly critical to the operations of their organisations - discussed the need for a centralised source of information and guidance in the field. Previously known as the Information Systems Audit and Control Association®, ISACA now goes by its acronym only, to reflect the broad range of Information Technology (IT) governance professionals it serves and to accommodate increasing technological advances.

Today, ISACA's constituency of more than 140,000 professionals worldwide is characterised by its diversity. As a non-profit, global membership association for IT and information systems professionals, ISACA is committed to providing its diverse constituency with the frameworks, tools, techniques and knowledge they need to achieve individual and organisational success. ISACA operates in six regions: Africa, Asia, Europe, Latin America, North America and Oceania. The South Africa Chapter forms part of the Africa region. There are 17 Chapters in total in the Africa region, and the South Africa Chapter has the most significant number of members within the region. ISACA provides globally recognised certification in information and technology assurance (Certified Information Systems Auditor), security (Certified Information Security Manager), governance (Certified in the Governance of Enterprise IT), and risk (Certified in Risk and Information Systems Control).

2. CRITERIA FOR RECOGNISING A PROFESSIONAL BODY

DRR evaluated the application against the *Policy and Criteria for Recognising a Professional Body and Registering a Professional Designation for the Purposes of the NQF Act.* ISACA South Africa Chapter (ISACA SA) meets all the criteria for recognising a professional body listed below:

2.1. Legally constituted entity

- The ISACA South Africa Chapter (ISACA SA) is a non-statutory body registered with the Companies and Intellectual Property Commission (CIPC) as a Non-Profit Company (NPC) with registration number 2003/004050/08. The ISACA has 5 Directors reflected on their CIPC certificate. The following document(s) were submitted:

- CIPC registration certificate
- CIPC disclosure certificate
- Memorandum of Incorporation (MOI)
- Bylaws
- List of Board members
- List of individual members

2.2. Human resources

- The professional body submitted its staff organogram.
- According to the organogram submitted, the professional body has two full-time staff members. These are the Finance (Office) Manager and a Marketing & Events Coordinator.
- A third staff member (possibly with general event coordination and graphic design skills) is in the process of being employed for 2020 onwards, and temporary staff are employed from time to time as and when required.
- The professional body outsources some administrative functions such as graphic design (TOME Studio & DN Productions), monthly accounting (Triton), website maintenance (Linchpin Project Management), company secretarial functions (PKF), videography (MW Productions), photography (Portrait Photography, Sam Phiri Photography), and travel bookings (Wings Travel).
- The Directors support the functions of the Chapter.

2.3. Financial resources

- The professional body submitted its audited financial statements for 2016, 2017 and 2018.
- According to the professional body report, the membership subscriptions, annual conference fees, yearly conference sponsorship, advertising and grants from ISACA international, from time to time are the major sources of income.
- The auditors' opinion in the audited financial statements present fairly, in all material respects, the financial position of Information Systems Audit and Control Association South Africa Chapter NPC as at 31 December 2018 and its financial performance and cash flows for the year then ended in accordance with International Financial Reporting Standard for Small and Medium-sized Entities and the requirements of the Companies Act of South Africa.

2.4. Good corporate governance practices

- The professional body submitted the:
  - Latest Elective Meeting minutes;
  - Terms of reference of the Board; and
  - List of Board members

- The Chapter appoints the Board for two years at the Chapter's annual general meeting (AGM).
- The ISACA 2020 Board of Directors list has twelve Board members and one resignation.
- All board members are expected to resign at the end of their term of office and may be eligible for reappointment, subject to the rules and regulations in the Chapter's MOI or Bylaws.
- The Board conducts its meetings per the Chapter's memorandum of incorporation (MOI) and Bylaws.
- The Board meets at least once each month, with additional meetings held as deemed necessary or advisable.
- A simple majority (50 +1) of the Chapter Board constitutes a quorum for any Board meeting.

- The Chapter President or Vice President must be present to form a quorum.
- The ISACA expects each Director to attend all meetings of the Board and any board committee of which he or she is a member.
- The professional body holds meetings of the Board in person, by telephone, or other forms of long-distance (virtual) electronic conference facility as circumstances may require, provided that they meet the required quorum and all participants can communicate with each other simultaneously.
- Any Board member, who is absent without leave of absence from two consecutive board meetings, may be removed from the Board, unless an acceptable excuse has been tabled and accepted by the Board, at the Board meeting following the second absence.
- The Board has unrestricted access to management and employees of the Chapter (including, for greater certainty, its members, partners and suppliers). It may invite them to Board meetings for a specific reason(s) but with no voting powers.
- In terms of the Chapter MOI and the Bylaws, the Board appoints Board committees. The Board delegates certain functions to well-structured committees but without abdicating its responsibilities. The Board remains collectively responsible for the decisions and actions taken by any board committee.

2.5. Code of Conduct and Protection of the Public

- The professional body submitted the following documents:
  - Code of ethics
  - Disciplinary Policy and Procedure
  - Appeals Policy and Procedure

- Membership of the Chapter requires adherence to the Code of Ethics, and the professional body communicates to all members during sign-up and membership renewal.
- The Code of Conduct/Ethics is also made available on the ISACA website on https://engage.isaca.org/southafricachapter/aboutchapter/policies.
- An Anti-Harassment policy is also in place and is made available on the ISACA website.
- The complaints reporting process is available on the ISACA website for members and the public http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/Code-of- Ethics-Frequently-Asked-Questions-FAQ-.aspx
- A complaint may be filed by completing an Ethics Complaint Form and submitting it to ethics@isaca.org.
- When a member submits a complaint to ISACA, the professional body conducts an initial assessment and recommends it to the Ethics Committee. In reviewing the recommendation and complaint, the Ethics Committee makes one of the following determinations:
  - Ethics Committee dismisses the complaint;
  - Complaint warrants a summary finding (as in the case of a reported criminal conviction affecting an individual's adherence to the Code of Ethics); or
  - The complaint will proceed for a formal investigation.
- ISACA notifies the respondent and the complainant of the complaint and Ethics ' 'Committee's course of action. Where a complaint proceeds to a formal investigation, the Ethics Committee allows the respondent to respond.
- If the Ethics Committee finds the respondent to have violated the ISACA Code of Professional Ethics, disciplinary action may be taken and could include the following: reprimand, the prohibition of participation in specified ISACA activities, suspension or revocation of membership, or cancellation of ISACA certifications held.
- Should the respondent wish to appeal a disciplinary action, an appeals process is available.

- The respondent must submit the appeals to the Ethics Appeals Committee. Based on the information provided the Appeals Committee will determine if the Ethics Committee failed to follow ISACA's Ethics Complaint Process or if there were material errors of fact in the information used as a basis for the determination. The respondent may also appeal to the severity of disciplinary action imposed. Decisions of the Appeals Committee are final.
- The ISACA has not had an instance at the ISACA South Africa Chapter, where there was a breach of the code of ethics.

2.6. Awarding of Professional Designations

- The professional body submitted the policy and procedures for developing, awarding and revoking professional designations.
- Any person who believes that he/she is eligible for a professional designation may apply, in writing, on the prescribed form to ISACA South Africa Chapter for the professional designation.
- Members can submit the completed application form, plus copies of relevant qualifications and statements of work experience.
- The person must meet the minimum requirements for the designation, including:
  - Proof of CISA or CISM certification in good standing, which requires a minimum of 5 years relevant proven experience across specified domains and subject to certain waivers;
  - Proof of membership and acceptance of the Code of Conduct;
  - Proof of a relevant degree, diploma or other qualification having a rating of at least NQF 7;
  - Proof of at least five years related experience; and
  - Proof of payment of the designation fee.
- Successful applicants are awarded their designations upon payment of the relevant designation fee and signing of acceptance of the ISACA Code of Conduct.
- Successful applicants are required to comply with the ongoing requirements of ISACA South Africa Chapter Continuing Professional Development Policy for the retention of their awarded designation.
- Unsuccessful applicants are informed of the Board's decision and given the reasons for refusal, in writing, by the ISACA South Africa Chapter Board Chairperson plus a list of remedial actions, if applicable, for the approval of the application at a later date.
- Unsuccessful applicants may appeal against the decision following the ISACA South Africa Chapter Appeals Policy and Procedures.

2.7. Recognition of Prior Learning (RPL)

- The professional body submitted its policy for Recognition of Prior Learning.
- ISACA SA considers RPL for the two designations; Information Systems Audit Professional - ISAP (SA) and Information Security Management Professional- ISMP (SA). Applicants who have the requisite number of 'years' experience in this sector, without the underlying National Qualifications Framework (NQF) Level 7 qualification may apply for a professional designation through recognition of prior learning.
- Such applicants must formally submit proof of a Senior Certificate and evidence of experience to the ISACA SA Chapter. The professional body independently verifies all experience with employers.
- Successful applicants are still required to complete the membership/professional designation application form and submit to ISACA SA to apply for the designation.
- ISACA has not received any applications for RPL.

ISAP (SA) Application for RPL:

- ISAP applicants must hold the Certified Information Security Manager (CISM) certification, a relevant ICT qualification recognised on the NQF, have a minimum of

five years experience in the Information Security/Assurance or related and signed the ISACA membership code of conduct.

- ISAP applicants must provide evidence of working in the sector; this evidence must be reflective of the work they are involved in, that it is linked to the CISM certification.
- For an applicant to receive the benefit of RPL, the designee must to hold a minimum of the National Senior Certificate and have been operating in Information Security/Assurance or related sector for at least ten years.

ISMP (SA) Application for RPL:

- ISMP applicants must hold the Certified Information Systems Auditor (CISA) certification, a relevant ICT qualification recognised on the NQF, have a minimum of five years experience in the Information System Auditing or related and signed the ISACA membership code of conduct.
- ISMP applicants must provide evidence of working in the sector; this evidence must be reflective of the work they are involved in, that it is linked to the CISA certification.
- For an applicant to receive the benefit of RPL, the designee will need to hold a Senior Certificate and have been operating in Information System Auditing or related sector for at least ten years.

2.8. Continuing Professional Development (CPD)

- The professional body submitted its Continuing Professional Development Policy and evidence of CPD implementation.
- The criteria for CISA/CISM maintenance are as follows:
- The ISACA Global CISA/CISM CPE policy requires the attainment of CPD hours over an annual and three-year certification period.
- CISA/CISM holders must comply with the following requirements to retain certification:
  - Attain and report an annual minimum of twenty (20) CPD hours. These hours must be appropriate to the currency or advancement of the CISA/CISM knowledge or ability to perform CISA or CISM-related tasks. The use of these hours towards meeting the CPD requirements for multiple ISACA certifications is permissible when the professional activity applies to satisfy the job-related knowledge of each certification.
  - Submit annual CPD maintenance fees to ISACA Global in full.
  - Attain and report a minimum of one hundred and twenty (120) CPD hours for a three-year reporting period.
  - Respond and submit the required documentation of CPD activities if selected for the annual audit.
  - Comply with ISACA's Code of Professional Ethics.
  - Abide by ISACA's IT auditing standards (CISA).
- Certified individuals who fail to comply with the CPD Policy will have their CISA certification credential revoked, will no longer be allowed to present themselves as certified individuals, and will be reported as such on requests for confirmation of certification. Following this, the professional body automatically revokes their ISAP (SA) or ISMP (SA) professional designation.

2.9. List of Members

- The professional body submitted the list of its of registered members.
- During the site visit, verification that the professional body has a total of 2 258 members as at 18 June 2020 took place.
- The membership demographics are as follows: 38% are females, and 64% are males.
- The professional body also successfully loaded dummy data to the NLRD.

2.10. Unfair Exclusionary Practices

- The professional body submitted its membership admission policy. No unfair exclusionary practices were in the submission.

- ISACA South Africa has 12 Directors on the Board of Directors, with 11 Directors of colour and three female directors.
- ISACA SA has a Transformation Policy and Plan in place to address the transformation agenda and acknowledges the past imbalances that existed in the country.

2.11. Career Advice Information

- Events through which members, the public and learners are reached include:
  - Annual General Meetings;
  - Student Chapter Events;
  - Regional Events in KZN, Eastern Cape, Western Cape, Pretoria and Johannesburg;
  - Combined Regional Events with (Memorandum of Understanding) MOU partners;
  - ISACA SA Annual Conference;
  - Conferences of MOU partners;
  - Stakeholder Events;
  - Breakfast Meetings;
  - Year-End Events; and
  - Annual Member Award Events.

2.12. Education and Training

The ISACA South Africa Chapter (ISACA SA) complies with Section 19 of the policy and criteria to the extent that it:

- is not accredited as an education and training provider by a Quality Council;
- is not registered as an education and training provider with the Department of Higher Education and Training;

2.13. The proliferation of professional bodies

The following organisations operate in a related or similar (but not the same) community of practice. ISACA's designations are primarily technology-focused. While organisations may operate within the same community, the areas of specialisation are different and hence ISACA can co-exist and work together. There is no overlap between the designations ISACA SA wishes to register with SAQA and that of other professional bodies. The missions of the respective professional bodies mentioned below are complementary to ISACA's Purpose & Promise. As such, ISACA South Africa has Memorandums of Understanding (MOUs) with these organisations.

Institute of Internal Auditors South Africa (IIA SA)

IIA SA focuses on providing a wide range of services dedicated to the education and advancement of internal auditors. In contrast, ISACA SA focuses on information security, cybersecurity, IT assurance, IT risk management and IT governance. We have an MOU in place with the IIA SA in the process of renewal.

CRITERION	DESCRIPTION
Underlying NQF Registered Qualification/Part -Qualification	Bachelor of Commerce: Information Systems/Management/Business Information Systems/Informatics/Financial Accounting: • Bachelor of Commerce in Information and Technology Management (71889) • Bachelor of Commerce: Information Systems (4431) • Bachelor of Commerce in Business Informatics (101104) • Bachelor of Accounting (90622) • Bachelor of Commerce in Accounting Sciences (7033) • Bachelor of Accounting Science (5535) • Postgraduate Diploma: Management: Financial Accounting (15497) • Postgraduate Diploma in Accounting (5191) Bachelor of Science: Computer Science/Informatics/Information Technology/Mathematical Science • Bachelor of Science Honours: Computer Science (4503) • Bachelor of Science in Informatics (79786) • Bachelor of Science: Information Technology (50363) • Bachelor of Science in Information Technology (80887) • Postgraduate Diploma: Mathematical Sciences (66511) Bachelor of Arts: Humanities with Socio Informatics (71650) Bachelor of Technology: Financial Information Systems • Bachelor of Information Technology in Business Systems (97804) • National Diploma: Financial Information Systems (80163), or • Any other related NQF Level 6 qualification
Experiential Learning / Practical Experience	A minimum of 5 years relevant proven Information Systems Audit experience across the following domains: • Domain 1 - The Process of Auditing Information Systems; • Domain 2 - Governance and Management of IT; • Domain 3 - Information Systems Acquisition, Development and Implementation; • Domain 4 - Information Systems Operations, Maintenance and Service Management; and • Domain 5 - Protection of Information Assets. If the applicant does not meet the 5-year experience requirement, he/she may opt to submit qualifying waivers for experience gained (up to a maximum of 3 years).
Board / Admission Examination / Assessment	CISA exam passed, and CISA certification attained. CISA Exam: • The examination is open to all individuals who have an interest in information systems audit, control and security. All are encouraged to work toward and take the examination. • A committee sets the exam at ISACA HQ, and the computer-based exam is administered locally by a vendor. • The professional body sends all information required to apply for certification with their notification of a passing score to successful candidates. CISA Certification: Candidates must meet the following requirements before certification: - Pass the CISA Exam within the last five years. For a member to qualify for CISA certification, they must submit a completed application within five years from the date of initially passing the examination. - Have the relevant full-time work experience in the CISA Job Practice Areas. All experience must be verified independently with employers. This experience must have been gained within the ten

	years preceding the application date for certification or within five years of passing the examination. Submit the CISA Certification Application form.
Continuing Professional Development (CPD) Requirements	Attain and report an annual minimum of twenty (20) CPD hours
Application of Recognition of Prior Learning (RPL)	RPL will be awarded in line with this policy as outlined below: • Applicants who have the requisite number of years experience in this sector (at least ten years experience), without the underlying NQF Level 7 qualification may apply for a professional designation through recognition of prior learning. • Such applicants must formally submit proof of a Senior Certificate and evidence of experience to the ISACA SA Chapter. The professional body independently verifies all experience with employers. Successful applicants are still required to complete the membership/professional designation application form and submit to ISACA SA to apply for the designation.

Designation competences:

Job practice areas cover designation competences.
Job practice areas consist of domains, subtopics, and supporting tasks representing the work performed in information systems audit, assurance and control. These domains, subtopics and tasks are the result of extensive research, feedback, and validation from subject matter experts and prominent industry leaders from around the globe. The below job practice was organised by tested domains for the first time in the June 2019 CISA exam. The CISA exam contains 150 questions testing the 2019 job practice. The job practice domains, knowledge and supporting tasks are as follows:

Domain 1-Information Systems Auditing Process
Providing audit services following standards to assist organisations in protecting and controlling information systems. Domain 1 affirms member's credibility to offer conclusions on the state of an organisation's IS/IT security, risk and control solutions.

Domain 2-Governance and Management of IT
Identify critical issues and recommend enterprise-specific practices to support and safeguard the governance of information and related technologies.

Domain 3-Information Systems Acquisition, Development, and Implementation

Domain 4- Information Systems Operations and Business Resilience
Domains 3 and 4 offer proof not only of competency in IT controls but also the member's understanding of how IT relates to business.

Domain 5-Protection of Information Assets
Understanding Cybersecurity and understanding its principles, best practices and pitfalls

Supporting Tasks
- Plan audit to determine whether information systems are protected, controlled, and provide value to the organisation.
- Conduct audit per IS audit standards, and a risk-based IS audit strategy.
- Communicate audit progress, findings, results, and recommendations to stakeholders.

- Conduct audit follow-up to evaluate the sufficient address of risks.
- Evaluate the IT strategy for alignment with the organisation's strategy and objectives.
- Evaluate the effectiveness of IT governance structure and IT organisational structure.
- Evaluate the organisation's management of IT policies and practices.
- Evaluate the organisation's IT policies and practices for compliance with regulatory and legal requirements.
- Evaluate IT resource and portfolio management for alignment with the organisation's strategies and objectives.
- Evaluate the organisation's risk management policies and practices.
- Evaluate IT management and monitoring of controls.
- Evaluate the monitoring and reporting of IT key performance indicators (KPIs).
- Evaluate the organisation's ability to continue business operations.
- Evaluate whether the business case for proposed changes to information systems meet business objectives.
- Evaluate whether IT supplier selection and contract management processes align with business requirements.
- Evaluate the organisation's project management policies and practices.
- Evaluate controls at all stages of the information systems development lifecycle.
- Evaluate the readiness of information systems for implementation and migration into production.
- Conduct post-implementation review of systems to determine the meeting of project deliverables, controls, and requirements.
- Evaluate whether IT service management practices align with business requirements.
- Conduct periodic review of information systems and enterprise architecture.
- Evaluate IT operations to determine whether they are controlled effectively and continue to support the organisation's objectives.
- Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organisation's objectives.
- Evaluate database management practices.
- Evaluate data governance policies and practices.
- Evaluate problem and incident management policies and practices.
- Evaluate change, configuration, release, and patch management policies and practices.
- Evaluate end-user computing to determine the effective control of processes.
- Evaluate the organisation's information security and privacy policies and practices.
- Evaluate physical and environmental controls to determine the adequate safeguard of information assets.
- Evaluate logical security controls to verify the confidentiality, integrity, and availability of information.
- Evaluate data classification practices for alignment with the organisation's policies and applicable external requirements.
- Evaluate policies and practices related to asset lifecycle management.
- Evaluate the information security program to determine its effectiveness and alignment with the organisation's strategies and objectives.
- Perform technical security testing to identify potential threats and vulnerabilities.
- Utilise data analytics tools to streamline audit processes.
- Provide consulting services and guidance to the organisation to improve the quality and control of information systems.
- Identify opportunities for process improvement in the organisation's IT policies and practices.
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.

Institute of Chartered IT Professionals (ICITP)
ICITP focuses on the knowledge and practice of the IT profession through developing, supporting, regulating and promoting professional standards for technical, entrepreneurial and ethical competence in the Media, Information and Communication Technology. In contrast, ISACA SA focuses on information security, cybersecurity, IT assurance, IT risk management and IT governance. ISACA provides this through good practices frameworks such as COBIT 2019 provided by its knowledge centre, events, conferences and online training.

Institute of Information Technology Professionals South Africa (IITPSA)
IITPSA focuses on the study, science and application of Information and Communications Technologies (ICTs); defining and improving standards of ICT knowledge; supporting the formulation of effective policies on ICT and related matters; and extending the knowledge and understanding and usage of ICTs in the community. Whereas ISACA SA focuses on information security, cybersecurity, IT assurance, IT risk management and IT governance good practices provided by its knowledge centre, events, conferences and online training.

Furthermore, ISACA has MOUs in place with:
SAQA recognised professional bodies
- IITPSA
- ACFE SA;
- The Institute of Directors South Africa;

Other institutions
- The Ethics Institute;
- Wits Link Centre; and
- CISO Alliance.

The ISACA SA Chapter continually looks for opportunities to partner with professional bodies in South Africa.

3. CRITERIA FOR RECOGNISING A PROFESSIONAL DESIGNATION

Designation(s) to be Registered

Designation Title: Information Systems Audit Professional - ISAP (SA)

Designation Title: Information Security Management Professional - ISMP (SA)

Underlying qualification(s)	Bachelor of Commerce: Information Systems/Management/Business Information Systems/Informatics/Financial Accounting: • Bachelor of Commerce in Information and Technology Management (71889) • Bachelor of Commerce: Information Systems (4431) • Bachelor of Commerce in Business Informatics (101104) • Bachelor of Accounting (90622) • Bachelor of Commerce in Accounting Sciences (7033) • Bachelor of Accounting Science (5535) • Postgraduate Diploma: Management: Financial Accounting (15497) • Postgraduate Diploma in Accounting (5191)

	Bachelor of Science: Computer Science/Informatics/Information Technology/Mathematical Science • Bachelor of Science Honours: Computer Science (4503) • Bachelor of Science in Informatics (79786) • Bachelor of Science: Information Technology (50363) • Bachelor of Science in Information Technology (80887) • Postgraduate Diploma: Mathematical Sciences (66511) Bachelor of Arts: Humanities with Socio Informatics (71650) Bachelor of Technology: Financial Information Systems • Bachelor of Information Technology in Business Systems (97804) • National Diploma: Financial Information Systems (80163), or • Any other related NQF Level 6 qualification
Experiential Learning and Practical Experience	A minimum of five years relevant proven Information Security Management experience across the following domains: • Domain 1-Information Security Governance (24%); • Domain 2-Information Risk Management (30%); • Domain 3-Information Security Program Development and Management (27%); and • Domain 4-Information Security Incident Management (19%). If the applicant does not meet the 5-year experience requirement, he/she may opt to submit qualifying waivers for experience (up to a maximum of 3 years)
Board / Admission Examination / Assessment	CISM exam passed & CISM certification attained. CISM Exam: • The examination is open to all individuals who have an interest in information systems audit, control and security. All are encouraged to work toward and take the examination. • A committee sets the exam at ISACA HQ, and the computer-based exam is administered locally by a vendor. • The professional body sends all information required to apply for certification with their notification of a passing score to successful candidates. CISM Certification: • Candidates must meet the following requirements before certification: - Pass the CISM Exam within the last five years. For a member to qualify for CISM certification, they must submit a completed application within five years from the date of initially passing the examination. - Have the relevant full-time work experience in the CISM Job Practice Areas. All experience must be verified independently with employers. This experience must have been gained within the ten years preceding the application date for certification or within five years of passing the examination. - Submit the CISM Certification Application form.
Continuing Professional Development (CPD) Requirements	Attain and report an annual minimum of twenty (20) CPD hours.

Application of Recognition of Prior Learning (RPL)	RPL will be awarded in line with this policy as outlined below: Applicants who have the requisite number of 'years' experience in this sector (at least 10 'years' experience), without the underlying qualification may apply for membership or a professional designation through recognition of prior learning. Such applicants must formally submit proof of a Senior Certificate and evidence of experience to the ISACA SA Chapter. Successful applicants are still required to complete the membership/professional designation application form and submit to ISACA SA to apply for the designation.

Designation Competencies

Job practice areas cover designation competences.

Job practice areas consist of domains, subtopics, and supporting tasks representing the work performed in information systems audit, assurance and control. These domains, subtopics and tasks are the result of extensive research, feedback, and validation from subject matter experts and prominent industry leaders from around the globe. The below job practice was organised by domains tested for the first time on the June 2019 CISA exam. The CISA exam contains 150 questions testing the 2019 job practice. The job practise fields, and task and knowledge statements are as follows:

Domain 1-Information Security Governance
Establish or maintain an information security governance framework and supporting processes to ensure that the information security strategy aligns with organisational goals and objectives.

Domain 2-Information Risk Management
Manage information risk to an acceptable level based on risk appetite to meet organisational goals and objectives.

Domain 3-Information Security Program Development and Management
Develop and maintain an information security program that identifies, manages and protects the organisation's assets while aligning to information security strategy and business goals, thereby supporting an effective security posture.

Domain 4-Information Security Incident Management
Plan, establish and manage the capability to detect, investigate, respond to and recover from information security incidents to minimise business impact.