PEN TESTING STANDARDS SOUTH AFRICA

SEPTEMBER 2021

ACFE™

Association of Certified Fraud Examiners

South Africa Chapter #91

TABLE OF CONTENTS

SECTION A

1. OVERVIEW OF THE FORENSIC STANDARD FORUM

2. THE ACFE

2.1 Background on the ACFE SA Chapter

2.3 Applicability of Code

2.4 Standards of Professional Conduct

2.5 Standards of Examination

2.6 Standards of Reporting

3. ACFE CODE OF ETHICS

SECTION B

1. FORENSIC STANDARD FORUM

1.1 Forensic Industry Standard Forum

1.2 Trademarks and Copyright –

SECTION C

1. RECOMMENDED BEST PRACTISE METHODOLOGIES:

SECTION A

1. OVERVIEW OF THE FORENSIC STANDARD FORUM

The aim of the Forensic Standard Forum under the auspices of the Association of Certified Fraud Examiners, South Africa Chapter (ACFE SA) is to standardise scientific methodologies employed in the course of forensic investigations, which are carried out in conjunction with criminal or civil legislation. Such investigations include almost all disciplines and practices involved.

It is instrumental to lead the way in terms of setting standards in all the disciplines of forensics applied during any given investigation. Although there are well-known and international standards in most of the disciplines, some changes may be required to address the situation in South Africa and Africa in the context of our environment and applicable legislation and/or legal systems and frameworks.

Forensic scientists and criminal investigators need to be guided with acceptable standards and procedures for carrying out such examinations. This document sets forth standards for digital forensic practitioners in South Africa. Although the Association of Certified Fraud Examiners (ACFE) refers to Certified Fraud Examiners (CFEs), it recognises the fact that a strong association exists with forensic examiners and practitioners. All forensic disciplines will accordingly be included in the Forensic Standard Forum.

2. THE ACFE

2.1 Background on The ACFE SA Chapter

The need to raise the standard of fraud examination in South Africa and for a professional body not limited to a specific profession such as accounting or law, resulted in the establishment of a local chapter with the mission to provide a community environment in which local forensic examination practitioners can associate. Local membership provides several benefits including a network of experienced professionals; a training framework for practitioners with "how-to" guidance; technical updates and ethical standards; regular discussion forums on issues relevant to the local environment; annual workshops on fraud examinations; and a video library with case studies. This chapter is a body of individuals in South Africa from all industries, who all

have a single goal mind; the reduction of white-collar crime in South Africa.

(ACFE Professional Standards: www.acfesa.co.za)

2.2 The preamble of the ACFE SA

The ACFE is an association of professionals committed to performing at the highest level of ethical conduct. Members of the Association pledge themselves to act with integrity and to perform their work professionally.

Members have a professional responsibility to their clients, the public interest and each other; a responsibility that requires subordinating self-interest to the interests of those served.

These standards express basic principles of ethical behaviour to guide members in the fulfilling of their duties and obligations. By following these standards, all CFEs will be expected to, and all Associate members will strive to demonstrate their commitment to excellence in service and professional conduct.

2.3 Applicability of Code

The CFE Code of Professional Standards applies to all members of the ACFE. The use of the word "member" or "members" in this Code refers to Associate members as well as regular members of the ACFE.

2.4 Standards of Professional Conduct

a. Integrity and Objectivity

- Members will conduct themselves with integrity, knowing that public trust is founded on integrity. Members will not sacrifice integrity to serve the client, their employer or the public interest.
- Before accepting the fraud examination, members will investigate potential conflicts of interest. Members will disclose any potential conflicts of interest to prospective clients who retain them or their employer.
- Members will maintain objectivity in discharging their professional responsibilities within the scope of the engagement.
- Members will not commit discreditable acts and will always conduct themselves in the best interests of the reputation of the profession.

- Members will not knowingly make a false statement when testifying in a court of law or other dispute resolution forums. Members will comply with lawful orders of the courts or other dispute resolution bodies. Members will not commit criminal acts or knowingly induce others to do so.

b. Professional Competence

- Members will be competent and will not accept assignments where this competence is lacking. In some circumstances, it may be possible to meet the requirement for professional competence by use of consultation or referral.
- Members will maintain the minimum Continuing Professional Education (CPE) requirements as set out by the ACFE. A commitment to professionalism combining education and experience will continue throughout the member's professional career. Members will continually strive to increase the competence and effectiveness of their professional services.

c. Due Professional Care

- Members will exercise due professional care in the performance of their services. Due professional care requires diligence, critical analysis and professional scepticism in discharging professional responsibilities.
- Conclusions will be supported with evidence that is complete, reliable and relevant.
- Members' professional services will be adequately planned. Planning controls the performance of a fraud examination from inception to completion and involves developing strategies and objectives for performing the services.
- Work performed by assistants on a fraud examination will be adequately supervised. The extent of supervision depends on the complexities of the work and the qualifications of the assistants.

d. Understanding with Client or Employer

- At the beginning of a fraud examination, members will reach an understanding with those retaining them (client or employer) about the scope and limitations of the fraud examination and the responsibilities of all parties involved.
- Whenever the scope or limitations of a fraud examination or the responsibilities of the parties change significantly, a new understanding will be reached with the client or employer.

e. Communication with Client or Employer

- Members will communicate significant findings made during the normal course of the fraud examination to those who retained them (client or employer).

f. Confidentiality

- Members will not disclose confidential or privileged information obtained during the fraud examination without the express permission of proper authority or order of a court. This requirement does not preclude professional practice or investigative body reviews as long as the reviewing organisation agrees to abide by the confidentiality restrictions.

2.5 Standards of Examination

a. Fraud Examinations

- Fraud Examinations are conducted by professionals / Fraud Examiners defined as follows: Individuals who make use of specialised skills in the prevention, detection and investigation of fraud and white-collar crimes. Fraud Examiners are registered on the occupational framework as a formal occupation with Organising Framework of Occupations (OFO) code 2019-242215.
- Fraud examinations will be conducted in a legal, professional and thorough manner. The fraud examiner's objective will be to obtain evidence and information that is complete, reliable and relevant.
- Members will establish predication and scope priorities at the outset of a fraud examination and continuously re-evaluate them as the examination proceeds. Members will strive for efficiency in their examination.
- Members will be alert to the possibility of conjecture, unsubstantiated opinion and bias of witnesses and others. Members will consider both exculpatory and inculpatory evidence.

b. Evidence

- Members will endeavour to establish effective control and management procedures for documents. Members will be cognizant of the chain of custody including origin, possession and disposition of relevant evidence and material. Members will strive

to preserve the integrity of relevant evidence and material.

- Members' work product may vary with the circumstances of each fraud examination. The extent of documentation shall be subject to the needs and objectives of the client or employer.

2.6 Standards of Reporting

a. General

- Members' reports may be oral or written, including fact witness and/or expert witness testimony, and may take many different forms. There is no single structure or format that is prescribed for a member's report; however, the report should not be misleading.

b. Report Content

- Members' reports will only contain information based on data that is sufficient and relevant to support the facts, conclusions, opinions and/or recommendations related to the fraud examination. The report will be confined to subject matter, principles and methodologies within the member's area of knowledge, skill, experience, training or education.
- No opinion regarding the legal guilt or innocence of any person or party will be expressed.

3. ACFE CODE OF ETHICS

All CFEs must meet the rigorous criteria for admission to the ACFE. Thereafter, they must exemplify the highest moral and ethical standards and must agree to abide by the bylaws of the ACFE and the CFE Code of Professional Ethics.

- An ACFE Member will, at all times, demonstrate a commitment to professionalism and diligence in the performance of his or her duties.
- An ACFE Member will not engage in any illegal or unethical conduct or any

activity which would constitute a conflict of interest.

- An ACFE Member will always exhibit the highest level of integrity in the performance of all professional assignments and will accept only assignments for which there is a reasonable expectation that the assignment will be completed with professional competence.
- An ACFE Member will comply with lawful orders of the courts and will testify to matters truthfully and without bias or prejudice.
- An ACFE Member, in conducting examinations, will obtain evidence or other documentation to establish a reasonable basis for any opinion rendered. No opinion w be expressed regarding the guilt or innocence of any person or party.
- An ACFE Member will not reveal any confidential information obtained during a professional engagement without proper authorisation.
- An ACFE Member will reveal all material matters discovered during an examination which, if omitted, could cause distortion of the facts.
- An ACFE Member will continually strive to increase the competence and effectiveness of professional services performed under his or her direction.

SECTION B

1. FORENSIC STANDARD FORUM

The list of Forensic Standards guidelines needs to be dictated to by discipline-specific specialists. To assist members of the forum to implement standards, qualification and ethics, it would be beneficial to standardise the input required in order to build the framework across all disciplines.

1.1 Forensic Industry Standard Forum

Discipline/title	Penetration Testing (Pen Testing)
Describe discipline	A pen test simulates the actions of an external and/or internal cyber attacker that aims to breach the information security of the organisation. Using many tools and techniques, the penetration tester (ethical hacker) attempts to exploit critical systems and gain access

	to sensitive data. Pen testing is a technology science process, also called ethical hacking, and is the practice of testing a computer system, network, software or web application to find security vulnerabilities that an attacker could exploit. Pen testing can be automated with software applications or be performed manually. Either way, the process involves gathering information about the target before the test; identifying possible entry points; attempting to break in, either virtually or for real; and reporting back the findings.
Science Application	Republic of South Africa
Purpose of the discipline	Pen testing is the process of identifying security vulnerabilities in computing applications by evaluating the system, network, or software with various malicious methodologies. In the end, the purpose is to identify security weaknesses in a network, machine, application, or software. The end-purpose of this test is to secure critical information from outsiders who continually try to gain unauthorised access to the system.

1.1.1 Criminalistics

Applicable organisations that deliver the above services must comply with policies and directions and all applicable South Africa laws, regulations and guidelines, including, but not limited to:

- Constitution of the Republic of South Africa Act 86/1996
- Human Rights Commission Act 56/1994
- Consumer Protection Act 68 of 2008
- South African Law of Contract A – 2012
- Cyber Crimes and security bill

- Common-Law – South Africa
- Proceeds of Crime Act 2002
- Prevention and Combating of Corrupt Activities Act 12 of 2004
- Criminal Procedure Act, Act 51 of 1977
- Financial Intelligence Centre Act 38 of 2001
- Investigation of Serious Economic Offences Amendment Act 46 of 1995
- Prevention of Organised Crime Act 121 of 1998
- Prevention of Organised Crime Amendment Act 24 of 1999
- Prevention of Organised Crime Second Amendment Act 38 of 1999
- Promotion of Access to Information Act 2 of 2000
- Promotion of Access to Information Amendment Act 54 of 2002
- Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002
- Protection of personal information Act 4 of 2013
- Occupational Health and Safety Act 85 of 1993 as amended
- Taxation Laws Amendment Act of 2012
- Customs and Excise Act 91 of 1964
- King-III and IV, for ethical leadership and good corporate governance

Applicable organisations that delivered the above discipline services, should always subject him or her to the law, regulations and guidelines of the legislation of the country in which the service is rendered.

1.1.2 Ethics in Administration

The code reflects the highest possible standards applicable to all organisations and embraces the principles of personal integrity and professionalism.

The applicable organisation that delivers the above discipline services expressly agrees to the following ethics prescribed by the ACFE:

- To behave honestly and with integrity
- To diligently execute the job description
- To execute any function or instruction only by way of lawful interactions and/or conduct

- To promote and uphold the good corporate reputation of all stakeholders
- To treat both internal and external clients with professionalism and respect
- To never take improper advantage of inexperience, lack of education, youth, lack of sophistication, language barrier or ill health of any client
- To disclose and take reasonable steps to avoid any conflict of interest
- Not to provide false or misleading information in response to a request for information from any of the key stakeholders
- To promote public confidence in the organisation and all its stakeholders through fair and conscientious dealings refraining from any deceit, misrepresentation, willful non-disclosure, undue influence or other harmful practice
- Never to seek personal gain or make any secret profit, acquire any financial interest or benefit in any matter entrusted to you
- To submit a detailed report after the services delivery
- To discuss findings in a professional way with clients
- To comply with the existing prescribed National and International ethics standards for the above science discipline
- Liaising with role players in law enforcement and intelligence agencies, where necessary
- To assist with preparing cases for clients, where necessary
- To provide evidence at disciplinary hearings and in criminal/civil courts, where necessary

1.1.3 Compliance with the code

The applicable organisations that deliver the above discipline services, hereby agreed that the reputation and future of the discipline and all stakeholders depend on both technical and ethical excellence. It is important that the applicable organisations not only adhere to the principles expressed in this Code, but also encourage and support adherence to the code by science organisations that deliver some of these discipline services.

Applicable organisations are accordingly also obliged to immediately inform the ACFE SA Forensic Industry Standard forum of transgressions by applicable organisations that delivered these discipline services, once becoming aware of such misconduct.

1.1.4 Non-compliance with the code

Adherence to this code is compulsory and any transgression will be viewed as gross misconduct resulting in the termination of the transgressor's ACFE SA membership.

Applicable organisation who delivers the above discipline services, expressly agree to the following:

- To maintain a sound knowledge of the code of conduct, policies and objectives of the ACFE SA chapter.
- To conduct the above science services in a manner that will not detract from or damage the reputation of the ACFE SA chapter or its authorised representatives in any way.
- That there should be clear principles of good practice outlining how applicable organisations should conduct the above science services.
- That drawing on the widest range of good practice, this code will further regulate applicable organisations' methodologies of addressing the above science services to help ensure that the highest standards are applied and maintained.

1.1.5 Application

This Code applies to all applicable organisations engaged in or acting on behalf of consulting companies carrying out duties involving the comprehensive Information Security services.

1.1.6 Breach of the Code of Conduct

A breach of the Code of Conduct will be investigated and, where appropriate, dealt with under disciplinary procedure.

1.1.7 Provisions General Conduct

Applicable organisations to which the Code applies must not:

- Exceed their actual authority or hold them out as having any authority not provided by legislation.
- Act in any way which exceeds the actual limits of their powers.
- Misuse their official position for any benefit or gain for themselves or another.

1.1.8 Legislation and Other Guidance

- Always Comply with existing legislation.
- Always comply with the existing prescribed National and International ethics standards for the above discipline.
- King-III and IV sets the tone for ethical leadership and good corporate governance. Strategy, risk, performance and sustainability are recognised as the cornerstones of good business and have become inseparable. IT Governance is addressed, with an emphasis on risk mitigation and protection of information. In exercising their duty of care, leadership is called upon to ensure that prudent and reasonable steps have been taken with regard to IT governance.
- Make use of existing methods against the loss of any data.
- Ensure that all information which may be relevant is analysed.
- Observe all other applicable legislation and internal and external guidance.
- Obtain written permission before the service is conducted.

1.1.9 Information

Applicable organisations to which the Code applies must not under any circumstances:

- conceal or fabricate information or knowingly allow any information to be fabricated or concealed;
- accept or offer any inducement, bribe or other advantage to anyone;
- use any information gathered in the course of their services for personal gain or coercion or otherwise misuse such information.

1.1.10 Disclosure of Interests

Applicable organisations must declare any circumstances or interests which may affect their ability to conduct a pen testing service independently or objectively.

1.1.11 Safeguarding Information

Applicable organisations must treat all information gathered or received during the course of a pen testing service as confidential and must not deliberately or negligently:

- disclose and discuss such information to an unauthorised third party, unless the disclosure is prescribed by law;
- reveal the source of information to an unauthorised third party, unless the disclosure is prescribed by law.

1.1.12 Personal Injury and Damage to Property

- Applicable organisations must exercise all reasonable care to prevent injury or loss or damage to public or private property and must not enter the public or private property except on the invitation of the occupier or responsible person or police officer.
- Deliberately or negligently destroy or damage any property or information.
- Deliberately or negligently destroy or damage any network, business, operational or technical deliverables.
- Use or threaten physical violence towards a colleague or member of the public.
- Applicable organisations must conduct themselves with integrity.
- Applicable organisations must be fair, honest and impartial in dealings, and treat others with dignity and respect.
- Applicable organisations must be aware of obligations to maintain the confidentiality of information. They must not use this information for personal gain, nor to the detriment of its stakeholders.
- Applicable organisations must exercise due skill, care and diligence in performing services and acknowledge their responsibility to maintain the currency of our knowledge, skills and technical competencies.

1.1.13 Application of the Code of Conduct

- It is important to recognise that in applying this Code of Good Practice, the personal characteristics of honesty, sincerity, impartiality and trustworthiness are key guiding attributes.
- The effectiveness of the parties relies on applicable organisation responsibility for their own behaviour and is committed to the standards.

1.1.14 Integrity

Applicable organisations should act with honesty, sincerity and integrity in their approach to their services.

1.1.15 Conflicts of interest

Applicable organisations should be free of any interest (financial or otherwise) which might be regarded as being in conflict or incompatible with their integrity and objectivity.

1.1.16 Confidentiality

Applicable organisations must protect the confidentiality of information acquired in the course of their service.

1.1.17 Fair and honest dealing

Applicable organisations must be fair and not allow bias or prejudice to influence or override their objectivity in academic, research, administrative, business or management matters.

1.1.18 Ethical behaviour

- Applicable organisations should conduct themselves in a manner which is consistent with the ACFE intentions, reputation and functions for which it was created. Applicable organisations should refrain from any conduct which might bring discredit to the ACFE.
- They should not allow dishonesty, personal prejudice or bias to influence the conduct of their employment.
- They should not accept gifts, benefits or hospitality if their nature and value may be seen as compromising their objectivity and influencing them in their official capacity.
- Their actions should be fair, honest and truthful.
- They should avoid actual or perceived conflicts of interest.
- They should not condone the use of any information which is misleading, false or deceptive.
- They should conduct themselves with care and skill and ensure their actions do not conflict with the requirements of integrity and objectivity of any Act.
- They should not use confidential or other information for personal advantage or for the advantage of another.

i) Knowledge and Skills – Pen Testing	
• **Formal education**	• Grade 12
• **Education and technical training in Pen Testing**	• Certified training and education at accredited recognised institute • Any computer science qualification Academic and trained background based on one or more of the following: – Certified Information System Security Professional (CISSP) – Certified Information Security Manager (CISM) – Certified Ethical Hacker (CEH) – Computer Hacking Forensic Investigator (CHFI) – Certified Incident Handler (CIH) – Certified Security Specialist (CSS) – Certified Security Analyst (CSA) – Project Management IT Security (PMIS) a. Recommend – Certified Fraud Examiner b. Membership of the ACFE
• **Experience and knowledge**	5 Years Experience and or knowledge in the following environments: – Information Security Management (ISM) – Certified Information System Security Professional (CISSP) – Certified Information Security Manager (CISM) – Data analyses – Pen testing – Software application evaluation – Network inspection

	– Target Scanning / Vulnerability Assessment – Communication Analysis – Information Gathering / Discovery – External Assessment – Methodology Framework (ISO 27000 Itil) – Policies and Governance – Software development – Mobile App assessment – Computer Forensic Investigations – Network Forensic Investigations – Business Impact Analysis – National and International Ethics Standards / Guidelines & Methodology – Vulnerability Assessment and Testing

1.2 Trademarks and copyright

The following training materials are protected by trademarks and copyright:

- Certified Ethical Hacker (CEH)
- Computer Hacking Forensic Investigator (CHFI)
- Certified Information Security Manager (CISM)
- Certified Information Security Officer (CISO)
- Certified Information System Security Professional (CISSP)
- Certified Incident Handler (CIH)
- Certified Security Specialist (CSS)
- Certified Security Analyst (CSA)
- Project Management IT Security (PMIS)
- PECB Certified ISO / IEC 27032 lead cyber security manager

SECTION C

1. RECOMMENDED BEST PRACTISE METHODOLOGIES

A best practice is a technique or methodology that, through experience and research, has proven to lead reliably to a desired result. A commitment to using the best practices in any field is a commitment to using all the knowledge and technology at one's disposal to ensure success.

The framework is underpinned by the internationally recognised standards and guidelines including but not limited to:

- The ISF Standard of Good Practice which addresses information security from a business perspective and focuses on the arrangements made by leading Organisation to keep the business risks associated with critical information systems under control.
- COBIT (Control Objectives for Information and Related Technology) – a generally applicable and accepted framework for good IT security and control practices.
- ITIL (Information Technology Infrastructure Library), in particular, Security Management, which focuses on the process of implementing security requirements identified in the IT Service Level Agreement, rather than considering business issues of security policy.
- Common Criteria / ISO 15408, which deals with functional and assurance requirements of specific IT equipment.
- GASSP (Generally Accepted System Security Principles) is a collection of security best practices.
- GMITS/ISO 13335 (Guidelines for the Management of IT Security) provides a conceptual framework for managing IT security.
- ISO 31000: the new International Risk Management Standard.
- ISO/IEC 31010:2009 – Risk Management – Risk Assessment Techniques.
- ISO Guide 73:2009 – Risk Management – Vocabulary.
- MISS (Minimum Information Security Standard with) emphasises the necessary procedures and measures for the protection of classified information.
- PCI-DSS 2.0 and 3.0: (Payment Card Industry Data Security Standard).
- King-III and IV, for ethical leadership and good corporate governance

Document compiled by: **Krappie Engelbrecht**

Date: **July 2021**

Document approved by: **Jaco de Jager**

Date: **September 2021**