

ACFE SA TECHNICAL
SURVEILLANCE COUNTER
MEASURES (TSCM)
STANDARDS



ACFETM

Association of Certified Fraud Examiners

South Africa Chapter #91

TABLE OF CONTENTS

- SECTION A4
- 1. OVERVIEW OF THE FORENSIC STANDARD FORUM5
- 2. THE ACFE.....5
 - 2.1 *Background on The ACFE SA Chapter*.....5
 - 2.2 *The preamble of the ACFE SA*.....6
 - 2.3 *Applicability of Code*6
 - 2.4 *Standards of Professional Conduct*.....6
 - 2.5 *Standards of Examination*8
 - 2.6 *Standards of Reporting*8
- 3. ACFE CODE OF ETHICS9
- SECTION B 11
- 1. FORENSIC STANDARDS FORUM 11
 - 1.1 *Criminalistics*..... 11
 - 1.2 *Ethics in Administration and the Protection of Personal Information Act*..... 12
 - 1.3 *Compliance with the code* 13
 - 1.4 *Non-compliance with the code*..... 13
 - 1.5 *TSCM Investigator Education and Training* 14
 - 1.6 *General practice - communication method applied by an investigator* 15
 - 1.7 *The most regular and complex challenges in the job*..... 16
 - 1.8 *Resources utilised by the assessor/investigator to solve problems or make decisions*..... 16
 - 1.9 *Planning cycle of the job*..... 16
 - 1.10 *Accountability*..... 16
- SECTION C 17
- 1. TSCM PROCEDURES 17
 - 1.1 *Introduction*..... 17
 - 1.2 *Information gathering*..... 17
 - 1.2.1 *Physical Source* 17
 - 1.2.2 *Non-Physical Source* 18
 - 1.2.3 *Threat* 18
 - 1.2.4 *Risk Analysis* 18
 - 1.2.5 *Threat Assessment*..... 18
- 2. COMMUNICATION SECURITY PROTECTION 20
 - 2.1 *Interception Techniques: “How?”* 20
 - 2.1.1 *Wireless Network* 20
 - 2.1.2 *Microphones (Hardwire Eavesdropping)*..... 20

- 2.1.3 *Radio Transmitters* 20
- 2.1.4 *Carrier Current Device (Babysitter)*..... 21
- 2.2 *Telephone Analysing (Analogue, Digital, VoIP, Etc.)* 21
 - 2.2.1 *Characteristics of Analogue Lines* 21
 - 2.2.2 *Characteristics of Digital Lines*..... 21
 - 2.2.3 *VoIP* 22
 - 2.2.4 *Telephone Threat*..... 22
 - 2.2.5 *SIM Cards* 22
- 2.3 *Protection of communication – counter electronic procedures* 23
- 3 **INVESTIGATIVE SEARCH FREQUENCY** 23
- 4 **TSCM OPERATIONAL CONTROL** 23
 - 4.1 *Operational Implementation*..... 23
 - 4.1.1 *In-House* 24
 - 4.1.2 *Outsourcing* 24
 - 4.2 *TSCM Equipment*..... 25
 - 4.3 *Outputs* 28
 - 4.4 *Interdisciplinary Forensic Science Standards* 28
 - 4.5 *Quality Control*..... 28
- 5 **STANDARDS** 29
 - 5.1 *Obtain and establish information on clients’ TSCM investigation requirements*..... 29
 - 5.2 *Determine electronic counter risks to clients’ assets* 30
 - 5.3 *Propose Solutions to meet Clients’ TSCM Requirements*..... 32
 - 5.4 *Manage TSCM Provision*..... 33
 - 5.5 *Carry out Technically Assisted & Physical Inspections of Premises*..... 34
 - 5.6 *Provide Post TSCM Inspection Support*..... 36
 - 5.7 *Maintain Knowledge and Understanding of Current TSCM Investigation Development*..... 36
 - 5.8 *Develop TSCM Techniques and Practices* 37
 - 5.9 *Maintain Knowledge and Understanding of Legislation, Regulation and Codes of Practice relevant to TSCM*..... 38
 - 5.10 *Present Information to Courts or other Hearings (South African Laws)* 39

RECORD MANAGEMENT		
Entity: ACFE SA		
Document Name: Technical Surveillance Counter Measures (TSCM)_V02		
Document Path: https://www.acfesa.co.za/ACFESA-Resources-anti-fraud		
Version Number	Date Published	Approval
V01	10 April 2022	ACFE SA Forensic Standards Forum
V02	31 March 2023	ACFE SA Forensic Standards Forum

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 follow: 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 will 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 STANDARDS FORUM

The list of forensic science standards guidelines needs to be dictated to by discipline specific specialists. To assist members of the science 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.

Forensic science discipline/title	Technical Surveillance Counter Measures (TSCM) “debugging”. This includes TSCM, mobile device analysis (Cellebrite or similar equipment) and Wi-Fi Security Assessments towards the protection of Intellectual Property (IP).
Describe forensic science discipline	Protection of Intellectual Property <ul style="list-style-type: none"> • Technical Surveillance Counter Measures Investigations (TSCM) “Debugging”
Forensic Science Application (Nationally and Internationally)	National and International
Purpose of the forensic science discipline	Due to the advancement of Global Corporate Competitiveness, there is a growing need amongst Corporate Institutions, especially at Executive Staff level, to protect all forms of Communication. It is of interest to note that more than 90% of the top listed Corporates in South Africa conduct a REGULAR programme of “Debugging”/TSCM

1.1 *Criminalistics*

An Investigator must comply with all ACFE SA chapter 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
- Electronic Communications and Transactions Act 25 of 2002
- 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
- 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

1.2 Ethics in Administration and the Protection of Personal Information Act

The primary goal of a TSCM investigator is the protection of Company Intellectual Property and sensitive information from theft and illegal dissemination.

Investigators have high visibility within the eyes of both internal and external clients and thus should always display appropriate personal and corporate values and behave in accordance with our strict behavioural code.

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

As a TSCM Investigator you expressly agree to the following:

- To behave honestly and with integrity.
- To diligently execute your job description
- To ensure prompt and efficient settlement of valid claims.
- 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 stake holders.
- 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.

- To not provide false or misleading information in response to a request for information from any of the key stakeholders.
- To promote public confidence in the organization and all its stake holders through fair and conscientious dealings refraining from any fraud, deceit, misrepresentation, wilful nondisclosure, undue influence, or other harmful practice.
- To never seek personal gain or make any secret profit, acquire any financial interest or benefit in any matter entrusted to you.
- To familiar yourself with the Protection of Personal Information Act and applicable legislation and to comply therewith.

1.3 Compliance with the code

As an Investigator it is hereby agreed that the reputation and future of the discipline, all stakeholders depend on both technical and ethical excellence. It is not only important that you adhere to the principles expressed in this Code, but also to encourage and support adherence to the code by other Investigators.

You are accordingly also obliged to immediately inform the ACFE of transgressions by other investigators once becoming aware of such misconduct.

1.4 Non-compliance with the code

Adherence to this code is compulsory and any transgression will be viewed as gross misconduct resulting in your ACFE membership being terminated.

As an Investigator you 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 investigations in a manner that will not detract from or damage the reputation of the ACFE SA Chapter or its authorised representatives in any way.
- To only collect material relevant to the TSCM investigation purpose. The collection must not involve the commission of a criminal offence or give rise to a civil action.
- To not enter any premises unlawfully and must not make any threat, promise or inducement when investigating.
- To avoid any actions which may unreasonably impinge on the privacy or other rights of other people.
- To collect and record only information relevant and responsive to the instructions from the client.

- To have in place appropriate measures to protect any material collected against loss, unauthorised access, use, modification, or disclosure.
- To store any material collected in a secure area and separately from other routine administrative information.
- To not divulge any information obtained during its instructions to any other person or company without the express written permission of the client he/she represent unless that disclosure is required by law.
- To maintain a log of all personnel accessing, using, or removing material collected in order to establish an audit trail, including when providing information to interstate employees or subcontractors. The log must include:
 - reason(s) for disclosure.
 - recipient's name and signature.
 - issuing officer's name.
 - time and date of access.
- To not directly or indirectly solicit, accept, offer, or give a benefit, gratuity, reward, gift, bribe, commission, or procurement fee, in connection with any activity associated with providing those services.
- To not discriminate against any person based on race, sex, colour, sexual orientation, political allegiance, impairment, or other unlawful grounds.
- To be subject to random file audit by the ACFE SA Chapter for compliance with this Code and must co-operate fully with access by the ACFE SA Chapter to files and data as required and answer any queries the ACFE SA Chapter may have in the conduct of an investigation.

1.5 TSCM Investigator Education and Training

The minimum qualification, experience, compliance requirements and operational requirements for the specific forensic science discipline. Training material/modules/qualifications to be specified, if exist. Note any additional specific special requirements for the specific forensic science discipline.

A) KNOWLEDGE AND SKILLS	
FORMAL EDUCATION	Grade 12
TECHNICAL/ LEGAL CERTIFICATION	Various Local and International TSCM Training Qualifications and verified practical experience.

EXPERIENCE	A minimum of 5 (five) years continuous relevant experience supported by a portfolio of evidence.	
B) COMPETENCIES IN ALL TSCM FIELDS		
FORENSIC SCIENCE KNOWLEDGE	GENERIC SKILLS	ATTRIBUTES
Crime scene management	Statistical techniques	Accuracy
Crime scene investigation	Computing skills	Assertiveness
Crime scene evidence	Report writing skills	Efficiency
Location and recovery of trace materials	Oral presentation skills	Honesty
Forensic analysis techniques	Information retrieval skills	Professionalism
Instrumental methods of analysis	Problem-solving skills	Self-discipline
Interpretation of analytical results	Team-working skills	Patience
Safe working procedures	Time management and organisational skills	
Quality assurance	Managing own learning	
Planning of casework related experiments	Communication skills	
Understanding relevant legal procedures	Conflict management skills	
Specific Knowledge to giving evidence (see details on pg. 38)	Interviewing skills	

1.6 General practice - communication method applied by an investigator

1.6.1 Verbal

- Making appointments with clients.
- Telephonic liaison with clients.
- Face-to face conversations.

1.6.2 Written Reports and Presentations

- Drafting or writing of written reports.
- E-mail feedback to clients or requesting of documentation.
- Preparation and presentation of presentations.

1.7 *The most regular and complex challenges in the job*

- Liaising with external role players.
- Diversity of client requirements regarding TSCM requests.

1.8 *Resources utilised by the assessor/investigator to solve problems or make decisions*

- Legal counsel.
- Company policies and procedures.

1.9 *Planning cycle of the job*

1.9.1 *Macro (Weekly)*

- Compiling planning notes and memoranda for tasks.
- Obtaining of all relevant information.

1.9.2 *Micro (Daily)*

- Scheduling of appointments with clients and Management of TSCM Team.
- Physical TSCM.
- Drafting of reports.

1.10 *Accountability*

1.10.1 *Investigator accountability*

- Making of appointments.
- Physical Investigation.
- Maintenance of Technical Equipment.

1.10.2 *Referral to Line Manager for approval*

- Reports and recommendations to clients.

SECTION C

1. TSCM PROCEDURES

1.1 Introduction

Due to the advancement of global corporate competitiveness, there is a growing need amongst Corporate Institutions, especially at executive staff levels, to protect all forms of communications.

Communication security encompasses all aspects of communications transmission - oral (spoken), written and data transmission, together with all relevant security techniques intended to achieve maximum possible protection of such transmission. More than 90% of the top listed corporates in South Africa conducts regular programmes of TSCM. Information is a corporate asset and managers, and staff have a responsibility to protect it.

Corporate Intelligence is the acquisition of relevant information, the collation, analysis and ultimately the evaluation of such information, aimed at identifying and thus protecting the Corporate from vulnerability to threat. It can also be used as a tool against a company.

This document addresses the practices, procedures, policies, systems, outputs, and standards for the following corporate intelligence:

Different levels of threat (ranging from petty theft, product extortion and fraud to economic espionage).

- Communication Security (to avoid corporate espionage).
- Implementation of corporate intelligence (countering the offensive activities aimed against a Corporate and must be considered essential in the overall security, policy and programme designed and implemented by that Corporate).
- Corporate Intelligence Agency operations albeit “in-house” or “outsourced”, functions both offensively and defensively in achieving optimal security for the Corporate.

1.2 Information gathering

The following are prime sources of information gathering:

1.2.1 Physical Source

- The human being, i.e., Management, Staff and often Associates - such sources transmit information either intentionally, frequently for personal gain or revenge, or unintentionally

“careless talk”. Irrespective, every effort should be taken to employ “the Need to Know” practices.

- Documents (Non-Oral).

1.2.2 Non-Physical Source

- Communication Interception.
- Data/Information Technology (Non-Oral).

1.2.3 Threat

Economic Espionage invariably incurs financial consequence. If successful, its high levels of sophistication, both nationally and internationally frequently incurs considerable consequences to not only corporate survival, but also Global and National economies. Regrettably, modern technological advances continually increase the sophistication of such espionage consequently requiring considerable advancement in Security Technology, Techniques and Training, Awareness, and Implementation, thus an ever-greater need for the highest levels of Corporate Intelligence and Pro-active Security Responses.

1.2.4 Risk Analysis

Risk analysis is the application of techniques employed to identify risks and the potential effect of such risk to the personnel and organisation being protected.

1.2.5 Threat Assessment

Threat assessment is the determination of the imminence and level of such threat to either personnel or elements of the organisation. In the event of such threats, as detailed previously, a Corporate requires formulated policies and contingency plans to guide the protective response of the Corporate. The overall protective strategy of the Corporate is a basic security policy decision achieved by Standing Operational Procedures (SOPs) designed and implemented to attain maximum possible security for the Corporate in any given environment. The following threat assessments are generally examined:

a. Potential Corporate Targets: “Who?”

- Listed Companies.
- Financial Institutions.
- Legal Practices.
- The Mining Industry.

- The Pharmaceutical Industry.
- Tender Boards/Committees.
- Small, Medium and Micro Enterprises (SMMEs) and e.g., Professionals working from home for Corporates or private entities.

b. Aim: “Why”?

- Intellectual Value.
- Acquisitions and Merges.
- Share Values.
- Strategic Planning for Business or Competitive Information.
- Conflict of Interest amongst Directors and Senior Management/Personnel.
- Recruitment (Head hunting) of Specialist or highly knowledgeable Personnel.

c. Potential areas of vulnerability: “Where?”

Internal

- Offices of Directors.
- Offices of Executive Management.
- Boardrooms.
- Specialist staff Workstations.
- All Conference- and associated Facilities’ locations.
- Directors’ and Executive Management’s vehicles.
- IT – Divisions.

External

- The Residences of Directors, Executive Management and identified Personnel employed on highly sensitive tasks.
- Specific Location Assignment.
- Selected Offices and Locations of persons closely associated with Contracts, Acquisitions, Legal and Financial Information/Activities, contracted to conduct business on behalf of the Corporate.
- Aircrafts and motor vehicles.

2. COMMUNICATION SECURITY PROTECTION

2.1 Interception Techniques: “How?”

The following technical and electronic instruments are most commonly used in the interception of verbal communication:

2.1.1 Wireless Network

A rogue access point, also referred to as rogue AP, is any Wi-Fi access point installed on a network that is not authorized for operation on that network nor is it under management of the network administrator.

Rogue access points often do not conform to wireless LAN (WLAN) security policies and, additionally, can allow anyone with a Wi-Fi device to connect to a network. These access points are usually created to allow a hacker to conduct a man-in-the-middle attack.

Rogue access points pose a security threat to large organisations with many employees. This is due to the ability for anyone with access to the premises to install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access by unauthorized parties into a secure network - while avoiding detection for extended periods of time.

2.1.2 Microphones (Hardwire Eavesdropping)

The “Hardwire Bug” comprises of three elements, namely:

- Microphone.
- Wire.
- Line Drive Amplifier.

The Microphone is normally installed in a non-conspicuous place in the room and is supplied with power by the eavesdropper, via the same wire that carries the Microphone Audio to the eavesdropper.

One does not always have to install a Microphone, as use can be made of items in the room, e.g. the Telephone Microphone, Intercom Systems, Television System and Radio Speakers can be adapted.

2.1.3 Radio Transmitters

A Transmitter is one of the most versatile and flexible means of gathering information and comes in various shapes and sizes.

The ideal type of Transmitter is one as small as possible, having a small signal (low watts), so that it is difficult to detect. Requiring the smallest of power sources and using the highest frequency possible, enables the use of a shorter antenna (i.e., VHF – UHF).

2.1.4 Carrier Current Device (Babysitter)

This Transmitter is connected into the electrical system of the target building. The Babysitter can be installed anywhere along the electrical system of the target building but must be on the same phase. This makes it difficult to detect the eavesdropper.

The Transmitter can be disguised in various things in the room without being detected, for example as a Plug Adapter. Once plugged into main sockets, the Transmitter will continuously transmit conversations using the power from the mains – to a receiver.

2.2 Telephone Analysing (Analogue, Digital, VoIP, Etc.)

Many people are under the impression that it is only their telephone calls that can be monitored, not knowing that what they say after the telephone is “hung up”, may also be overheard via the same Telephone Instrument. This is possible by using any one of the Microphones in the Telephone.

Whatever ones needs, Telephone Transmitters provide the ability to discreetly and automatically transmit all telephone conversations. These are easily installed either on the Telephone Wire, in the Telephone Socket or within the Instrument itself. Telephone users will have absolutely no indication of their presence.

2.2.1 Characteristics of Analogue Lines

- Information represented by constantly and smoothly varying voltage, current, amplitude, or frequency of waves and pulses.
- Do not switch suddenly between levels.
- The transmitter signal varies in relation to and is analogous (similar) to the original signal.
- With an Amplifier or a Telephone Instrument a person can listen to the audio on the line.

2.2.2 Characteristics of Digital Lines

- In Audio, signals characterised by a sequence of unique pulses or digital numbers corresponding to a particular value of the Audio Signal at a specific moment of time, must be converted to Analogue to be intelligible to humans.
- With a voice logger installed, Digital Telephones can be tapped on a limited basis.
- The voice logger must be operated by one person with a security clearance. The room must be locked with a security lock and proper access control measures in place.

2.2.3 VoIP

Voice over IP (VoIP, or voice over Internet Protocol) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are *IP telephony*, *Internet telephony*, *voice over broadband (VoBB)*, *broadband telephony*, and *broadband phone*.

A major development that started in 2004 was the introduction of mass-market VoIP services using existing broadband Internet access, by which subscribers place/receive telephone calls in much the same manner as they would via the public switched telephone network (PSTN). Full-service VoIP phone companies provide inbound and outbound service with Direct Inbound Dialling. Many offers unlimited domestic calling for a flat monthly subscription fee.

Dedicated VoIP phones connect directly to the IP network using technologies such as wired Ethernet or wireless Wi-Fi. They are typically designed in the style of traditional digital business telephones.

Irrespective of the technology used, all these systems are vulnerable and vulnerable via the latest software tools which enables theft of data as easy as browsing the web. Currently very few network security products are available in the market that can understand both the working and functionality of VoIP devices and VoIP technology, and which can provide added security features to ensure secure communication between two or more VoIP communication channels.

2.2.4 Telephone Threat

- The Telephone Transmitter is in the Telephone or Online and uses Telephone Power.
- Audio Transmitter in Telephone or room, Self-Powered.
- Telephone Notification.
- Hidden Microphone in Telephone or Online in the Office.
- Room and Telephone Listening Device in Telephone or Online in the Office.
- Telephone Tap Online.

2.2.5 SIM Cards

Sim cards can be placed into multi-plugs, thereby allowing eavesdropping from anywhere in the world by connecting remotely or calling into the device and even recording conversations in a room, provided the plug is switched on.

2.3 Protection of communication – counter electronic procedures

In conducting a Counter Measures Programme, the following services are implemented:

- A comprehensive Threat Assessment will be made for all designated target areas and a plan developed to best implement the TSCM.
- A full Radio Frequency Spectrum Analysis will be performed to check for hidden Room Transmitters and Telephone connected Transmitters.
- Electrical Power Lines and other Lines will be inspected with specialised equipment in order to locate Line “Carrier Current Device”, “VLF Transmitters”.
- A thorough Physical Search will be conducted in all designated target areas.
- A complete Electronic Analysis and Physical Inspection will be accomplished on all target areas: Telephones, Incoming Telephones, and Incoming Telephone Lines.
- Testing for Active and Passive Devices in respect of Telephones and Intercommunication Systems and Equipment.
- Testing for Rogue Wi-Fi devices

3 INVESTIGATIVE SEARCH FREQUENCY

In attempting to achieve maximum possible security provision, the Investigation should be conducted within the following programmed frequency:

- Overall Facilities Sweep: Conducted Twice Yearly via a full Physical Sweep of all Offices and Facilities and to include Marking/De-marking of Wire Cables.
- To assist in the identification of Offices and Locations considered to be most vulnerable i.e., Directors’ Offices, Executive Management Offices, Specialist Personnel Offices, Boardrooms, PA Offices etc., these should be identified and given a Threat Rating Identification e.g., “Threat Level 3”.
- Such Offices and Locations undergo a Daily, Weekly Silent Sweep and on a Monthly Basis an Overall Facilities Full Physical Sweep.

4 TSCM OPERATIONAL CONTROL

Due to the sensitivity, specialisation and security implications of these investigations’ security, control and management should be delegated to qualified “Crime Intelligence Security Personnel” only.

4.1 Operational Implementation

TSCM can be implemented in two ways:

4.1.1 In-House

Through extensive in-depth research and investigation, it has been determined that in-house implementation is not advisable due to:

- Constant improved technical development of TSCM Equipment; thus, increased sophistication of techniques employed by the perpetrators.
- Additional training of personnel to keep up to date with frequently upgraded or new equipment, together with regular continuation training required to achieve and maintain operational efficiency.
- The need to have existing equipment upgraded/re-calibrated at least annually to maintain operational efficiency. Currently this can only be obtained by returning the equipment to the manufacturers. Yet, this service is not available in South Africa.
- When considering the financial implications of implementing the above, together with the considerable expenditure of purchasing specialist equipment and selection and training of personnel, it was found to be non-cost effective. Consequently, it is considered preferable to outsource this service.
- Personnel can conduct TSCM tasks with company equipment “moonlighting”.

4.1.2 Outsourcing




The following should be implemented when outsourcing for TSCM:

Obtain at least three (3) tender proposals from recognised Specialist Agencies in the field of TSCM. This might also not be an option due to the sensitive nature of certain tasks. These tenders must be submitted based on a detailed Brief compiled and issued by the nominated Manager, and requiring:

- Full Company Background of the Submitting Agency.
- Details of Specialist Qualifications of the Agencies’ personnel undertaking the Investigation.
- Details of the Specialist and Non-Specialist Equipment to be used in conducting the Sweep and Investigation.
- Areas, Locations and Equipment to be investigated.
- Frequency of Sweeps and Investigations.
- Full costing.
- An agreement by the Agency, that “should they be appointed to conduct the investigation, they agree to undergo Vetting and Clearance at their “Own Cost”, as a condition of appointment”.


4.2 TSCM Equipment

Only relevant equipment is used in performing different tasks, of which the following types can be used. There is also other similar equipment available in the global market which could provide the required quality of service.

DESCRIPTION	APPLICATION	PICTURE
1. OSCOR BLUE	Spectrum Analyser	
2. MESA (MOBILITY ENHANCED SPECTRUM ANALYSER)	DETECTS: RF Wi-Fi, Bluetooth, Cell phones and Illicit transmissions	
3. A.N.D.R.E DE LUXE (ADVANCED NEAR FIELD DETECTION RECEIVER)	Detects nearby ambient RF energy	

DESCRIPTION	APPLICATION	PICTURE
4. RAPTOR RXi	Ultra-fast scanning countersurveillance receiver	
5. KESTREL TSCM® PROFESSIONAL SOFTWARE	Highly evolved TSCM specific, operator centric SDR application	
6. TALAN 3.0 DPA-7000	Telephone and line Analyser	
7. ORION 2.4 NON-LINEAR JUNCTION DETECTOR	Detects electronic semiconductor components in walls, floors, ceilings, fixtures, furniture, containers, or other surfaces.	

DESCRIPTION	APPLICATION	PICTURE
<p>9. BLOODHOUND</p>	<p>To test for hidden and live microphones on telephones and lines</p> <ul style="list-style-type: none"> • Cable tracing. • Carrier Current device detection. Physical inspection and evaluation of all suspect areas and fixtures. 	
<p>10. VIDEO POLE CAMERA</p>	<p>White LED illumination for colour inspection in dark areas, i.e., drop ceilings, behind immovable objects, around corners, other difficult to reach areas and in dark situations</p>	
<p>11. SEEK SHOTPRO THERMAL IMAGING CAMERA</p>	<p>Most advanced thermal imaging camera for professionals</p>	

DESCRIPTION	APPLICATION	PICTURE
12. CELLEBRITE	Universal Forensic Extraction Device (UFED) Touch Ultimate	

4.3 *Outputs*

All investigations are concluded with a thorough report to the client, indicating:

- Findings of the investigation.
- Shortcomings in the client's physical security measures that can facilitate eavesdropping attempts.
- Identified and potential eavesdropping threats and scenarios.
- Treated as a Crime Scene due to the specific Laws when eavesdropping devices are discovered.

4.4 *Interdisciplinary Forensic Science Standards*

Please indicate whether national or international standards for your specific forensic science discipline exist. In the absence of any standards, please share your views in terms of minimum standards a company should comply with:

- International Standards aligned with the South African Legal and Judiciary systems

4.5 *Quality Control*

How do you maintain exact outcomes in terms of consistency, quality, and succession?

Investigators should undertake the following:

- Submit themselves to polygraph tests to affirm that they have not and will not install any devices on the client's premises.

- If eavesdropping equipment is found on the client's premises, our investigators undertake to subject themselves to polygraph testing, in order to substantiate truthfulness in respect of who is responsible for planting the eavesdropping device.
- Allows the client to have all our equipment checked prior to and after the investigation, to ensure that no eavesdropping devices are taken onto the client's property by our investigators.

Should any eavesdropping equipment be found, the steps listed below will be followed:

- The Executives/Legal department will be informed and consulted in managing the situation
- The device will not be removed.
- In conjunction with the client, investigators will manage the situation to establish the origin of the device (Crime scene standards according to the collection of evidence).

5 STANDARDS

There are 10 standards that sets out the skills, knowledge and understanding of TSCM operations:

5.1 *Obtain and establish information on clients' TSCM investigation requirements*

This unit consists of three elements:

- a. Respond to clients who require TSCM services.
- b. Record details of clients' TSCM aims and objectives.
- c. Identify clients' potential TSCM requirements.

5.1.1 *Performance Criteria: Respond to clients who require TSCM services*

You must be able to:

- a. Respond effectively and promptly to clients, using appropriate methods of communication suitable to your clients.
- b. Confirm the authority and responsibility of the person seeking TSCM services.
- c. Confirm your understanding of your clients' requirements.
- d. Explain and confirm your clients understanding of the scope and limitations of the actions that you and your organisation can take.
- e. Maintain the security and confidentiality of information relevant to clients and their TSCM objectives.

5.1.2 *Performance Criteria: Record details of clients' TSCM aims and objectives*

You must be able to –

- a. Record details accurately and in a retrievable format.

- b. Record relevant information sufficient to develop proposals to meet the aims and objectives of clients' TSCM.
- c. Take prompt and appropriate action to deal with identified loopholes of information.
- d. Maintain the security and confidentiality of information relevant to clients and their security objectives.

5.1.3 Performance Criteria: Identify clients' potential TSCM Requirements

You must be able to –

- a. Liaise with appropriate persons to identify clients' TSCM requirements.
- b. Ensure that you have sufficient information to identify clients' potential TSCM requirements.
- c. Take account of potential constraints when identifying clients' TSCM.
- d. Provide sufficient details and supporting information to your clients to enable them to make informed decisions about their TSCM requirements.
- e. Provide clients with advice on the implications of accepting, modifying or rejecting their TSCM.
- f. Maintain the security and confidentiality of information relevant to your clients and their TSCM objectives.

5.2 Determine electronic counter risks to clients' assets

This unit consists of four elements:

- a. Identify and evaluate clients' assets
- b. Identify and evaluate threats to clients' assets
- c. Identify and evaluate electronic counter vulnerabilities in clients' current security arrangements
- d. Determine the risks to the clients' assets

5.2.1 Performance Criteria: Identify and evaluate clients' assets

You must be able to –

- a. Gather relevant information from different sources sufficiently to assist in identifying and evaluating clients' assets.
- b. Collate and take account of all relevant information to support the evaluation of assets.
- c. Use logical and systematic analysis of information to evaluate clients' assets.
- d. Determine the potential impact to your clients through the loss or compromise of identified assets.

- e. Prioritise the value of identified assets in accordance with service criteria agreed with your clients.
- f. Evaluate relevant information according to its usefulness.
- g. Maintain the security and confidentiality of information relevant to your clients' assets.

5.2.2 Performance Criteria: Identify and evaluate threats to clients' assets

You must be able to –

- a. Gather relevant information from different sources sufficiently to identify and evaluate threats to clients' assets.
- b. Collate and take account of all relevant information to support the evaluation of threats, including the sources of threats.
- c. Use logical and systematic analysis of information to evaluate threats to the security of clients' assets.
- d. Categorise possible threats and vulnerabilities on assets and potential security measures.
- e. Evaluate relevant information to determine its usefulness.
- f. Maintain the security and confidentiality of information relevant to threats to your clients' assets.

5.2.3 Performance Criteria: Identify and evaluate electronic counter vulnerabilities in clients' current security arrangements

You must be able to –

- a. Gather relevant information from different sources sufficiently to identify and evaluate vulnerabilities in clients' security arrangements.
- b. Collate and take account of all relevant information to support the evaluation of vulnerabilities.
- c. Use logical and systematic analysis of information to identify and evaluate vulnerabilities in clients' security arrangements.
- d. Evaluate relevant information according to its usefulness.
- e. Identify actual and potential electronic counter vulnerabilities in clients' electronic counter security arrangements.
- f. Maintain the security and confidentiality of information relevant to the vulnerabilities in your clients' security arrangements.

5.2.4 Performance Criteria: Determine the risks to the clients' assets

You must be able to –

- a. Take account of sufficient valid information to determine the risks to the protection of clients' assets.
- b. Determine the levels of actual and acceptable risk to clients' assets, based on systematic analysis and evaluation of threats and vulnerabilities.
- c. Inform clients promptly of situations where there are risks to assets.
- d. Record information in a suitable and retrievable format.
- e. Maintain the security and confidentiality of information relevant to risks to clients' assets.

5.3 Propose Solutions to meet Clients' TSCM Requirements

This unit consists of three elements:

- a. Research options to meet clients' TSCM requirements.
- b. Determine potential costs, benefits, and effectiveness of options.
- c. Make recommendations to the clients for meeting their TSCMI requirements.

5.3.1 Performance Criteria: Research options to meet clients' TSCM requirements

You must be able to –

- a. Confirm that you have sufficient, complete, and accurate details of the TSCM requirements of your clients.
- b. Research relevant data required to meet clients' requirements based on the evaluation of risks.
- c. Consider options that are objective and that have no bias.
- d. Identify and record details of constraints that may have an impact on the proposed options.
- e. Maintain the security and confidentiality of information relating to your clients' data.
- f. Constraints: operational capabilities and limitations, financial, time limits, availability of resources.

5.3.2 Performance Criteria: Determine potential costs, benefits, and effectiveness of options

You must be able to –

- a. Confirm you have sufficient accurate information on which to determine potential costs, benefits, and effectiveness of proposed options, including possible constraints.
- b. Identify, assess, and record the details of any areas of concern affecting the potential effectiveness of proposed options.
- c. Maintain the security and confidentiality of information relating to your proposals.

5.3.3 Performance Criteria: Make recommendations to the clients for meeting their TSCM requirements

You must be able to –

- a. Prepare recommendations that have the potential to meet the TSCM requirements of your clients.
- b. Provide complete and accurate details of potential resource costs, benefits, effectiveness, limitations, and constraints of recommendations.
- c. Provide recommendations of security options in the agreed format to the specified person within agreed timeframes.
- d. Provide sufficient details and supporting information to your clients to enable them to make informed decisions about your recommendations.
- e. Provide the clients with considered advice on the implications of accepting, modifying or rejecting TSCM Investigation options.
- f. Take account of your clients' culture and nature of business.
- g. Maintain the security and confidentiality of information relating to your clients.

5.4 Manage TSCM Provision

This unit consists of three elements:

- a. Manage the provision of TSCM against agreed specifications.
- b. Manage TSCM against agreed operational requirements.
- c. Assess the effectiveness of implementing TSCM.

5.4.1 Performance Criteria: Manage the provision of TSCM against agreed specifications

You must be able to –

- a. Confirm that appropriate persons responsible for implementation have read and understand the requirements of relevant specifications before work is started.
- b. Confirm with appropriate persons clearly the responsibilities that individuals have for meeting the counter measure requirements.
- c. Agree with appropriate persons arrangements for inspecting and controlling the quality of work and recording the outcomes.
- d. Identify work which fails to meet the recommended variations and agree on corrective action.
- e. Identify potential improvements and recommend to the client, highlighting benefits of the improvements.

- f. Negotiate and agree on amendments to manage variation with the clients and accurately record relevant details.
- g. Maintain the security and confidentiality of information relevant to the clients and their security aims and objectives.

5.4.2 Performance Criteria: Manage TSCM against agreed operational requirements

You must be able to –

- a. Agree to arrangements with appropriate persons to monitor and record the progress of the TSCM.
- b. Identify and determine the implications of any deviations from planned progress which have occurred.
- c. Agree with the appropriate persons and implement any action necessary to prevent disruption.
- d. Inform the clients at agreed intervals about the progress, changes to the operational programme or resource needs and suggest any actions that could improve the implementation of security measures.
- e. Complete required documentation accurately and within agreed time limits.
- f. Maintain the security and confidentiality of information relevant to the clients and their security aims and objectives.

5.4.3 Performance Criteria: Assess the effectiveness of implementing TSCM

You must be able to –

- a. Set up and apply processes for monitoring the effectiveness of TSCM.
- b. Identify potential improvements to TSCM and recommend them to your clients, emphasizing the benefits of the improvements.
- c. Maintain the security of assets whilst implementing new arrangements.
- d. Maintain the security and confidentiality of information relevant to your clients and their security aims and objectives.

5.5 Carry out Technically Assisted & Physical Inspections of Premises

This unit consists of four elements:

- a. Prepare to carry out inspections.
- b. Carry out inspections.
- c. Complete inspections.
- d. Respond to devices found.

5.5.1 Performance Criteria: Prepare to carry out inspections

You must be able to –

- a. Confirm you have sufficient details and the necessary authority to carry out inspections.
- b. Confirm inspection activities with your clients, based on identified threats and vulnerabilities.
- c. Confirm that all necessary inspection equipment is available, functioning correctly and calibrated where necessary.
- d. Brief all relevant personnel and confirm their understanding of the purpose and process of inspection, prior to starting inspection activities.
- e. Take effective measures to avoid alerting potential attackers.
- f. Take effective measures to maintain the security and confidentiality of TSCM inspections and procedures.
- g. Provide advice and recommendations to clients to maintain the integrity of the environment following completion of inspection.

5.5.2 Performance Criteria: Carry out inspections

You must be able to –

- a. Use equipment in line with best practices to achieve its TSCM purpose.
- b. Use the correct tools and equipment safely and effectively and confirm the equipment you use is functioning correctly.
- c. Use a range of inspection procedures, tools, and methods to detect devices according to different threats and vulnerabilities, as well as search patterns that are logical and effective.
- d. Use detection methods appropriate to the nature of the immediate threat to your clients.
- e. Comply with relevant health and safety requirements.
- f. Obtain other specialist help and advice when required.
- g. Take appropriate and authorised action on discovering technical security vulnerabilities and other anomalies.
- h. Take effective measures to maintain the security and confidentiality of TSCM inspections and procedures.

5.5.3 Performance Criteria: Complete inspections

You must be able to –

- a. Report inspection results to your clients within agreed timeframes.
- b. Give your clients advice on further action to counter technical security vulnerabilities.
- a. Re-instate premises to pre-inspection state (blinds, furniture, access, etc.).

- c. Complete records of inspections in accordance with appropriate procedures.
- d. Carry out equipment check to confirm all present and correct.
- e. Preserve the integrity of evidence of suspicious or illicit surveillance devices.
- f. Take effective measures to maintain the security and confidentiality of TSCM inspections and procedures.
- g. Provide detailed records of all work carried out, results obtained, and recommendations made to clients.

5.5.4 Performance Criteria: Respond to devices found

You must be able to –

- a. Correctly identify devices found during inspections.
- b. Act in line with clients' instructions upon discovering devices.
- c. Record and report the relevant details relating to the devices to the appropriate persons.
- d. Complete required reports and documentation relevant to the devices, legibly, accurately and within required time limits.
- e. Maintain the health, safety and welfare of yourself and others, while responding to finding devices.

5.6 Provide Post TSCM Inspection Support

5.6.1 Performance Criteria: Provide ongoing support to clients

You must be able to –

- a. Provide clients with relevant and accurate information relating to the electronic counter risk within agreed timeframe.
- b. Provide recommendations to address residual risk.
- c. Communicate with your clients using appropriate methods of communication.
- d. Present information in a style and format that assist your clients to increase the awareness of risk associated with the loss of information and unauthorised surveillance.
- e. Assist in decisions about TSCM.
- f. Provide clients with information which has no impact/influence in line with codes of practice of the Company.
- g. Maintain the security and confidentiality of information relating to TSCM services.

5.7 Maintain Knowledge and Understanding of Current TSCM Investigation Development

This unit consists of three elements:

- a. Research and evaluate technical developments relevant to TSCM.
- b. Apply new knowledge to TSCM development.
- c. Contribute to TSCM technical knowledge within your organisation.

5.7.1 Performance Criteria: Research and evaluate technical developments relevant to TSCM

You must be able to –

- a. Identify emerging areas of technical developments relevant to your work.
- b. Identify and access appropriate sources of relevant information.
- c. Use research methods that are efficient and effective in obtaining relevant information.
- d. Evaluate the usefulness and relevance of technical developments to your work.
- e. Maintain the confidentiality of information appropriate to the source and sensitivity.

5.7.2 Performance Criteria: Apply new knowledge to TSCM

You must be able to -

- a. Confirm you have the authority to apply new knowledge.
- b. Determine the potential effects of applying new knowledge.
- c. Apply new knowledge to update TSCM procedures and techniques to confirm its efficacy.
- d. Confirm the application of new knowledge meets its intended purpose.
- e. Rectify any undesirable effects of the application of new knowledge.
- f. Obtain other specialist help and advice when required.
- g. Record accurate and full details of the results of applying new knowledge.

5.7.3 Performance Criteria: Contribute to TSCM technical knowledge within your organisation

You must be able to –

- a. Confirm you have the authority to share new knowledge with others.
- b. Propose potential improvements in practices that contribute to the effectiveness of TSCM operations.
- c. Make sure your contributions comply with relevant legislation, regulation, and codes of practice.
- d. Provide full and accurate details to support new developments, in formats and styles that aid understanding.
- e. Maintain the confidentiality of details of TSCM practices.

5.8 Develop TSCM Techniques and Practices

This unit consists of two elements:

- a. Evaluate trends, technology, clients' needs and relevant legislation.
- b. Propose new techniques and practices to maintain the security of information.

5.8.1 Performance Criteria: Evaluate trends, technology, client needs and relevant legislation

You must be able to –

- a. Identify vulnerabilities in the security of information that could be susceptible to attacks.
- b. Determine the potential impact of clients' policies or procedures on security of information.
- c. Identify the sources or causes of threats to technical security.
- d. Recognise trends in attacks on technical security that have the potential to be a threat to security of information.
- e. Determine the possibility of treating vulnerabilities within current practices and legislation.
- f. Recognise when another specialist assistance is required.

5.8.2 Performance Criteria: Propose new techniques and practices to maintain the security of information

You must be able to –

- a. Propose new techniques and practices that have the potential to improve security of information.
- b. Ensure that your proposals conform to current legislation, regulation, guidelines, and codes of practice relating to security of information.
- c. Inform relevant people of proposals as required.
- d. Provide details of your proposals in a language and format that aids understanding.
- e. Explain new techniques and practices to people who need to understand them.
- f. Maintain the confidentiality of details of TSCM techniques and practices.

5.9 Maintain Knowledge and Understanding of Legislation, Regulation and Codes of Practice relevant to TSCM

This unit consists of two elements:

- a. Apply new knowledge to TSCM practices.
- b. Contribute to the increase of knowledge of legislation, regulation, and codes of practice among colleagues.

5.9.1 Performance Criteria: Apply new knowledge to TSCM practices

You must be able to –

- a. Confirm you have the authority to apply new knowledge.
- b. Determine accurately the potential effects of applying new knowledge.
- c. Apply new knowledge to update TSCM practices to confirm its efficiency.
- d. Confirm the application of new knowledge meets its intended purpose.
- e. Report any undesirable effects of the application of new knowledge to the appropriate authority.
- f. Identify other specialist help and advice when required.
- g. Record accurate and full details of the results of applying new knowledge.

5.9.2 Performance Criteria: Contribute to the increase of knowledge of legislation, regulation, and codes of practice among colleagues

You must be able to –

- a. Confirm you have the authority to share new knowledge with others.
- b. Identify and explain fully the potential impact of legislation, regulation, and codes of practice on TSCM Investigation practices.
- c. Propose potential improvements in practices that contribute to increased effectiveness of TSCM operations.
- d. Make sure your contributions comply with relevant legislation, regulation, and codes of practice.
- e. Provide full and accurate details to support proposed improvements, in formats and styles that aid understanding.

5.10 Present Information to Courts or other Hearings (South African Laws)

This unit has been imported from Skills for Justice Suite of Standards.

5.10.1 Performance Criteria: Present information to courts or other hearings

You must be able to –

- a. Consider the information in advance of the hearing and ensure that you are in possession of the appropriate notes and materials.
- b. Present yourself at the venue in a timely manner and in possession of all necessary notes and Materials.
- c. Ensure your appearance and behaviour always conforms to acceptable professional standards.

- d. Provide information and respond to questions in an appropriate manner with due regard for the rules and the procedures of the venue.
- e. Provide oral evidence that is consistent with any written materials provided by you as part of the case.
- f. Respond to all directions of the court or hearing promptly and appropriately.
- g. Report any breaches of court procedure or protocol that come to your attention promptly to the relevant authority.

5.10.2 Specific Knowledge

5.10.2.1 Legal and organisational requirements

- a. Current, relevant legislation, policies, procedures, and codes of practice for presenting evidence to court and other hearings.
- b. Current, relevant legislation and organisational requirements in relation to race, diversity, and human rights.
- c. Procedures and protocols in courts and at hearings.
- d. The legislation relevant to the case in question.

5.10.2.2 Preparing for court or other hearings

- a. How to prepare and make available notes and materials in a manner that maintain their continuity and integrity.
- b. The importance of considering your evidence in advance.
- c. How and where to locate and obtain evidence, notes, and materials for presentation.
- d. How to liaise with prosecuting authorities.

5.10.2.3 Presenting evidence at court or other hearings

- a. How to give evidence effectively in a court or hearing.
- b. How and when you can refer to any notes and materials in your possession.
- c. Techniques for maintaining control and composure under cross examination.
- d. The permitted liaison with victims, witnesses, and defendants.
- e. The support services (e.g., victim support, duty solicitor) available at court/hearing and their role and Responsibilities.
- f. The roles and responsibilities of court personnel.
- g. What constitutes a breach of court protocol or procedure and to whom any breaches should be reported.

Version number V02
Version date 31 Mar 2023

The latest terminology for Sweep/Debugging is TSCM - Technical Surveillance Counter Measures.

Document Compiled by and date: Riaan Bellingan 1 August 2017

Document Reviewed by and date: Riaan Bellingan 10 October 2020 and 10 April 2022

Document Approved by and date: ACFE SA Forensic Standards Forum 31 March 2023