Association of Certified Fraud Examiners

Introduction: The Forensic Industry Standard Forum

The aim of the Forensic Industry Standard Forum under the auspices of the ACFE SA is to standardise and regulate 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 and although there are well known and international standards in most of the disciplines, some changes may be required in order to address the situation in South Africa and Africa in the context of our own environments and applicable legislation and/or legal systems and frameworks.

Scientists and forensic investigators need to be guided with acceptable standards and procedures for carrying out such examinations. Although the ACFE refers to "certified fraud examiners" it recognises the fact that a strong association exists with forensic examiners and practitioners. All forensic disciplines will accordingly be included in the Forensic Industry Standard Forum.

The ACFE SA Chapter: Background:

The need to raise the standard of fraud examination in South Africa and for a professional body which was 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 a number of 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 collection of individuals in South Africa from all industries and professionals, who all have a single goal in mind; the reduction of white-collar crime in South Africa.

Preamble of the ACFE SA

The Association of Certified Fraud Examiners 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 in a professional manner.

Members have a professional responsibility to their clients, to 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 Certified Fraud Examiners shall be expected, and all Associate members shall strive to demonstrate their commitment to excellence in service and professional conduct.

II. Applicability of Code

The CFE Code of Professional Standards shall apply to all members and all Associate members of the Association of Certified Fraud Examiners. The use of the word "member" or "members" in this Code shall refer to Associate members as well as regular members of the Association of Certified Fraud Examiners.

III. Standards of Professional Conduct

A. Integrity and Objectivity

1. Members shall conduct themselves with integrity, knowing that public trust is founded on integrity. Members shall not sacrifice integrity to serve the client, their employer or the public interest.

2 Prior to accepting the fraud examination, members shall investigate for potential conflicts of interest. Members shall disclose any potential conflicts of interest to prospective clients who retain them or their employer.

3. Members shall maintain objectivity in discharging their professional responsibilities within the scope of the engagement.

4. Members shall not commit discreditable acts, and shall always conduct themselves in the best interests of the reputation of the profession.

5. Members shall not knowingly make a false statement when testifying in a court of law or other dispute resolution forum. Members shall comply with lawful orders of the courts or other dispute

resolution bodies. Members shall not commit criminal acts or knowingly induce others to do so.

B. Professional Competence

1. Members shall be competent and shall 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.

2. Members shall maintain the minimum program of continuing professional education required by the Association of Certified Fraud Examiners. A commitment to professionalism combining education and experience shall continue throughout the member's professional career. Members shall continually strive to increase the competence and effectiveness of their professional services.

C. Due Professional Care

1. Members shall exercise due professional care in the performance of their services. Due professional care requires diligence, critical analysis and professional scepticism in discharging professional responsibilities.

2. Conclusions shall be supported with evidence that is relevant, competent and sufficient.

3. Members' professional services shall be adequately planned. Planning controls the performance of a fraud examination from inception through completion and involves developing strategies and objectives for performing the services.

4. Work performed by assistants on a fraud examination shall be adequately supervised. The extent of supervision required varies depending on the complexities of the work and the qualifications of the assistants.

D. Understanding with Client or Employer

1. At the beginning of a fraud examination, members shall 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.

2. Whenever the scope or limitations of a fraud examination or the responsibilities of the parties change significantly, a new understanding shall be reached with the client or employer.

E. Communication with Client or Employer

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

F. Confidentiality

1. Members shall not disclose confidential or privileged information obtained during the course of 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 organization agrees to abide by the confidentiality restrictions.

IV. Standards of Examination

A. Fraud Examinations

1. Fraud examinations shall be conducted in a legal, professional and thorough manner. The fraud examiner's objective shall be to obtain evidence and information that is complete, reliable and relevant.

2. Members shall establish predication and scope priorities at the outset of a fraud examination and continuously re-evaluate them as the examination proceeds. Members shall strive for efficiency in their examination.

3. Members shall be alert to the possibility of conjecture, unsubstantiated opinion and bias of witnesses and others. Members shall consider both exculpatory and inculpatory evidence.

B. Evidence

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

2. 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.

V. Standards of Reporting

A. General

1. 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

1. Members' reports shall contain only information based on data that are sufficient and relevant to support the facts, conclusions, opinions and/or recommendations related to the fraud examination. The report shall be confined to subject matter, principles and methodologies within the member's area of knowledge, skill, experience, training or education.

2. No opinion shall be expressed regarding the legal guilt or innocence of any person or party.

Forensic Industry Standard Forum:

Discipline/title	Information Security Management (ISM)
Describe discipline	Information Security Management (ISM) is an Information Security technology science process by which the total risks (Internal and External), vulnerabilities, software, mobile applications, business, operational and technical deliverables of an organization is identified, analyses and prioritized by experts who are highly skilled with technique or practice
Science Application	Republic of South Africa
Purpose of the discipline	Information Security Management (ISM), involves the assessment and pen testing of an organizations active system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities.

A. Criminalistics:

Science organizations 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:

1. Constitution of the Republic of South Africa Act 86/1996
2. Human Rights Commission Act 56/1994
3. Consumer Protection Act 68 of 2008
4. South African Law of Contract A – 2012
5. Electronic Communications and Transactions Act 25 of 2002
6. Common Law – South Africa

7. Proceeds of Crime Act 2002
8. Prevention and Combating of Corrupt Activities Act 12 of 2004
9. Criminal Procedure Act, Act 51 of 1977
10. Financial Intelligence Centre Act 38 of 2001
11. Investigation of Serious Economic Offences Amendment Act 46 of 1995
12. Prevention of Organised Crime Act 121 of 1998
13. Prevention of Organised Crime Amendment Act 24 of 1999
14. Prevention of Organised Crime Second Amendment Act 38 of 1999
15. Promotion of Access to Information Act 2 of 2000
16. Promotion of Access to Information Amendment Act 54 of 2002
17. Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002
18. The Protection of Personal Information Act (POPI)
19. Occupational Health and safety Act 85 of 1993 as amended
20. Taxation Laws Amendment Act 2012
21. Customs and Excise Act 91 of 1964
22. King-III and IV , for ethical leadership and good corporate governance

Science organizations 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.

B. **Ethics in Administration**:

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

A science organization that deliver the above discipline services, expressly agrees to the following ethics prescribed by the ACFE:

1. To behave honestly and with integrity
2. To diligently execute the job description
3. To execute any function or instruction only by way of lawful interactions and/or conduct
4. To promote and uphold the good corporate reputation of all stake holders
5. To treat both internal and external clients with professionalism and respect
6. To never take improper advantage of inexperience, lack of education, youth, lack of sophistication, language barrier or ill health of any client
7. To disclose and take reasonable steps to avoid any conflict of interest
8. To not provide false or misleading information in response to a request for information from any of the key stakeholders

9. To promote public confidence in the organization and all its stake holders through fair and conscientious dealings refraining from any deceit, misrepresentation, willful non-disclosure, undue influence or other harmful practice
10. To never seek personal gain or make any secret profit, acquire any financial interest or benefit in any matter entrusted to you.
11. To submit a detailed report after the services delivery.
12. Discuss findings in a professional way with clients
13. To always comply below, with the existing prescribed National and International ethics standards for the above science discipline:
14. Liaising with role players in law enforcement and intelligence agencies, where necessary
15. Assisting with preparing cases for clients, where necessary
16. Providing evidence at disciplinary hearings and in criminal / civil courts, where necessary

C. Compliance with the code:

Science organizations, that deliver the above discipline services, 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 science organizations should adhere to the principles expressed in this Code, but also encourage and support adherence to the code by science organizations, that deliver some of these discipline services.

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

D. Non-compliance with the code:

Adherence to this code is compulsory and any transgression will be viewed as gross misconduct resulting in his/her ACFE SA chapter membership being terminated.

All science organizations that deliver the above discipline services, expressly agree to the following:

1. To maintain a sound knowledge of the code of conduct, policies and objectives of the ACFE SA chapter.

2. 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.

3. There should be clear principles of good practice outlining how science organizations should conduct the above science services.

4. Drawing on the widest range of good practice, this code will further regulate science organizations methodologies of addressing, the above science services to help ensure that the highest standards are applied and maintained.

E. Application:

1. This Code applies to all science organizations engaged or acting on behalf of consulting companies carrying out duties involving the comprehensive Information Security services.

F. Breach of the Code of Conduct:

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

G. Provisions General Conduct:

Science organizations to whom the Code applies must not:

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

H. Legislation and other Guidance:

1. Always Comply with existing legislation.
2. Always comply, with the existing prescribed National and International ethics standards for the above discipline.
3. 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 inseperable. 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.
4. Make use of existing methods against loss of any data.
5. Ensure that all information which may be relevant is analyses.
6. Observe all other applicable legislation and internal and external guidance.

7. Obtain written permission before the service is conducted.

I. Information:

Science organizations to whom the Code applies must not under any circumstances:

1. Conceal or fabricate information or knowingly allow any information to be fabricated or concealed.
2. Accept from or offer any inducement, bribe or other advantage to anyone.
3. Use any information gathered in the course of their services for personal gain or coercion or otherwise misuse such information

J. Disclosure of Interests:

1. Science organizations must declare any circumstances or interests which may affect their ability to conduct an Information Security Management (ISM) service independently or objectively.

K. Safeguarding Information:

Science organizations must treat all information gathered or received during the course of an Information Security Management (ISM) service as confidential and must not deliberately or negligently:

1. Disclose and discussed such information to an unauthorized third party
2. Reveal the source of information to an unauthorized third party
3. Unless the disclosure is prescribed by law.

L. Personal Injury and Damage to Property:

Science organizations must exercise all reasonable care to prevent injury or loss or damage to public or private property and must not enter public or private property except on the invitation of the occupier or responsible person or police officer.

1. Deliberately or negligently destroy or damage any property or information.
2. Deliberately or negligently destroy or damage any network, business, operational or technical deliverables.
3. Use or threaten physical violence towards a colleague or member of the public.
4. Science organizations must conduct themselves with integrity.
5. Science organizations must be fair, honest and impartial in dealings, and treat others with dignity and respect.

6. Science organizations must be aware of obligations to maintain confidentiality of information. They must not use this information for personal gain, nor to the detriment of its stakeholders.
7. Science organizations must exercise due skill, care and diligence in performing services and acknowledge their responsibility to maintain currency of our knowledge, skills and technical competencies.

M. Application of the Code of Conduct:

1. It is important to recognize that in applying this Code of Good Practice, the personal characteristics of honesty, sincerity, impartiality and trustworthiness are key guiding attributes.
2. The effectiveness of the policies relies on responsibility for their own behaviour and being committed to the standards.

N. **Integrity:**

1. Science organizations should act with honesty, sincerity and integrity in their approach to their services.

O. **Conflicts of interest:**

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

P. **Confidentiality:**

1. Science organizations must protect the confidentiality of information acquired in the course of their service.

Q. Fair and honest dealing:

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

R. **Ethical behavior:**

1. Science organizations should conduct themselves in a manner which is consistent with the ACFE intentions, reputation, and functions for which it was created. Science organizations should refrain from any conduct which might bring discredit to the ACFE.
2. They should not allow dishonesty, personal prejudice or bias to influence their conduct of their employment.

3. 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.
4. Their actions should be fair, honest, and truthful.
5. They should avoid actual or perceived conflicts of interest.
6. They should not condone the use of any information which is misleading, false or deceptive.
7. 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.
8. They should not use confidential or other information for personal advantage or for the advantage of another.

i) KNOWLEDGE AND SKILLS – INFORMATION SECURITY MANAGEMENT (ISM)	
FORMAL EDUCATION	➢ Grade 12
EDUCATION AND TECHNICAL TRAINING IN INFORMATION SECURITY MANAGEMENT (ISM)	1. Certified training and education at accredited recognised institute 2. Any computer science qualification 3. Academic and trained background based on one or more of the following: a) Any Computer science qualifications b) Any ICT qualifications c) Certified Ethical Hacker (CEH) d) Computer Hacking Forensic Investigator (CHFI) e) Secure computer user (SCU) f) Certified Incident Handler (CIH) g) Certified Security Specialist (CSS) h) Certified Security Analyst (CSA) i) Project Management IT Security (PMIS) 4. Recommend – Certified Fraud Examiner 5. Membership of the ACFE
EXPERIENCE AND KNOWLEDGE	1. 5 Years 2. Experience and or knowledge in the following environment: a) Information Security Management (ISM) b) Data analyses c) Pen testing d) Software application evaluation e) Network inspection f) Target Scanning / Vulnerability Assessment g) Communication Analysis h) Information Gathering / Discovery i) External Assessment j) Methodology Framework k) Network Risk - Vulnerability and Application Evaluation l) Policies and Governance m) Software development n) Mobile App assessment o) Computer Forensic Investigations p) Network Forensic Investigations q) Network security r) Business Impact Analysis s) Network Assessments t) National and International Ethics Standards / Guidelines & Methodology

S. Minimum experience and knowledge:

II) MINIMUM EXPERIENCE AND KNOWLEDGE –INFORMATION SECURITY MANAGEMENT (ISM)	
MINIMUM EXPERIENCE AND KNOWLEDGE	➢ 5 years

T. Information Security Management (ISM) Processes:

1. Apply Internationally accepted methodologies in line with best practice methodologies.
2. Alignment of best practice methodologies with best practice standards as guideline.
3. Make use of International partner's skills, experience and knowledge.

U. Information Security Management (ISM) Science Glossary:

A
Active Attack **An attack which results in an unauthorized state change, such as the manipulation of files, or the adding of unauthorized files.** **Ad Blocker** **A program that helps to prevent unsolicited windows from appearing on your screen; these windows usually contain advertisements.** **Ad Killer** **A program that helps to prevent unsolicited windows from appearing on your screen; these windows usually contain advertisements.** **Administrative Security** **The management constraints and supplemental controls established to provide an acceptable level of protection for data.** **Adware** **While not necessarily malware, adware is considered to go beyond the reasonable advertising that one might expect from freeware or shareware. Typically a separate program that is installed at the same time as a shareware or similar program, adware will usually continue to generate advertising even when the user is not running the originally desired program. See also cookies, spyware, and web bugs** **AIS** **Automated Information System - any equipment of an interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware.** **Alert** **A formatted message describing a circumstance relevant to network security. Alerts are often derived from critical audit events.**

Ankle-Biter

A person who aspires to be a hacker/cracker but has very limited knowledge or skills related to AIS's. Usually associated with young teens who collect and use simple malicious programs obtained from the Internet.

AntiSpam

A Software or service to help prevent unsolicited mail and to complicate a spammer's method of collecting email addresses.

Application Level Gateway

(Firewall) A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.

Assessment

Surveys and Inspections; an analysis of the vulnerabilities of an AIS. Information acquisition and review process designed to assist a customer to determine how best to use resources to protect information in systems.

Assurance

A measure of confidence that the security features and architecture of AIS accurately mediate and enforce the security policy.

Attack

An attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Audit

The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures and to recommend any indicated changes in controls, policy, or procedures.

Audit Trail

In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

Authenticate

To establish the validity of a claimed user or object.

Authentication

To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Automated Security Monitoring

All security features needed to provide an acceptable level of protection for hardware, software, and classified, sensitive, unclassified or critical data, material, or processes in the system.

Availability

Assuring information and communications services will be ready for use when expected.

B

Back Door

A hole in the security of a computer system deliberately left in place by designers or maintainers. Synonymous with trap door; a hidden software or hardware mechanism used to circumvent security controls.

Breach

The successful defeat of security controls which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.

Buffer Overflow

This happens when more data is put into a buffer or holding area, then the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes. This can result in system crashes or the creation of a back door leading to system access.

Bug

An unwanted and unintended property of a program or piece of hardware, especially one that causes it to malfunction.

C

CGI

Common Gateway Interface - CGI is the method that Web servers use to allow interaction between servers and programs.

CGI Scripts

Allows for the creation of dynamic and interactive web pages. They also tend to be the most vulnerable part of a web server (besides the underlying host security).

Circuit Level Gateway

One form of a firewall. Validates TCP and UDP sessions before opening a connection. Creates a handshake, and once that takes place passes everything through until the session is ended.

Click-reload

A popup that opens when you click on a link which at the same times reloads the page you are viewing.

COAST

Computer Operations, Audit, and Security Technology - is a multiple project, multiple investigator laboratory in computer security research in the Computer Sciences Department at Purdue University. It functions with close ties to researchers and engineers in major companies and government agencies. Its research is focused on real-world needs and limitations, with a special focus on security for legacy computing systems.

Computer Abuse

The wilful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation.

Computer Fraud

Computer-related crimes involving deliberate misrepresentation or alteration of data in order to obtain something of value.

Computer Network Attack

(CAN) Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or

the computers and networks themselves. (DODD S-3600.1 of 9 Dec 96)

Computer Security

Technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system.

Computer Security Incident

Any intrusion or attempted intrusion into an automated information system (AIS). Incidents can include probes of multiple computer systems.

Computer Security Intrusion

Any event of unauthorized access or penetration to an automated information system (AIS).

Computer Worm

A self-reproducing program which is distinguished from a virus by copying itself without being attached to a program file, or which spreads over computer networks, particularly via email.

Confidentiality

Assuring information will be kept secret, with access limited to appropriate persons.

Countermeasures

Action, device, procedure, technique, or other measure that reduces the vulnerability of an automated information system. Countermeasures that are aimed at specific threats and vulnerabilities involve more sophisticated techniques as well as activities traditionally perceived as security.

Crack

A popular hacking tool used to decode encrypted passwords. System administrators also use Crack to assess weak passwords by novice users in order to enhance the security of the AIS.

Cracker

One who breaks security on an AIS.

Cracking

The act of breaking into a computer system.

Crash

A sudden, usually drastic failure of a computer system.

Cryptography

The art of science concerning the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form.

Cyberspace

Describes the world of connected computers and the society that gathers around them. Commonly known as the INTERNET.

D

Dark-side Hacker

A criminal or malicious hacker.

DARPA

Defence Advanced Research Projects Agency.

Data Driven Attack

A form of attack that is encoded in innocuous seeming data which is executed by a user or a process to implement an attack. A data driven attack is a concern for firewalls, since it may get through the firewall in data form and launch an attack against a system behind the firewall.

Data Encryption Standard

Definition 1) (DES) An unclassified crypto algorithm adopted by the National Bureau of Standards for public use. Definition 2) A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology (NIST), is intended for public and government use.

Demon Dialler

A program which repeatedly calls the same telephone number. This is benign and legitimate for access to a BBS or malicious when used as a denial of service attack.

Denial of Service

Action(s) which prevent any part of an AIS from functioning in accordance with its intended purpose.

Derf

The act of exploiting a terminal which someone else has absent-mindedly left logged on.

DES

See Data Encryption Standard

DMZ

Demilitarized Zone - A part of the network that is neither part of the internal network nor directly part of the Internet. Basically a network sitting between two networks.

DNS Spoofing

Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

E

Email Worm

A self-reproducing program which is distinguished from a virus by copying itself without being attached to a program file, or which spreads over computer networks, particularly via email.

Encapsulating Security Payload

(ESP) A mechanism to provide confidentiality and integrity protection to IP datagram's.

Ethernet Sniffing

This is listening with software to the Ethernet interface for packets that interest the user. When the software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like login or password.

F

False Negative

Occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behaviour.

False Positive

Occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action.

Fault Tolerance

The ability of a system or component to continue normal operation despite the presence of hardware or software faults.

Firewall

A system or combination of systems that enforces a boundary between two or more networks. Gateway that limits access between networks in accordance with local security policy. The typical firewall is an inexpensive micro-based Unix box kept clean of critical data, with many modems and public network ports on it, but just one carefully watched connection back to the rest of the cluster.

Firewall Test

A series of probes to detect hardware or software vulnerabilities in equipment used to protect a computer or network.

Fishbowl

To contain, isolate and monitor an unauthorized user within a system in order to gain information about the user.

H

Hacker

A person who enjoys exploring the details of computers and how to stretch their capabilities. A malicious or inquisitive meddler who tries to discover information by poking around. A person who enjoys learning the details of programming systems and how to stretch their capabilities, as opposed to most users who prefer to learn on the minimum necessary.

Hacking

Unauthorized use or attempts to circumvent or bypass the security mechanisms of an information system or network.

Hacking Run

A hack session extended long outside normal working times, especially one longer than 12 hours.

Host

A single computer or workstation; it can be connected to a network.

Host Based

Information, such as audit data from a single host which may be used to detect intrusions.

I

IDEA

(International Data Encryption Algorithm) - A private key encryption-decryption algorithm that uses a key that is twice the length of a DES key.

IDIOT

Intrusion Detection In Our Time. A system that detects intrusions using pattern-matching.

Integrity

Assuring information will not be accidentally or maliciously altered or destroyed.

Internet Worm

A worm program (see: Worm) that was unleashed on the Internet in 1988. It was written by Robert T. Morris as an experiment that got out of hand.

Intrusion

Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusion Detection

Pertaining to techniques which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

IP Splicing / Hijacking

An action whereby an active, established, session is intercepted and co-opted by the unauthorized user. IP splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP splicing rely on encryption at the session or network layer.

IP Spoofing

An attack whereby a system attempts to illicitly impersonate another system by using IP network address.

K

Key

A symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text in order to encrypt or decrypt.

Key Escrow

The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees.

Keystroke Monitoring

A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the AIS returns to the user.

L

LAN

Local Area Network - A computer communications system limited to no more than a few miles and using high-speed connections (2 to 100 megabits per second). A short-haul communications system that connects ADP devices in a building or group of buildings within a few square kilometres, including workstations, front-end processors, controllers, switches, and gateways.

Launch-close

Popups that open when you click on a link which at the same time closes the page being viewed. Since the popup opens at the same time the main window is closed, your popup blocker may incorrectly interpret it as a "unload"

popup window.

Leapfrog Attack

Use of userid and password information obtained illicitly from one host to compromise another host. The act of TELNETing through one or more hosts in order to preclude a trace (a standard cracker procedure).

Letterbomb

A piece of e-mail containing live data intended to do malicious things to the recipient's machine or terminal. Under UNIX, a letterbomb can also try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly to denial of service.

M

Mailbomb

The mail sent to urge others to send massive amounts of e-mail to a single system or person, with the intent to crash the recipient's system. Mailbombing is widely regarded as a serious offense.

Malicious Code

Hardware, software, of firmware that is intentionally included in a system for an unauthorized purpose; e.g. a Trojan horse.

Malware

A generic term increasingly being used to describe any form of malicious software; eg, viruses, trojan horses, malicious active content, etc.

MaurerHour

A security algorithm that executes a large sum of code in less than 60 minutes

Metric

A random variable x representing a quantitative measure accumulated over a period.

Mockingbird

A computer program or process which mimics the legitimate behaviour of a normal system feature (or other apparently useful function) but performs malicious activities once invoked by the user.

Multihost Based Auditing

Audit data from multiple hosts may be used to detect intrusions.

N

Nak Attack

Negative Acknowledgment - A penetration technique which capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly and thus; leaves the system in an unprotected state during such interrupts.

Net Send Spam

Windows messenger vulnerability also known as net send spam, messenger spam or winpopup. These types of ads usually take the form of a gray pop up box bearing spam (unsolicited advertisements) with an "OK" button.

Network

Two or more machines interconnected for communications.

Network Based

Network traffic data along with audit data from the hosts used to detect intrusions.

Network Level Firewall

A firewall in which traffic is examined at the network protocol (IP) packet level.

Network Security

Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects. Network security includes providing for data integrity.

Network Security Officer

Individual formally appointed by a designated approving authority to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an automated information system network.

Non-Repudiation

Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

O

On-unload

Loads a popup as you leave the webpage.

Open Security

Environment that does not provide environment sufficient assurance that applications and equipment are protected against the introduction of malicious logic prior to or during the operation of a system.

Open Systems Security

Provision of tools for the secure internetworking of open systems.

Operational Data Security

The protection of data from either accidental or unauthorized, intentional modification, destruction, or disclosure during input, processing, or output operations.

Operations Security

Definition 1) The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities. Definition 2) An analytical process by with the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.

Orange Book

See Trusted Computer Security Evaluation Criteria.

OSI

Open Systems Interconnection. A set of internationally accepted and openly developed standards that meet the needs of network resource administration and integrated network utility.

P

Packet

A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.

Packet Filter

Inspects each packet for user defined content, such as an IP address but does not track the state of sessions. This is one of the least secure types of firewall.

Packet Filtering

A feature incorporated into routers and bridges to limit the flow of information based on predetermined communications such as source, destination, or type of service being provided by the network. Packet filters let the administrator limit protocol specific traffic to one network segment, isolate e-mail domains, and perform many other traffic control functions.

Packet Sniffer

A device or program that monitors the data traveling between computers on a network.

Passive Attack

Attack which does not result in an unauthorized state change, such as an attack that only monitors and/or records data.

Passive Threat

The threat of unauthorized disclosure of information without changing the state of the system. A type of threat that involves the interception, not the alteration, of information.

PEM (Privacy Enhanced Mail)

An IETF standard for secure electronic mail exchange.

Penetration

The successful unauthorized access to an automated system.

Penetration Signature

The description of a situation or set of conditions in which a penetration could occur or of system events which in conjunction can indicate the occurrence of a penetration in progress.

Penetration Testing

The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation that may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users

Perimeter Based Security

The technique of securing a network by controlling access to all entry and exit points of the network. Usually associated with firewalls and/or filters.

Perpetrator

The entity from the external environment that is taken to be the cause of a risk. An entity in the external environment that performs an attack, i.e. hacker.

Personnel Security

The procedures established to ensure that all personnel who have access to any classified information have the required authorizations as well as the appropriate clearances.

PGP (Pretty Good Privacy)

A freeware program primarily for secure electronic mail.

Phage

A program that modifies other programs or databases in unauthorized ways; especially one that propagates a virus or Trojan horse.

PHF

Phone book file demonstration program that hackers use to gain access to a computer system and potentially read and capture password files.

PHF hack

A well-known and vulnerable CGI script which does not filter out special characters (such as a new line) input by a user.

Phracker

An individual who combines phone phreaking with computer hacking.

Phreak(er)

An individual fascinated by the telephone system. Commonly, an individual who uses his knowledge of the telephone system to make calls at the expense of another.

Phreaking

The art and science of cracking the phone network.

Physical Security

The measures used to provide physical protection of resources against deliberate and accidental threats.

Piggy Back

The gaining of unauthorized access to a system via another user's legitimate connection.

Ping of Death

The use of Ping with a packet size higher than 65,507. This will cause a denial of service.

Plaintext

Unencrypted data.

Popup blocker

A program that helps to prevent unsolicited windows from appearing on your screen; these windows usually contain advertisements.

Popup check

A site that allows you to check your ad blocking software's ability to prevent unwanted advertisements. A complete test such as `popupcheck' is necessary to make such a determination.

Popup stopper

A program that helps to prevent unsolicited windows from appearing on your screen; these windows usually contain advertisements.

Popup test

A site that allows you to check your ad blocking software's ability to prevent unwanted advertisements. A complete test such as `popupcheck' is necessary to make such a determination.

Popup

A new browser window that appears unrequested (by you) on your screen. A gratuitous, easily-programmed visual effect exploited by many web sites often to the consternation of the hapless user. Commonly used for advertisements. Particularly annoying are those termed exit popups: browser windows that spring to life when you leave a site or when you close a browser window. (Scripting languages call these "onUnload" and "onClose" events.) We have never encountered one of these that were useful.

Port Scan

A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning, a favourite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.

Private Key Cryptography

An encryption methodology in which the encrypt or and decrypt or use the same key, which must be kept secret. This methodology is usually only used by a small group.

Probe

Any effort to gather information about a machine or its users for the apparent purpose of gaining unauthorized access to the system at a later date.

Procedural Security

See Administrative Security.

Profile

Patterns of a user's activity which can detect changes in normal routines.

Promiscuous Mode

Normally an Ethernet interface reads all address information and accepts follow-on packets only destined for itself, but when the interface is in promiscuous mode, it reads all information (sniffer), regardless of its destination.

Protocol

Agreed-upon methods of communications used by computers. A specification that describes the rules and procedures that product should follow to perform activities on a network, such as transmitting data. If they use the same protocols, products from different vendors should be able to communicate on the same network.

Proxy

A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

Public Key Cryptography

Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text.

R

Red Book

See Trusted Network Interpretation.

Replicator

Any program that acts to produce copies of itself examples include; a program, a worm, a fork bomb or virus. It is even claimed by some that UNIX and C are the symbiotic halves of an extremely successful replicator.

Retro-Virus

A retro-virus is a virus that waits until all possible backup media are infected too, so that it is not possible to restore the system to an uninfected state.

Risk Assessment

A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

Risk Management

The total process to identify, controls, and minimize the impact of uncertain events. The objective of the risk management program is to reduce risk and obtain and maintain DAA (Designated Approving Authority) approval.

Rootkit

A hacker security tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan Horse software. Rootkit is available for a wide range of operating systems.

Router

An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.

Routing Control

The application of rules during the process of routing so as to chose or avoid specific networks, links or relays.

RSA Algorithm

RSA stands for Rivest-Shamir-Aldeman. A public-key cryptographic algorithm that hinges on the assumption that the factoring of the product of two large primes is difficult.

Rules Based Detection

The intrusion detection system detects intrusions by looking for activity that corresponds to known intrusion techniques (signatures) or system vulnerabilities. Also known as Misuse Detection.

S

Samurai

A hacker who hires out for legal cracking jobs, snooping for factions in corporate political fights, lawyers pursuing privacy-rights and First Amendment cases, and other parties with legitimate reasons to need an electronic locksmith.

SATAN

Security Administrator Tool for Analyzing Networks - A tool for remotely probing and identifying the vulnerabilities of systems on IP networks. A powerful freeware program which helps to identify system security weaknesses.

Scanner

A program which examines computers and network systems examining configurations and looking for security vulnerabilities. This type of program can be used by both defenders and attackers.

Script Kiddies

See Ankle Biters

Secure Network Server

A device that acts as a gateway between a protected enclave and the outside world.

Secure Shell

A completely encrypted shell connection between two machines protected by a super long pass-phrase.

Security

A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

Security Architecture

A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements.

Security Audit

A search through a computer system for security problems and vulnerabilities.

Security Countermeasures

Countermeasures that are aimed at specific threats and vulnerabilities or involve more active techniques as well as activities traditionally perceived as security.

Security Domains

The sets of objects that a subject has the ability to access.

Security Features

The security-relevant functions, mechanisms, and characteristics of AIS hardware and software.

Security Incident

Any act or circumstance that involves classified information that deviates from the requirements of governing security publications. For example, compromise, possible compromise, inadvertent disclosure, and deviation.

Security Kernel

The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

Security Officer

The ADP official having the designated responsibility for the security of and ADP system.

Security Perimeter

The boundary where security controls are in effect to protect assets.

Security Policies

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Policy Model

A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information.

Security Requirements

Types and levels of protection necessary for equipment, data, information, applications, and facilities.

Security Scan

A search through a computer system for security problems and vulnerabilities.

Security Service

A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

Security Violation

An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources.

Server

A system that provides network service such as disk storage and file transfer, or a program that provides such a service. A kind of daemon which performs a service for the requester, which often runs on a computer other than the one which the server runs.

Simple Network Management Protocol (SNMP)

Software used to control network communications devices using TCP/IP.

Smurfing

A denial of service attack in which an attacker spoofs the source address of an echo-request ICMP (ping) packet to the broadcast address for a network, causing the machines in the network to respond en masse to the victim thereby clogging its network.

Snarf

To grab a large document or file for the purpose of using it with or without the author's permission.

Sneaker

An individual hired to break into places in order to test their security; analogous to tiger team.

Sniffer

A program to capture data across a computer network. Used by hackers to capture user id names and passwords.

Software tools that audits and identifies network traffic packets. Is also used legitimately by network operations and maintenance personnel to troubleshoot network problems.

Spam

To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.

Spam

Unsolicited "junk" e-mail sent to large numbers of people to promote products or services. Sexually explicit unsolicited e-mail is called "porn spam." Also refers to inappropriate promotional or commercial postings to discussion groups or bulletin boards.

Spoofing

Pretending to be someone else. The deliberate inducement of a user or a resource to take an incorrect action. Attempt to gain access to AIS by pretending to be an authorized user. Impersonating, masquerading, and mimicking are forms of spoofing.

Spyware

A general term for a program that surreptitiously monitors your actions. While they are sometimes sinister, like a remote control program used by a hacker, software companies have been known to employ spyware to gather data about customers. The practice is generally frowned upon.

SSL (Secure Sockets Layer)

A session layer protocol that provides authentication and confidentiality to applications.

Steganography

The activity of concealing a message by hiding the fact that that communication is happening. Steganography is often referred to as "hiding in plain sight."

Subversion

Occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur.

SYN Flood

When the SYN queue is flooded, no new connection can be opened.

T

TCP/IP

Transmission Control Protocol/Internetwork Protocol. The suite of protocols the Internet is based on.

tcpwrapper

A software tool for security which provides additional network logging, and restricts service access to authorized hosts by service.

Term Rule-Based Security Policy

A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

Terminal Hijacking

Allows an attacker, on a certain machine, to control any terminal session that is in progress. An attack hacker can

send and receive terminal I/O while a user is on the terminal.

Threat

The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.

Threat Agent

Methods and things used to exploit a vulnerability in an information system, operation, or facility; fire, natural disaster and so forth.

Threat Assessment

Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Tiger

A software tool which scans for system weaknesses.

Tiger Team

Government and industry - sponsored teams of computer experts who attempt to break down the defences of computer systems in an effort to uncover, and eventually patch, security holes.

Tinkerbell Program

A monitoring program used to scan incoming network connections and generate alerts when calls are received from particular sites, or when logins are attempted using certain ID's.

Toolbar

A row, column, or block of onscreen buttons or icons that, when clicked, activate certain functions of the program. For example, the standard toolbar in Word includes buttons for changing text to italic, bold, or other styles.

Topology

The map or plan of the network. The physical topology describes how the wires or cables are laid out, and the logical or electrical topology describes how the information flows.

Trace Packet

In a packet-switching network, a unique packet that causes a report of each stage of its progress to be sent to the network control centre from each visited system element.

Traceroute

An operation of sending traces packets for determining information; traces the route of UDP packets for the local host to a remote host. Normally traceroute displays the time and location of the route taken to reach its destination computer.

Tripwire

A software tool for security. Basically, it works with a database that maintains information about the byte count of files. If the byte count has changed, it will identify it to the system security manager.

Trojan Horse

An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

Trojan Horse

An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

Trusted Computer System Evaluation Criteria

(TCSEC) A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information.

Trusted Computing Base (TCB)

The totality of protection mechanisms within a computer system including hardware, firmware, and software - the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system.

Trusted Network Interpretation

The specific security features, the assurance requirements and the rating structure of the Orange Book as extended to networks of computers ranging from isolated LANs to WANs.

TTY Watcher

A hacker tool that allows hackers with even a small amount of skill to hijack terminals. It has a GUI interface.

Vaccines

Program that injects itself into an executable program to perform a signature check and warns if there have been any changes.

V

Virus

A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.

Vulnerability

Hardware, firmware, or software flow that leaves AIS opens for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Vulnerability Analysis

Systematic examination of an AIS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Vulnerability Analysis

The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures

Vulnerability Assessment

A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack

W

WAN

Wide Area Network. A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than

those served by local area networks.

War Dialer

A program that dials a given list or range of numbers and records those which answer with handshake tones, which might be entry points to computer or telecommunications systems.

Web bug

A link on a given Web page or embedded in an email message that contains a link to a different Web site and therefore passes a call, and information, unknown to the user, to a remote site. Most commonly a web bug is either invisible or unnoticeable (typically it is one pixel in size) in order not to alert the user to its presence.

Worm

Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads.

Z

Zombie

A specialized type of backdoor or remote access program designed as the agent, or client (middle layer) component of a DDoS (Distributed Denial of Service) network. Once a zombie is installed on a computer, it identifies itself to a master computer, and then waits for instructions from the master computer. Upon receipt of instructions from the master computer, a number of zombie machines will send attack packets to a target computer. Zombie may refer to the control program run to control one of the middle layer computers, or it may refer to a computer so controlled.

Digital Science Glossary:

A

Acquisition

The process of creating a duplicate copy of digital media for the purposes of examining it

C

Computational forensics

Computational forensics is digital forensics with the use of artificial intelligence

D

Digital media

Used within the fields to refer to the physical medium (such as a hard drive) or data storage device

E

e-discovery or eDiscovery

A common acronym for electronic discovery

Exhibit

Digital media seized for investigation is usually referred to as an "exhibit"

H

Hashing

Within the field "hashing" refers to the use of hash functions (e.g. CRC, SHAI OR D5) to verify that an "image" is identical to the source media

I

Image

A duplicate copy of some digital media created as part of the forensic process

Imaging

Synonym of "acquisition"

L

Live analysis

Analysis of a piece of digital media from within itself; often used to acquire data from RAM where this would be lost upon shutting down the device

S

Slack space

The unused space at the end of a file in a file system that uses fixed size clusters (so if the file is smaller than the fixed block size then the unused space is simply left). Often contains deleted information from previous uses of the block

Steganography

The word steganography comes from the Greek name “steganos” (hidden or secret) and “graphy” (writing or drawing) and literally means hidden writing. Steganography uses techniques to communicate information in a way that is hidden

U

Unallocated space

Cluster of a media partition not in use for storing any active files. They may contain pieces of files that were deleted from the file partition but not remove from the physical disk

V
Verification
A term used to refer to the hashing of both source media and acquired image to verify the accuracy of the copy

W
Write blocker
The common name used for a forensic disk controller, hardware used to access digital media in a read only fashion

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)

Document compiled by: Marthinus Engelbrecht 30th September 2015

Document Reviewed by: ***25 July 2014***

Document Approved by: ***6 April 2016***

RECOMMENDED BEST PRACTISE METHODOLOGIES:

Information Security ERM) Information Technology (IT) frameworks and standards provide an organization with approaches for identifying, analysing, responding to and monitoring risks (opportunities and threats) within the internal and external contexts in which it operates. How an organization applies external frameworks and standards depends on its nature.

The Security Management framework is underpinned by the internationally recognised standard of ISO/IEC 27001: The Code of Practice for Information Security Management. The ISO/IEC 27001 is an Information Security Management Standard, first published by the International Organization for Standardisation, or ISO, in December 2000 as ISO/IEC 17799. ISO/IEC 27001 is high level, broad in scope, and conceptual in nature, and is suited to multiple types of enterprises and applications.

The framework also incorporates additional standards and guidelines that include:

- The ISF Standard of Good Practice which addresses information security from a business perspective and focuses on the arrangements made by leading Organization 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 (Iinformation 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 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 inseperable. 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.