



USAID
FROM THE AMERICAN PEOPLE

PHILIPPINE GOVERNMENT INTERNAL AUDIT MANUAL

FORENSIC AUDITING

JUNE 15, 2011

This publication was produced for review by the United States Agency for International Development. It was prepared by Management Systems International.

GOVERNMENT INTERNAL AUDIT MANUAL

FORENSIC AUDITING



A SUBSIDIARY OF COFFEY INTERNATIONAL, LTD.

600 Water Street, SW, Washington, DC 20024, USA

Tel: +1.202.484.7170 | Fax: +1.202.488.0754

www.msiworldwide.com



Contracted under Cooperative Agreement 492-A-00-09-00032-00

The Integrity Project

DISCLAIMER

The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

LIST OF ACRONYMS

AuditCom	Audit Committee
DS	Department Secretary
GB	Governing Board
GFI	Government Financial Institution
GOCC	Government-Owned and/or -Controlled Corporation
HoA	Head of Agency
HoIA	Head of Internal Audit
ICS	Internal Control System
IA	Internal Auditor
IAS/IAU	Internal Audit Service/Internal Audit Unit
IIA	Institute of Internal Auditors
NGICS	National Guidelines on Internal Control Systems
PGIAM	Philippine Government Internal Audit Manual

TABLE OF CONTENTS

INTRODUCTION	1
CHAPTER I. FRAUD-EFFECTIVE INTERNAL CONTROL SYSTEM (ICS).....	2
I. ICS AND FRAUD PREVENTION AND DETECTION	2
1.1. <i>The Strength of an Organization’s Internal Controls Must Be Assessed</i>	2
1.2. <i>Checklist Models for Performing Internal Control Assessments</i>	3
1.2.1. Physical Security Controls.....	4
1.2.2. Organizing Controls.....	4
1.2.3. Supervision and Output Controls.....	5
1.2.4. Monitoring Controls.....	6
1.2.5. Evaluation Controls.....	7
1.2.6. Staffing Controls.....	7
1.2.7. Asset Accounting Controls.....	8
II. MANAGEMENT’S RESPONSIBILITY TO ESTABLISH A FRAUD AVOIDANCE SYSTEM ENCOMPASSING THE FOUR PILLARS OF FRAUD MANAGEMENT	9
II.1. <i>Prevention Pillar</i>	9
II.2. <i>Detection Pillar</i>	9
II.3. <i>Investigation Pillar</i>	9
II.4. <i>Prosecution Pillar</i>	9
III. THE AUDITOR’S RESPONSIBILITIES FOR FRAUD DETECTION	9
III.1. <i>General IA Responsibilities</i>	10
III.1.1. Planning	10
III.1.2. Execution.....	11
III.1.3. Reporting.....	11
III.2. <i>Relevant International Standards</i>	11
III.3. <i>Why Auditors Do Not Detect More Fraud</i>	12
III.4. <i>Incorporating Fraud Detection Into the Audit Program</i>	12
CHAPTER II. FRAUD	14
I. MEANING AND CONCEPT OF FRAUD	14
1.1. <i>Fraud Definitions and Characteristics</i>	14
1.2. <i>Characteristics Common to All Fraud</i>	14
II. CORRUPTION AS A CATEGORY OF FRAUD.....	15
III.1. <i>Common Corruption Offenses</i>	15
II.1.1. MALVERSATION.....	15
II.1.1.1. Malversation of Public Funds or Property (Article 217, RPC).....	15
1. Elements of Malversation under Article 217 of the RPC.....	15
2. Presumption of Misappropriation	16
II.1.1.2. Illegal Use of Public Funds (Article 220, RPC); Elements.....	16
II.1.1.3. Failure to Render Accounts (Article 218, RPC); Elements.....	16
II.1.1.4. Failure to Render Accounts before Leaving the Country (Article 219, RPC); Elements ...	17
II.1.1.5. Failure to Deliver Public Funds or Property (Article 221, RPC); Elements.....	17
II.1.2. BRIBERY. KINDS OF BRIBERY UNDER THE RPC.....	17
II.1.2.1. Direct Bribery (Article 210); Elements.....	17
II.1.2.2. Indirect Bribery (Article 211, RPC).....	18
II.1.2.3. Qualified Bribery (Article 211-A, RPC); Elements.....	18
II.1.2.4. Corruption of Public Officials (Article 212, RPC); Elements.....	18
II.1.3. ANTI-GRAFT AND CORRUPT PRACTICES ACT (R.A. NO. 3019).....	18
II.1.3.1. Paragraph 3(e); Elements.....	18
II.1.3.2. Paragraph 3(g), R.A. No. 3019; Elements	19
II.1.4. PLUNDER	19
1. Elements.....	19
2. Evidence.....	19
II.1.5. FALSIFICATION OF PUBLIC DOCUMENTS (ARTICLE 171, RPC).....	20

1.	Elements.....	20
2.	Ways of Committing Falsification	20
III.2.	CIVIL FORFEITURE OF ILL-GOTTEN WEALTH.....	20
II.2.1.	R.A. No. 1379	20
II.2.2.	Supreme Court A.M. No. 05-11-04-SC	21
II.2.3.	Civil Forfeiture for Non-Filing of Statements of Assets Liabilities and Net Worth under R.A. 3019 and R.A. 6713.....	21
III.3.	<i>Factors That Influence Decisions To Commit Fraud.....</i>	21
III.4.	<i>How Fraud Occurs</i>	23
III.5.	<i>Exposure to Fraud.....</i>	23
II.5.1.	Internal Fraud.....	23
II.5.2.	External Fraud	23
II.5.3.	Collusion	24
III.	FRAUD DETECTION BY PHILIPPINE GOVERNMENT INTERNAL AUDITORS	24
III.1.	<i>Recognizing Red Flags</i>	24
III.1.1.	Procurement and Contracting	25
III.1.1.1.	Common Procurement and Contracting Fraud Indicators	25
III.1.2.	Treasury/Cash Functions.....	25
III.1.2.1.	Common Petty Cash Fraud Indicators	26
III.1.2.2.	Common Cash from Bank Account Fraud Indicators	26
III.1.3.	Assets/ Inventory.....	26
III.1.3.1.	Common Assets and Inventory Fraud Indicators	26
III.1.4.	Pension And Investment Fund Operations	26
III.1.5.1.	Common Pension and Investment Fund Fraud Indicators.....	27
III.1.5.	Travel Expenses.....	27
III.1.5.1.	Common Travel Fraud Indicators	27
III.1.6.	Fraud in a Computerized Environment.....	28
III.1.6.1.	Common Computer Area Fraud Indicators	28
III.2.	<i>Responding To the Existence of Red Flags.....</i>	28
III.3.	<i>Reacting to Allegations.....</i>	29
III.4.	<i>When Positive Fraud Indictors Are Identified.....</i>	29
III.5.	<i>Demonstrating the Probability of Fraud.....</i>	30
	CHAPTER III. FORENSIC AUDITING.....	32
I.	MEANING AND SCOPE OF FORENSIC AUDITING	32
II.	WHEN DOES THE AUDIT STOP AND A FORENSIC AUDIT/INVESTIGATION BEGIN?	32
II.1.	<i>WHEN FORENSIC AUDIT/INVESTIGATION BEGINS</i>	33
II.1.1.	Jurisdiction of the Internal Auditor	33
II.1.2.	Deciding to Conduct a Forensic Audit/Investigation	34
II.1.3.	Planning and Preparing For the Forensic Audit.....	34
II.1.4.	An Attorney Should Be Assigned to the Fraud Audit/Investigation.....	36
II.1.5.	An Investigative Theory Must Be Developed.....	36
III.	FORENSIC AUDIT TECHNIQUES.....	37
III.1.	<i>Formulating Investigative Questions</i>	37
III.2.	<i>Forensic Audit Evidence Standards.....</i>	38
	CHAPTER IV. FORENSIC EVIDENCE UNDER THE CONTEXT OF PHILIPPINE LAW	40
I.	DEFINITION AND PURPOSE OF EVIDENCE.....	40
I.1.	<i>Definition</i>	40
I.2.	<i>Purpose.....</i>	40
I.3.	<i>Characteristics.....</i>	40
II.	STANDARD OF PROOF IN CRIMINAL CASES.....	41
II.1.	<i>Probable Cause.....</i>	41
II.2.	<i>Guilt Beyond Reasonable Doubt</i>	41
III.	TYPES OF EVIDENCE	41
III.1.	<i>Based on the Form of the Evidence.....</i>	41
III.1.1.	Objects.....	41
III.1.2.1.	Real Evidence.....	42
III.1.2.2.	Demonstrative Evidence.....	42

III.1.2.	Documents	42
III.1.2.1.	Public Documents	42
III.1.2.2.	Private documents – ALL other writings that are not public.....	42
III.1.2.3.	Electronic documents	42
III.1.3.	Testimony.....	42
III.2.	<i>Based on the Connection to the Factual Issue</i>	43
III.2.1.	Direct Evidence	43
III.2.2.	Circumstantial Evidence	43
III.2.3.	Substitute for Evidence.....	43
III.2.3.1.	Mandatory judicial notice.....	43
III.2.3.2.	Discretionary judicial notice.....	43
III.2.3.3.	Judicial admissions.....	44
III.2.3.4.	Conclusive presumptions.....	44
III.2.3.5.	Disputable presumptions	44
IV.	RULES OF ADMISSIBILITY OF EVIDENCE	44
IV.1.	<i>Authentication</i>	44
IV.1.1.	Real Evidence	45
IV.1.1.1.	Ready identifiability	45
IV.1.1.2.	Chain of custody.....	45
IV.1.2.	Demonstrative Evidence	45
IV.1.3.	Challenging the Authenticity of Object Evidence.....	46
IV.1.4.	Documents.....	46
IV.1.4.1.	Best Evidence Rule.....	46
1.	General Rule	46
2.	Exceptions; Proof of contents by secondary evidence	47
IV.1.5.	Testimony.....	49
IV.1.5.1.	Qualifications	49
IV.1.5.2.	Disqualifications	49
1.	Mental condition	49
2.	Immaturity.....	49
IV.1.5.3.	Testimonial Privilege.....	50
IV.1.5.4.	Admissions and Confessions.....	52
IV.1.5.5.	Conduct as Evidence.....	54
IV.1.5.6.	Testimonial Knowledge	55
IV.1.5.6.1.	Hearsay Rule	55
IV.1.5.6.2.	Opinion	57
IV.1.5.6.3.	Character Evidence.....	58
IV.2.	<i>Relevance</i>	58
IV.3.	<i>Competency</i>	59
V.	WEIGHT AND SUFFICIENCY OF EVIDENCE	59
V.1.	<i>Direct Evidence</i>	59
V.2.	<i>Circumstantial Evidence</i>	60
V.3.	<i>Probable Cause</i>	60
V.4.	<i>Preponderance of Evidence</i>	60
V.5.	<i>Proof beyond Reasonable Doubt</i>	61
V.6.	<i>Substantial Proof</i>	61
VI.	RULE ON ELECTRONIC EVIDENCE	61
VI.1.	<i>Defined Terms under the E-Commerce Act</i>	61
VI.2.	<i>Electronic Documents</i>	63
VI.2.1.	Electronic documents as functional equivalent of paper-based documents.....	63
VI.2.2.	Admissibility	63
VI.2.3.	Privileged communication	64
VI.3.	<i>Best Evidence Rule</i>	64
VI.3.1.	Original of an electronic document	64
VI.3.2.	Copies as equivalent of the originals.....	64
VI.4.	<i>Authentication of Electronic Documents</i>	64
VI.4.1.	Burden of proving authenticity.....	64
VI.4.2.	Manner of authentication	64
VI.5.	<i>Electronic Signatures</i>	65
VI.5.1.	Definition.....	65
VI.5.2.	Authentication of electronic signatures	65

VI.5.3.	Disputable presumptions relating to electronic signature	65
VI.5.4.	Disputable presumptions relating to digital signatures.....	66
VI.5.5.	Evidentiary Weight of Electronic Documents.....	66
VI.5.6.	Integrity of an Information and Communication system.....	66
VI.5.7.	Business Records as Exception to the Hearsay Rule	67
VI.5.8.	Overcoming the presumption.....	67
VI.6.	<i>Method of Proof</i>	67
VI.6.1.	Affidavit evidence	67
VI.6.2.	Cross-examination of deponent.....	67
VII.	AUDIO, PHOTOGRAPHIC, VIDEO, AND EPHEMERAL EVIDENCE	67
VII.1	<i>Audio, video and similar evidence</i>	67
VII.2	<i>Ephemeral electronic communication</i>	68
VIII.	TECHNIQUES FOR COLLECTING FORENSIC EVIDENCE	68
VIII.1.	<i>Document Examination and Analysis Techniques</i>	68
VIII.2.	<i>Examining Documents for Alterations</i>	68
VIII.3.	<i>Detecting Forged Documents</i>	69
VIII.4.	<i>Document Analysis Techniques</i>	69
VIII.4.1.	Link analysis.....	69
VIII.4.2.	Telephone records analysis.....	69
VIII.4.3.	Flow analysis.....	70
VIII.4.4.	Behavioral analysis.....	70
VIII.4.5.	Financial analyses.....	70
VIII.5.	<i>Laboratory Analysis Techniques</i>	71
VIII.6.	<i>Observations and Surveillance Techniques</i>	72
VIII.6.1.	Observations.....	72
VIII.6.2.	Surveillance	72
VIII.6.3.	Undercover Investigation Techniques.....	73
VIII.6.4.	Modified Undercover Techniques.....	73
VIII.7.	<i>Interviewing Techniques</i>	73
VIII.7.1.	General Interviewing Guidelines	74
VII.7.1.1.	Interviews with Witnesses.....	75
VII.7.1.2.	Interviews with Suspects	75
VII.7.1.3.	Choosing Question Types for Interviews.....	75
VII.7.1.4.	Confessions and Admissions of Wrongdoing During an Interview	76
VIII.7.2.	Preliminary Interview	77
VIII.7.3.	Final Interview.....	77
VIII.8.	<i>Records of all Interviews Must be Prepared</i>	77
IX.	ORGANIZING AND DOCUMENTING THE WORK PERFORMED	78
IX.1.	<i>Collecting and Maintaining Documents</i>	78
IX.2.	<i>The Chain of Custody and the Care of Forensic Evidence</i>	79
IX.2.1.	Marking seized documents	79
	CHAPTER V. INTERIM AND FINAL INVESTIGATION REPORTS; TESTIFYING IN COURT	81
I.	INTERIM REPORT PREPARATION GUIDANCE.....	81
II.	FINAL REPORTS	82
III.	TESTIFYING IN COURT	83

INTRODUCTION

This Internal Audit Manual on Forensic Auditing discusses forensic auditing as a tool to prevent, detect, investigate and support the prosecution of fraud. It explains the auditor's responsibility to take a proactive approach in detecting, documenting, and referring instances of probable fraud, the concept and principles underlying forensic audit; the standards in the effective conduct of forensic audit; the techniques, analytical tools and approaches used in forensic auditing; the gathering, preservation and use of forensic evidence for purposes of establishing administrative, civil and criminal liability; the specific stages and the logical procedures involved in forensic audit; and fraud detection and investigative processes specific in the conduct of forensic audit and investigation.

Chapter I. starts with a discussion of the role of a fraud-effective ICS. This is similar to the discussion in Part I, Chapter II, of the PGIAM Manual, but within the context of fraud prevention. It continues with the discussion of the role of the IA in forensic audit, the attitude and necessary skills that they have to imbibe. Chapter II discusses the concept of fraud as it relates to administrative and criminal standards and prosecution. Chapter III proceeds with a discussion of forensic audit – its concept and principles, the audit/investigative process, the techniques in gathering and preserving evidence, as well as the standards of evidence that need to be met. Chapter IV discusses forensic evidence under the context of Philippine law. Finally, Chapter V discusses investigation reports and best practices for testifying in court.

CHAPTER I. FRAUD-EFFECTIVE INTERNAL CONTROL SYSTEM (ICS)

I. ICS AND FRAUD PREVENTION AND DETECTION

The establishment of a good ICS to prevent and detect fraud is primarily the responsibility of operating management and can help reduce the probability of fraud. Strong internal controls can help eliminate the elements that encourage fraud and prevent or deter fraud from occurring.

Some frauds are facilitated because of system weaknesses. Other frauds result from the failure to follow proper internal control procedures. Sometimes fraud occurs because too much trust has been placed in one individual with no effective separation of duties. When internal controls are not followed, or are ignored, or are overridden by management or others, the elements that enable fraud to occur emerge, and prime opportunities for fraudulent behavior exist.

Some fraud occurs because of the absence of a hands-on or supervisory review of transactions. For example, computer frauds, defined as those where the computer is instrumental in the perpetration of the fraud, sometimes result when transactions are processed that would ordinarily be questioned if they were processed manually and had been subject to a hands-on review.

While some individuals would never contemplate perpetrating a fraud, others may choose to engage in fraudulent actions if they think their fraudulent actions cannot be prevented or will be undetected. A high probability of detection by internal controls that are designed to prevent or detect fraud will help deter the commission of fraud.

However, fraud may still occur regardless of the strength of those internal controls.

Prevention of fraud is always preferable to the detection of fraud. Management must therefore develop a strong ICS to prevent fraud. However, these preventive controls are almost never sufficient to stop those determined to attempt to carry out a fraudulent act or engage in fraudulent behavior. Therefore detection controls are also important. Detection controls are established to detect fraud, errors, and omissions after these events have taken place, and if they have not been prevented.

I.1. The Strength of an Organization's Internal Controls Must Be Assessed

Strong internal controls reduce the probability of fraud; conversely, weak controls increase the probability of fraud. Therefore, IAs must assess these controls so that they can identify weaknesses in them, or determine that appropriate controls do not exist at all. Weaknesses in internal controls may indicate to the IA the real potential for fraudulent acts. Accordingly, the IA should consider internal controls as important fraud deterrent and detection system components.

As a technique for detecting the absence of, or weaknesses in any of these internal controls, it is a usual audit practice to develop an internal control checklist for each relevant area to be audited for use in assessing the adequacy of those internal controls. That checklist should be tailored to accommodate the audit environment. The results of the execution of each checklist by the auditor will provide him or her with information about the adequacy of the internal

controls in each area, and contribute to the auditor’s assessment regarding the potential for the existence of fraud.

For example, an internal control checklist for procurement controls may include the following questions:

**Table I. CHECK LIST
INTERNAL CONTROLS - PROCUREMENT CONTROLS**

Question Number	Check List Internal Controls – Procurement Controls	Yes	No
1	Is the delivery of materials checked to assure that they conform to contract or purchase order requirements for quality, quantity, and timely delivery?		
2	Have alternate sources of supply been developed or have purchases generally been made from single sources?		
3	Have contracts or purchase orders only awarded to the lowest responsible bidder?		
4	Are material changes to the contract or purchase order made after the award, subject to a documented review and approval process?		
5	Is a procedure in place to justify, document, and review the disqualification of contractors or vendors?		
6	Has a bid and proposal evaluation committee been established that evaluates bids and proposals using a documented bid/proposal evaluation process?		
7	Are procedures in place to prevent the release of procurement information to preferred or selected contractors or vendors?		
8	Is there a procedure in place to verify contractor or vendor certification as to the stage of contract completion or delivery?		
9	Are procedures in place to assure that all the bids and/or proposals received are valid and genuine?		
10	Have the controls ever detected fraud in this area?		

I.2. Checklist Models for Performing Internal Control Assessments

Every component and activity of an organization must have internal controls in place to:

- help assure that the desired objectives of that component are accomplished efficiently, effectively, and economically,
- protect assets,
- assure that all transactions are promptly and accurately recorded,
- assure that all applicable laws and regulations are complied with, and
- prevent and detect fraud.

The following are illustrations of model checklists with accompanying questions, which might be modified and used by auditors when assessing the adequacy of internal controls in certain specific areas. A determination by the IA that controls are inadequate or more significantly, non-existent, is an indication of the risk of fraud.

1.2.1. Physical Security Controls

These controls monitor and restrict access to an organization's assets. Physical assets can range from documents, files and accounting records, to computer equipment, databases and information systems hardware, to office supplies, furniture and equipment, to the stock of checks used to pay suppliers, contractors, and employees. These security controls apply not only to assets, but also to an organization's premises, and to all the areas on the premises that are critical to the operation of the organization.

All such assets and property must be carefully controlled and secured. There should be an assurance that access to them is restricted to only those who have a need to use them. These controls should function to assure that there is no damage, or theft or unauthorized use.

Access to computer systems is an important area that should be very carefully controlled, not only to prevent unauthorized access and use, but also to protect the integrity of the stored data. The computer itself is also vulnerable to theft, both in terms of hardware and software. This type of theft carries with it the additional risk and associated costs of potentially causing a major disruption to the core operations of an organization.

An internal control check list for assessing the adequacy of physical security controls may include the following questions:

**Table 2: CHECK LIST
INTERNAL CONTROLS-PHYSICAL SECURITY**

Question Number	Check List Internal Controls – Physical Security	Yes	No
1	Are procedures in place that restrict access to accounting records to only authorized personnel?		
2	Are procedures in place that restrict access to information systems to only authorized personnel?		
3	Are inventory records maintained of all desktop computers and other computer equipment?		
4	Are periodic physical inventories taken of all desktop computers and computer equipment and other assets?		
5	Is the stock of blank checks used to pay suppliers, contractors, employees, and others kept in a secure, locked place?		
6	Is access to the stock of blank checks used to pay suppliers, contractors, employees, and others restricted to only authorize persons?		
7	Is access to the organization's premises controlled by a security force or, by other appropriate security measures?		
8	Are inventory records maintained of all furniture and office equipment?		
9	Have the controls ever detected fraud in this area?		

1.2.2. Organizing Controls

Organizing involves the allocation of responsibility to individuals or groups so that they work together to achieve objectives in the most efficient manner, and to prevent or reduce the opportunities to commit fraud. Major control principles in organizing relevant to fraud include:

- *A clear definition of the responsibility of all individuals for resources, activities, objectives and goals.* This includes defining the levels of authority. For example, a

preventive control might set a limit on the amounts of cash that may be disbursed or authorized for disbursement by individual members of the organization. To be effective, controls must be installed to ensure that payments have been properly authorized.

- *Establishment of clear reporting lines and effective spans of command to facilitate adequate supervision.* This helps assure that responsibility and accountability for assigned duties are unambiguous and clearly understood.
- *Separating duties to avoid conflicts of interest or opportunities for abuse.* This is largely a preventive control that helps assure that the key functions and controls over a process are not all carried out by the same individual. For example the function of ordering goods should be kept separate from receipt of the goods ordered, and from the distribution and the use of the goods. Similarly, authorization and payment of invoices for those goods should also be handled separately.

An internal control checklist for assessing the adequacy of organizing controls may include the following questions:

**Table 3: CHECK LIST
INTERNAL CONTROLS - ORGANIZING CONTROLS**

Question Number	Check List Internal Controls – Organizing Controls	Yes	No
1	Has a table of organization been developed?		
2	Have the duties and responsibilities of all the positions on the table of organization been clearly defined and documented?		
3	Have position descriptions been prepared for all the positions on the table of organization?		
4	Are position descriptions subject to a periodic desk audit to determine whether the position descriptions reflect the duties actually being performed?		
5	Have the goals and objectives of the organization been clearly defined and documented?		
6	Have the levels of authority, including the use and application of resources, for all the positions on the table of organization been established, clearly articulated, and documented?		
7	Have clear reporting lines been established and documented?		
8	Do the lines of reporting assure the most effective spans of control and provide for adequate supervision?		
9	Have any instances of fraud been detected by these controls?		

1.2.3. Supervision and Output Controls

Supervision is the function by which operating managers closely review the work and performance of their staff. It provides operating management with a means to determine whether the staff is performing at a level that meets established standards, and in accordance with management’s instructions. Supervision and output review includes checks over adherence with internal controls by staff at all levels. It acts as both a prevention and detection measure and involves monitoring the working methods and outputs of staff. These internal controls are especially vital where staff is dealing with cash or accounting records. Random, unannounced spot checks by managers can be an effective anti-fraud measure.

An internal control checklist for assessing the adequacy of supervision and output controls may include the following questions:

**Table 4: CHECK LIST
INTERNAL CONTROLS-SUPERVISION AND OUTPUT CONTROLS**

Question Number	Check List Internal Controls – Supervision and Output Controls	Yes	No
1	Have guidelines been established for setting staff-supervisor expectations?		
2	Have those guidelines been disseminated to all staff and all supervisors?		
3	Have procedures and standards been established to guide supervisory review?		
4	Are the results of supervisory reviews documented, filed and available for review?		
5	Are procedures in place to assure that supervisory reviews take place?		
6	Are procedures in place that provide for follow up or corrective action based on the supervisory review?		
7	Does the supervisory review process include random checks or unannounced checks or observations of staff output?		
8	Does the supervisory review process include the examination of staff output and work products?		
9	Have any of the supervisory reviews uncovered fraud?		

1.2.4. Monitoring Controls

Management information systems should include measures and indicators of performance to help determine efficiency, effectiveness, economy and quality of service and detect fraud. Effective monitoring, including random checks, should help deter and detect some types of fraudulent activity.

An internal control checklist for assessing the adequacy of monitoring controls may include the following questions:

**Table 5: CHECK LIST
INTERNAL CONTROLS-MONITORING CONTROLS**

Question Number	Check List Internal Controls – Monitoring Controls	Yes	No
1	Has a performance measurement system been established to monitor the activities of each component of the organization?		
2	Do the performance measures include uniform, recognized measurement standards?		
3	Are these uniform, recognized standards periodically assessed to assure current applicability?		
4	Do the performance measures include assessments of efficiency?		
5	Do the performance measures include assessments of economy?		
6	Do the performance measures include assessments of effectiveness?		
7	Do the performance reviews include period-to-period comparisons of operational and financial data?		

Question Number	Check List Internal Controls – Monitoring Controls	Yes	No
8	Are deviations from performance standards documented and followed up to determine the reasons for the deviation?		
9	Have any of the performance measurement initiatives disclosed fraud?		

1.2.5. Evaluation Controls

Policies and activities should be evaluated periodically for economy, efficiency and effectiveness. The managers of the operation may perform evaluations, but they are usually more effective when performed by an independent team, i.e., the IAS/IAU. Such evaluations are often effective in detecting fraudulent activities.

An internal control checklist for assessing the adequacy of evaluation controls may include the following questions:

**Table 6: CHECK LIST
INTERNAL CONTROLS-EVALUATION CONTROLS**

Question Number	Check List Internal Controls – Evaluation Controls	Yes	No
1	Has an evaluation process been established to assure that the policies and procedures guiding each organizational component are periodically evaluated?		
2	Is the evaluation process being carried out as planned?		
3	Is a written report prepared after each evaluation documenting the results?		
4	Are the results of the evaluation process analyzed to determine whether corrective action is required?		
5	Are the reasons for the need for corrective action determined?		
6	Are corrective actions taken when warranted?		
7	Are the corrective actions taken analyzed to determine their effectiveness?		
8	Do independent evaluators perform the evaluations?		
9	Have any of the evaluations disclosed fraud?		

1.2.6. Staffing Controls

Adequate staffing is essential for a system to function effectively. Weaknesses in staffing can negate the effect of other controls. Positions involving control of particularly high value assets or resources may need the application of additional vetting procedures. Rotation of staff between positions can help prevent or detect collusion or fraud.

An internal control checklist for assessing the adequacy of staffing controls may include the following questions:

**Table 7: CHECK LIST
INTERNAL CONTROLS-STAFFING CONTROLS**

Question Number	Check List Internal Controls – Staffing Controls	Yes	No
1	Are all positions supported by a documented position description?		
2	Are background checks and credential verifications performed of all		

	potential employees before they are offered a position?		
3	Is all employment subject to a probationary period?		
4	Is the performance of all employees evaluated at least annually using a standard staff evaluation format?		
5	Are the employees who staff sensitive positions bonded or insured?		
6	Is provision made in staffing assignments for the separation of duties to prevent collusion?		
7	Is there a staff rotation policy in place for sensitive positions?		
8	Are spot checks and unannounced visits made to employee work Stations to monitor performance?		
9	Have any of the staffing controls detected fraud?		

1.2.7. Asset Accounting Controls

Asset registers / inventory records are used for management accounting purposes. Well-informed decision-making requires access to reliable data. The most important role played by an asset register is to provide a basis for the analysis of vital property information. This relies upon a solid data collection methodology, data integrity and flexibility of analysis. Asset registers provide a robust form of data collection and storage, enabling a readily accessible and dynamic basis for asset control and can help detect fraud related losses.

An internal control checklist for assessing the adequacy of asset accounting controls may include the following questions:

**Table 8: CHECK LIST
INTERNAL CONTROLS-ASSET ACCOUNTING CONTROLS**

Question Number	Check List Internal Controls – Asset Accounting Controls	Yes	No
1	Is the asset register and the physical inventory periodically reconciled?		
2	Is there a written procedure in place to assure that all acquired assets are recorded promptly upon acquisition?		
3	Is there a procedure in place to assure that asset disposal is properly transacted and promptly recorded?		
4	Are all the assets subjected to a periodic review for obsolescence?		
5	Is the condition of all the assets subject to a periodic inspection?		
6	Is a physical inventory taken each year of all assets?		
7	Are there policies and procedures in place to monitor the use of all assets?		
8	Are there controls in place to prevent the use of assets by employees and other unauthorized users?		
9	Is there a security system in place protecting all assets?		
10	Has fraud ever been detected by these controls?		

If as a result of assessing controls, potential deficiencies or weaknesses are identified, the IA must consider that these inadequacies suggest opportunities for fraud to occur and should be considered during audit planning.

II. MANAGEMENT'S RESPONSIBILITY TO ESTABLISH A FRAUD AVOIDANCE SYSTEM ENCOMPASSING THE FOUR PILLARS OF FRAUD MANAGEMENT

Prevention, detection, investigation, and prosecution are considered the four pillars of fraud management. Each is as critical as each of the others if a fraud management system or initiative is to be successful in combating fraud.

II.1. Prevention Pillar

The prevention pillar must detail how an organization will try to prevent fraudulent acts from occurring. It will assign responsibility for fraud prevention measures and hold those assigned the responsibility accountable of their efforts. Examples of fraud prevention measures include implementing an anonymous tip reporting system, conducting employment background checks and ensuring the physical security of assets.

II.2. Detection Pillar

The detection pillar is the second phase of fraud management. It involves a detailed detection initiative or systematic process of detecting fraud. At a minimum, organizations must designate and train their staff to carry out fraud detection activities.

II.3. Investigation Pillar

The investigation pillar brings the prevention and detection pillars together and provides evidence that either supports or refutes fraud allegations. Similar to the first two pillars of a fraud management program, organizations should clearly outline how allegations will be investigated and by whom. During the investigation pillar, predication must be determined to exist. Predication is simply a set of facts that would lead a reasonable individual to believe a fraud has occurred, is occurring, or will occur. Without predication, an investigation is not warranted.

II.4. Prosecution Pillar

The prosecution pillar is the fourth and final pillar in a system for combating fraud. Prosecution is the institution and conduct of legal proceedings against a defendant for criminal behavior. A judicial proceeding commences and a determination of a person's innocence or guilt by due process of law results.

Prevention, detection, and investigation have little meaning unless there is a commitment to the prosecution of those who commit acts of fraud in government.

The absence of a fraud management system which does not encompass each of the four pillars of fraud management may indicate to the IA that management may not be fully committed to combating fraud, or that its efforts addressing fraud may need improvement.

III. THE AUDITOR'S RESPONSIBILITIES FOR FRAUD DETECTION

The IA should have sufficient knowledge to identify the indicators of fraud but is generally not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud. Among the principal duties of the IA is to be proactive in identifying opportunities that could allow fraud to take place, assess the need for investigation by

evaluating these opportunities and, if necessary, extending audit procedures that will allow a conclusion to be drawn as to whether probable fraud exists, and notifying the appropriate authorities if an incident or incidents of probable fraud are documented.

When an IA suspects wrongdoing, prompt recommendation need to be given to management to establish or enhance cost-effective controls to help deter fraud, and to the DS/HoA or GB/AuditCom. The IA may recommend whatever investigation is considered necessary in accordance with law, given the circumstances. Hence, if during an audit assignment (i.e., assessment of ICS) the IA identifies control weaknesses that could allow fraud, or finds evidence that fraud may have been perpetrated or is occurring, the following actions should immediately be taken:

- a. Refer to local internal audit policy/procedures on handling suspected fraud and/or the organization's fraud response plan;
- b. Decide whether to extend the audit work and design additional tests directed towards the identification of activities which may be indicators of possible fraud;
- c. Decide whether there is clear evidence of possible fraud sufficient to recommend an investigation to the specialized fraud/forensic auditing group of the IAS/IAU (but only after extended procedures have been performed);
- d. Ensure that the extent of the concern is captured and communicated through appropriate evidence so that implications can be considered in the formation of the HoIA's overall report;
- e. Consider, after consultation with appropriate authorities, at what point management should be advised of the IAS/IAU's concerns, who should be advised and how (e.g. staff with designated anti-fraud responsibilities); and
- f. Consider who might be involved in the suspected probable fraud so as to ensure that alleged perpetrators are not alerted and given an opportunity to tamper with or destroy evidence.¹

III.1. General IA Responsibilities

The general responsibilities of the IA may be summarized into: Planning, Execution and Reporting.

III.1.1. Planning

In planning an audit, the IA auditors must develop an awareness of the characteristics and types of fraud associated with the area being audited, in addition to awareness of the vulnerabilities created by identified weaknesses in controls and the lack of a rational system for eliminating fraud. This awareness allows a risk assessment with vulnerability-to-fraud components to be developed and executed, and an audit planned which provides a reasonable expectation of detecting possible fraud and other irregularities if they exist. Essential to planning the audit is a knowledge and understanding of the general and specific laws and regulations, as well as the policies and procedures that govern the area to be audited.

¹ Found at http://www.hm-treasury.gov.uk/d/fraud_internal_auditor_250510 last visited April 12, 2011.

III.1.2. Execution

In carrying out an audit, the IA must exercise due professional care in recognizing and pursuing indications of possible fraud, irregularities, and other illegal acts. Audit work must not interfere with or otherwise obstruct potential future investigations, and legal or prosecutorial proceedings.

III.1.3. Reporting

In communicating audit results, auditors should report all fraud, irregularities, illegal acts, and other noncompliance.

III.2. Relevant International Standards

Virtually all contemporary audit standards impose an obligation on the auditor, to take positive actions that will help assure the detection of probable fraud if it exists. For example:

- Standards promulgated by the Institute of Internal Auditors (“IIA”)- Standard 1210.A2 states, “The internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.”

IIA Practice Advisory 1210.A2-1: Identification of Fraud, and

IIA Practice Advisory 1210.A2-2: Responsibility for Fraud Detection, interpret that Standard and provide guidance for its implementation.

- Standards promulgated by the American Institute of Certified Public Accountants- The AICPA Statement on Auditing Standards 99 (SAS 99) supersedes the Auditing Standards Board’s earlier fraud standard, Statement on Auditing Standards 82. The key provisions of SAS 99 include:

- **Increased Emphasis on Professional Skepticism.** Putting aside any prior beliefs as to management’s honesty, members of the audit team must exchange ideas or brainstorm how frauds could occur in the area under audit. These discussions are intended to identify fraud risks and should be conducted while keeping in mind the characteristics that are present when frauds occur: incentives, opportunities, and ability to rationalize. Throughout the audit, the engagement team should think about and explore the question, “If someone wanted to perpetrate a fraud in this area, how would it be done?” From these discussions, the engagement team should be in a better position to design audit tests that are responsive to the risks of fraud.
- **Discussions with Management.** The engagement team is expected to inquire of management and others in the organization as to the risk of fraud and specifically whether they are aware of any frauds or potential for fraud. The IA should make a point of talking to employees in and outside management, present employees as well as employees that are no longer working for the organization. Giving employees and others the opportunity to “blow the whistle” may encourage someone to step forward and advise the auditors as to whether fraud may have occurred. It might also help deter others from committing fraud if they are concerned that a co-worker will turn them in.
- **Unpredictable Audit Tests.** During an audit, the engagement team should test areas, locations and accounts that otherwise might not be tested. The team should design tests that would be unpredictable and unexpected by the auditee. The audit team should not discuss these audit procedures with anyone outside the audit team.

- **Responding to Management Override of Controls.** Because management is often in a position to override controls in order to commit fraud, a test of management override of internal controls must be a part of every audit.
- Standards promulgated by the International Federation of Accountants- International Standards on Auditing, ISA 240, provides explicit guidance regarding the auditor's responsibility to consider the probability of fraud and error when planning and performing an audit.

III.3. Why Auditors Do Not Detect More Fraud

Some studies show that only about 18 percent of all fraud cases are discovered as a result of audit initiatives. Some of the reasons why auditors do not discover more fraud include:

- Lack of audit skills.
- No experience, skill, or training in fraud awareness, detection, or investigation.
- The failure to include fraud detection when planning audits.
- Lack of an awareness of the probabilities of fraud occurring in the area being audited.
- Unaware of the implications of red flags and other fraud indicators.
- Failure to follow up on fraud symptoms and indicators.

IAs must become more effective in detecting possible fraud and thus to help deter its continued occurrence. Accordingly, each auditor must understand the auditor's responsibilities in this important area, know how those responsibilities are to be carried out, and technically and professionally prepare to implement those responsibilities.

III.4. Incorporating Fraud Detection Into the Audit Program

In accordance with all relevant audit standards, all internal audits must be planned to already include audit procedures that would anticipate and provide a reasonable expectation of detecting possible fraud and other irregularities if they exist. To plan, execute and report the results of audits, IAs must:

- Develop an awareness of the characteristics and types of potential irregularities, and fraud, associated with the area being audited.
- Be aware of all the pertinent laws and regulations that apply to the area under audit.
- Prepare and execute a risk assessment scheme, incorporating factors including weaknesses in controls, which suggest fraud vulnerability for use during the planning process to help assess the potential for fraud in areas to be audited.
- Develop audit steps which focus on determining whether fraud may be occurring or may have occurred in vulnerable areas.
- Exercise due professional care in executing those audit steps so as not to jeopardize a future investigation or prosecution, and
- Plan to report the results of those audit steps, which may include possible fraud, in accordance with internal audit policies and procedures.

In order to avoid conflict of interest, management should ideally establish an independent group within the IAS/IAU that would focus on internal fraud detection and prevention. If and when such a separate fraud unit is instituted, the relationship between this group and internal audit should be formally defined and lines of communication and cooperation established (See Chapter I, Section 2 above.).

IAs should arrange with management to be informed of all suspected or detected fraud. This enables the IA to evaluate the implications of the suspected fraud on management's risk management, internal control, and governance systems. Recommendations to management regarding any needed improvement in any of these systems, and whether there is a need for further investigation is within the scope of internal audit's responsibilities.

Audit procedures, even when performed with the utmost of due professional care, cannot totally assure that existing fraud will be detected. In spite of that, IAs are required to be proactive during all aspects of their work in recognizing signs of risks and exposures that could permit fraud to occur and to indications that fraud may have taken place.

CHAPTER II. FRAUD

I. MEANING AND CONCEPT OF FRAUD

The term fraud is generally used to encompass such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts, and collusion. For all practical purposes fraud is a corrupt act. It uses deception with the intention of obtaining an advantage, avoiding an obligation, or causing loss to another party.

I.1. Fraud Definitions and Characteristics

COA Memorandum No. 93-813, dated July 9, 1993, defines fraud as follows: “Fraud is deemed to comprise anything calculated to deceive, including all acts, omissions, and concealment involving a breach of legal or equitable duty, trust, or confidence justly reposed, resulting in damage to another, or by which an undue and unconscionable advantage is taken of another. Fraud indicates that there has been disclosure or detection of deceit, abuse, wastage or illegal act that has resulted in loss or damage to public funds and properties. Consequently, there has been a violation of law, rule or regulation.”

On the other hand, the IIA defines Fraud as illegal acts characterized by deceit, concealment or violation of trust. These acts are not dependent upon the application of threat of violence or of physical force. Frauds are perpetrated by parties and organizations to obtain money, property or services; to avoid payment or loss of services; or to secure personal or business advantage.

Hence, fraud encompasses an array of irregularities and illegal acts, specifically characterized by intentional deception and usually always involves the deliberate concealment of facts. Fraud can be described in a number of ways:

- The intentional misrepresentation or concealment of a material fact that results in financial or other damages to another party.
- The use of deception, false suggestions, suppression of the truth, or other unfair means, which is believed and relied upon to deprive another of property or money, resulting in a loss to the party that believed and relied upon the deception.
- An illegal act characterized by deceit, concealment or violation of trust committed by individuals or organizations to obtain money, property or services, avoid payment or loss of services, or to secure personal or business advantage.
- The intentional deception perpetrated by individuals or organizations, either internal or external to the organization, which could benefit themselves, others, or the organization or which could cause detriment to others or the organization, including falsifying financial or other records to cover up the theft of money or other assets.

I.2. Characteristics Common to All Fraud

Regardless of the definition used, the following characteristics are common to virtually all fraud:

- Misrepresentation of a material fact,
- Made knowingly and with the intent to deceive,
- Reliance by the victim on the misrepresentation, and
- Resulting in injury or damage from such reliance.

II. CORRUPTION AS A CATEGORY OF FRAUD

There are many different types of fraud. It is useful to categorize these types into groups to provide an overview of the wide range of investigations that could be carried out. The category of fraud which is of current concern to the Philippine government is corruption.

The variety of ways in which corruption is committed is limited only by the creativity of dishonest public officers. It is, therefore, important not only for an anti-graft investigator or a public prosecutor, but also for an IA (in order to assist the forensic auditing process), to be able to identify the specific offense or offenses committed in these imaginative schemes, as well as their respective elements, to build a case for either an administrative litigation or a criminal action. These are:

- Malversation of Public Funds and Property penalized under Chapter 4, Title 7, Book II of the Revised Penal Code²;
- Bribery, penalized under Section 2, Chapter 2, Title 7, Book II of the RPC;
- Sections 3(e) and 3(g) of Republic Act³ No. 3019, as amended, otherwise known as the Anti-Graft and Corrupt Practices Act;
- Plunder as defined and penalized under R.A. No. 7080; and
- Falsification of Public Documents under Article 171, RPC.

Corruption also relates to the violation of the requirements under Section 7 of R.A. 3019 and Section 8 of R.A. 6713, as amended, otherwise known as Code of Conduct and Ethical Standards for Public Officials and Employees, in relation to R.A. 1379. To reiterate, the IA should be familiar with these offenses, as well as their elements in order to know the kind of evidence that she should look out for, and how to gather and preserve the same for purposes of presenting them as evidence before the appropriate administrative tribunal or trial court.

III.1. Common Corruption Offenses

II.1.1. MALVERSATION

II.1.1.1. Malversation of Public Funds or Property (Article 217, RPC)

I. Elements of Malversation under Article 217 of the RPC

a. Public Officer

Aside from public officers defined under Art. 203, private persons who, in any capacity, have custody of public funds or property, can be liable for malversation and the related felonies, even if the funds or property belong to a private person.⁴

b. Accountable

Article 217 requires that only an “accountable” public officer (i.e., one who has custody or control of public funds or property by reason of the duties of his or her office), can be liable

² “RPC.”

³ “R.A.”

⁴ Article 222, RPC.

for malversation. A public officer who takes public funds or property of which he or she is not the custodian or for which he or she is not accountable, commits theft, robbery or *estafa*, depending upon the manner of the taking. The nature of the duties performed by the defendant is determinative of such accountability. The title or designation of the office or the fact that the official is not bonded is not determinative.⁵

c. Public Funds or Property

“*Public funds or property*” includes all money and property owned or held by the State. It may also include money or property that, while private in origin or ownership, is vested with public interest. This will include money or property in *custodia legis* (i.e. those that have been seized or held by virtue of a writ of attachment or a search warrant properly issued by a court), or those lawfully seized without warrant.

Funds that, although private in origin, are collected through statutorily enforced contributions, intended for the use of the public (or a considerable portion thereof), are in the nature of a tax and vested with public interest, and should, therefore, be considered public funds and may be the object of a charge for *malversation*.

d. Official Custody or Control

The public officer must have custody or control of the funds or property by reason of the functions of his office. A distinction must, therefore, be made between property that is in custodial *legis* and property that is merely in custody. The former implies dominance and supremacy of the law over private rights to the funds or property, often by virtue of a legal or judicial order; whereas the latter connotes mere physical possession unaccompanied by any authority, such as for temporary safekeeping.

e. Appropriate, take or misappropriate, or allow others to take funds or property, with consent or through negligence

The following are not elements of malversation:

- Demand
- Damage

2. Presumption of Misappropriation

Direct evidence of misappropriation is not necessary to convict a public officer for malversation. In its place, the law raises a presumption of misappropriation of public funds or property from the offender’s failure to present or account for the same upon proper demand.

II.1.1.2. Illegal Use of Public Funds (Article 220, RPC); Elements

- a. Use of public funds or property;
- b. For public purpose; and
- c. Purpose is different from that for which the money is appropriated or property intended

This is commonly referred to as “technical malversation”. A common example is when funds budgeted for a particular purpose are used for another purpose (e.g., funds released for capital expenditure are used to pay for consultants’ fees).

II.1.1.3. Failure to Render Accounts (Article 218, RPC); Elements

- a. Public officer;
- b. In service or separated by resignation or other cause;
- c. Legally required to render an account to the proper officer; and
- d. Fails to do so within 2 months from the time required to do so.

⁵ Quiñon vs. People, G.R. No. 136462, September 19, 2002.

II.1.1.4. Failure to Render Accounts before Leaving the Country (Article 219, RPC); Elements

- a. Public officer; and
- b. Unlawfully leaves or attempts to leave the country without a certification clearing him of accountability.

The rationale for this article is the same as Article 218.

II.1.1.5. Failure to Deliver Public Funds or Property (Article 221, RPC); Elements

- a. Public officer;
- b. Legally required to pay money or deliver property; and
- c. Unjustifiably fails or refuses to make such payment or deliver

II.1.2. BRIBERY. KINDS OF BRIBERY UNDER THE RPC

II.1.2.1. Direct Bribery (Article 210); Elements

1. Who can be liable

- a. Public officers, as defined under Article 203, RPC; or
- b. Private persons performing public duties

2. What “bribe” may consist of

- a. Money, gift, and offer or promise of money or a gift; and
- b. That is of value or otherwise capable of pecuniary estimation.

3. What constitutes a bribe depends upon the type of bribery

- a. For Direct Bribery -- in order to perform an act constituting a crime or to refrain from doing official duty, the bribe may consist of either an offer, promise, gift or present.
- b. For Direct Bribery -- in consideration of performing an act not constituting a crime, the bribe must consist of a gift or present, an offer or promise not being sufficient.
- c. For Qualified Bribery -- the bribe may consist of an offer, promise, gift or present.
- d. For Indirect bribery -- the bribe must consist of a gift or present.

4. How offender receives the bribe

- a. He accepts or receives the bribe by himself or through another;
- b. Physical possession of the bribe money, unaccompanied by any other act or circumstance, is not sufficient to prove that the offender “accepted or received” the bribe.

5. Why s/he accepts a bribe

- a. To commit a crime related to his or her duties:
 - Must be in relation to his or her duties;
 - Mere promise to perform the crime is sufficient;
 - Mere acceptance of the offer or promise is sufficient; and
 - If the crime is committed, impose penalty for the crime in addition to that for bribery
- b. To do an act that is not a crime but is related to duties:
 - Must be money or gift, not a mere offer or promise;
 - Offender must receive the money or gift; and
 - Offender must take steps towards the execution of the act, not merely agree to take said steps.

- c. To fail to perform official duty:
 - Bribe may be a gift or promise; and
 - The failure to perform official duty must not be a crime by omission.

II.1.2.2. Indirect Bribery (Article 211, RPC)

1. Elements

- a. Public officer;
- b. Accepts gift; and
- c. Offered by reason of his office.

2. Rationale for Indirect Bribery

- a. Fallback position for direct bribery:
 - In case of insufficient evidence; and
 - In case of failure to prove direct bribery.
- b. Easier to prove: Need not prove consideration for the bribe.

II.1.2.3. Qualified Bribery (Article 211-A, RPC); Elements

- a. Law enforcement officer;
- b. Refrains from arresting or prosecuting an offender who has committed a crime punishable by *reclusion perpetua* and/or death;
- c. because of an offer, promise or gift.

II.1.2.4. Corruption of Public Officials (Article 212, RPC); Elements

- a. Offender offers/promises or gives gift to public officer; and
- b. Under circumstances that would make public officer liable for direct or indirect bribery

II.1.3. ANTI-GRAFT AND CORRUPT PRACTICES ACT (R.A. NO. 3019)

II.1.3.1. Paragraph 3(e); Elements

- a. Public officer;
- b. In relation to the discharge of administrative, judicial, or official duties;
- c. Causes or gives:
 - Undue injury
 - Unwarranted benefit, advantage, or preference
- d. Through:
 - Manifest partiality
 - Evident bad faith
 - Gross inexcusable negligence
 - In general

(a) These three phrases merely describe the different modes by which Section 3(e) may be committed, and the use of all three in the same information does not mean that the information charges three distinct offenses⁶;

(b) “Partiality”, “bad faith”, or “negligence” is not enough. Partiality must be manifest, Bad faith must be evident, and the negligent act must be gross and inexcusable⁷;

⁶ Gallego vs. Sandiganbayan, G.R. No. L-57841, 30 July 1982.

⁷ Sistoza vs. Desierto, G.R. No. 144784, September 3, 2002.

- (c) “Urgency” may be a justification for acts otherwise culpable⁸;
- (d) There can be neither evident bad faith nor gross inexcusable negligence where the defendant acted in accordance with the *prevailing regulations*. Defendant cannot be faulted should such regulations be subsequently changed⁹; and
- (e) Prescription -- Offenses under R.A. 3019 prescribe in 15 years. If the violation is unknown at the time of commission, prescription begins to run from discovery of the constitutive acts.¹⁰

II.1.3.2. Paragraph 3(g), R.A. No. 3019; Elements

- a. Public officer
- b. Enters into a contract or transaction on behalf of the government
- c. Grossly disadvantageous

II.1.4. PLUNDER

1. Elements

- a. Amass, accumulate, or acquire:
 - By himself;
 - In connivance with other.
- b. Ill-gotten wealth of at least P50M;
- c. Through a combination or series:
 - “Combination” refers to at least two acts falling under different categories of the enumeration of overt and criminal acts under Section 1(d); and
 - “Series” requires two or more overt or criminal acts falling under the same category in the enumeration under Section 1(d).
- d. Overt or criminal acts
 - Misappropriation, conversion, misuse or malversation of public funds or raids on the public treasury;
 - Receiving, directly or indirectly, any commission, gift, share, percentage, kickbacks or any other form of pecuniary benefit from any person and/or entity in connection with any government contract or project or by reason of his or her office or position;
 - Illegal or fraudulent conveyance or disposition of assets of the government;
 - Obtaining, receiving, or accepting, directly or indirectly, any shares of stock, equity, or any other form of interest or participation, including the promise of future employment in any business enterprise or undertaking;
 - Establishing any agricultural, industrial, or commercial monopolies or other combinations and/or implementation of any orders and decrees intended to benefit particular persons or special interests; and
 - Taking undue advantage of official position, authority, relationship, connection or influence to unjustly enrich himself or themselves at the expense and to the damage and prejudice of the Filipino people and the country.¹¹

2. Evidence

It is not necessary to prove each and every criminal act done to amass, accumulate or acquire the ill-gotten wealth; it is sufficient to establish a pattern of overt or criminal acts indicative of the over-all scheme or conspiracy.¹²

⁸ Baylon vs. Ombudsman & Sandiganbayan, G.R. No. 142738, December 14, 2001.

⁹ Garcia vs. Ombudsman, G.R. No. 127710, February 16, 2000).

¹⁰ Domingo vs. Sandiganbayan, G.R. No. 109376, January 20, 2000.

¹¹ Section 4, R.A. 7080.

¹² Id.

Pattern consists of at least a combination or series of the overt or criminal acts enumerated in Section 1(d) that show a conspiracy or scheme that is directed towards the same purpose or goal, which is to amass, accumulate, or acquire ill-gotten wealth.

“Pattern” is not an element of the offense, but rather a procedural rule for proving plunder.¹³

II.1.5. FALSIFICATION OF PUBLIC DOCUMENTS (ARTICLE 171, RPC)

1. Elements

- a. Public officer
 - includes a notary public with respect to notarized documents and registers; and
 - includes an ecclesiastical minister, with respect to records and registers affecting a person’s civil status (i.e., marriage and baptismal records);
- b. Commits any of the acts enumerated in Article 171;
- c. Upon a “document”
- d. By taking advantage of his or her office.

2. Ways of Committing Falsification

- a. Counterfeiting or imitating any handwriting, signature or rubric.
- b. Causing it to appear that persons have participated in any act or proceeding when they did not in fact so participate.
- c. Attributing to persons who have participated in an act or proceeding statements other than those in fact made by them.
- d. Making untruthful statements in a narration of facts.
- e. Altering true dates.
- f. Making any alteration or intercalation (i.e. insertion) in a genuine document which changes its meaning.
- g. Issuing in authenticated form a document purporting to be a copy of an original document when no such original exists, or including in such copy a statement contrary to, or different from, that of the genuine original.
- h. Intercalating any instrument or note relative to the issuance thereof in a protocol, registry, or official book.

III.2. CIVIL FORFEITURE OF ILL-GOTTEN WEALTH

There are two possible forms of civil forfeiture proceedings, one under R.A. No. 1379 and another under Supreme Court A.M. No. 05-11-04-SC.

II.2.1. R.A. No. 1379

- a. Requirements for a prima facie case:
 - Acquisition of property;
 - During incumbency; and
 - Manifestly out of proportion to lawful income.
- b. Requirements for forfeiture:
 - Failure of respondent to prove lawful acquisition

¹³ Estrada vs. Sandiganbayan, G.R. No. 148560, November 19, 2001.

II.2.2. Supreme Court A.M. No. 05-11-04-SC

Applies to proceedings for the civil forfeiture, asset preservation, and freezing of monetary instruments, properties, or proceeds representing, involving, or relating to a money laundering offense under R.A. No. 9160.

II.2.3. Civil Forfeiture for Non-Filing of Statements of Assets Liabilities and Net Worth under R.A. 3019 and R.A. 6713

An incumbent public officer or employee's failure or omission to include in his statement of assets and liabilities, and net worth¹⁴ property which is manifestly out of proportion to his salary and to his other lawful income and the income from legitimately acquired property, may give cause to his prosecution under R.A. No. 1379, for harboring unexplained wealth.¹⁵ The SALN must be accomplished as truthfully, as detailed and as accurately as possible.¹⁶ Repeated and consistent failure to reflect truthfully and adequately all assets and liabilities in the SALN may be deemed an act of dishonesty and lead to dismissal from government service.¹⁷ Every asset acquired by a civil servant must be declared in the SALN. In one case, the Supreme Court had occasion to say that even if a motor vehicle was acquired through chattel mortgage, it is a government employee's ethical and legal obligation to declare and include the same in his SALN.¹⁸ On the other hand, the non-filing of the SALN, or improper filing thereof, by a public official may lead to a finding of gross misconduct and dishonesty for violation of Section 7 of R.A. 3019 and R.A. 6713.¹⁹ The Supreme Court explained that for gross misconduct to exist, there must be reliable evidence showing that the acts complained of were corrupt or inspired by an intention to violate the law, or were in persistent disregard of well-known legal rules.²⁰ As for dishonesty, it is committed by intentionally making a false statement in any material fact, or practicing or attempting to practice any deception or fraud. Dishonesty is understood to imply a disposition to lie, cheat, deceive, or defraud; untrustworthiness; and lack of integrity.²¹ Hence, the Supreme Court relieved a public official from liability for gross misconduct and dishonesty for not properly completing his SALN considering that he made a candid admission of his shortcomings in properly and completely filling out his SALN. The Supreme Court also found noteworthy the public official's endeavor to clarify the entries in his SALN, to provide all other necessary information, and his submission of supporting documents. These were deemed by the Supreme Court to negate any intention on the part of the public official to conceal his properties. The Court also stated that intent is an essential element of gross misconduct and dishonesty.²²

III.3. Factors That Influence Decisions To Commit Fraud

There are many factors that may be present in the audit environment that may influence a person's choice to commit fraud or engage in fraudulent behavior. Knowing, understanding,

¹⁴ Hereafter, "SALN".

¹⁵ Ombudsman and CIR vs. Peliño. G.R. No. 179261. April 18, 2008. Sections 8 and 9, R.A. 3019, as amended.

¹⁶ Flores vs. Montemayor. G.R. No. 170146. August 25, 2010.

¹⁷ Id.

¹⁸ Id.

¹⁹ Salvador A. Pleyto vs. PNP-CIDG. G.R. No. 169982. November 23, 2007. See also The Ombudsman, Fact-Finding and Intelligence Bureau, Office of the Ombudsman, and Preliminary Investigation and Administrative Adjudication Bureau, Office of the Ombudsman vs. Nestor S. Valeroso. G.R. No. 167828. April 2, 2007; and Ombudsman and CIR vs. Peliño. G.R. No. 179261. April 18, 2008.

²⁰ Salvador A. Pleyto vs. PNP-CIDG. G.R. No. 169982. November 23, 2007.

²¹ Id.

²² Id.

and recognizing these factors, if they exist in the audit environment, can help IAs better carry out their responsibilities. Being aware of these factors will assist the IA in developing a risk assessment scheme during audit planning that encompasses these vulnerable-to-fraud factors and help the auditor detect possible fraud if it exists.

1. Work environment influences
 - a. Opportunity
 - Poor internal controls
 - Remote locations
 - Lack of monitoring and review
 - Political influences
 - Motivational influences
 - b. Pressures and stress
 - Organizational pressures
 - Stress of personal problems
 - Probability of gain
 - Likelihood of possible discovery
 - Nature of possible punishment

2. Attitudinal influences: Personal and organizational
 - a. Inadequate reward system
 - b. Lack of management concern about fraud detection and prevention
 - c. Poor staff supervision
 - d. Inappropriate level of interpersonal trust

3. Organizational policies
 - a. No code of ethics
 - b. No fraud policies
 - c. Reliance on audit to detect and prevent fraud
 - d. Frequent management override of internal controls
 - e. Indifferent tone at the top towards fraud, waste, and abuse

4. Geographical considerations
 - a. Nature of the mission
 - b. Cultural implications
 - c. Multiple locations
 - d. Inadequate resources

5. Governance mechanism. Organizations with governance styles that are most vulnerable to fraud include those with:
 - a. Autocratic and centralized management.
 - b. Critical, negative performance feedback mechanisms.
 - c. A politically administered, monetary based reward system.
 - d. Short range, centralized planning systems.
 - e. Routine reporting systems.
 - f. Performance assessments predicated on short term, quantitative measures.
 - g. Rigid, strongly enforced rules.
 - h. Crisis managed.
 - i. Inadequate accounting systems.
 - j. Weak internal controls.

Each of the factors discussed above and others, individually, collectively, or in combination, suggest conditions that encourage fraud. Accordingly, when an audit team begins to plan or conduct an audit, or is otherwise engaged in an audit, it is important that the audit team be

alert to the existence of such factors in the environment. Being alert to the existence of such factors will tend to heighten the audit team's concern for the presence of potential fraud and guide their decisions so as to facilitate the detection of possible fraud if fraud is present.

A risk assessment, conducted as an adjunct to audit engagement planning should include risk-of-fraud components.

III.4. How Fraud Occurs

Generally there must be four basic elements present that are necessary for a fraud to occur. There must be:

1. Someone willing to carry out the fraud.
2. That someone may be within the organization, someone from outside the organization, or a group of people working together from both inside or outside the organization.
3. Assets or something of value that can be fraudulently acquired.
4. Fraud is generally motivated by the desire to obtain something of value such as money, property, or an advantage that one is not legally entitled to.
5. Intent to commit the fraud.
6. For fraud to take place there must be intent to commit fraud. Fraud cannot be committed accidentally or unknowingly, it is a deliberate act.
7. The opportunity to commit fraud must exist.

For fraud to be committed an individual or individuals must be in a position to commit that fraud, and must have access to the means to commit the fraud.

III.5. Exposure to Fraud

Any organization can be exposed to the risk of fraud in a number of different ways:

- Internal fraud
- External fraud
- Collusion

II.5.1. Internal Fraud

This fraud is perpetrated by individuals inside the organization. Staff that has access to easily converted assets like cash, property, or equipment most often carry out internal fraud. It is likely that the risk of fraud and its scale will increase if staff is able to conceal the irregularities by also having authorized or unauthorized access to accounting records. It may be opportunistic, perhaps due to the lack of strong internal controls, though such fraud can also be planned and carried out over a long period of time.

II.5.2. External Fraud

This fraud is perpetrated by individuals outside the organization and covers activities such as burglary, theft, deception and computer hacking by external parties. It is very often systemic and continuous, stemming from the inherent problem of safeguarding certain types of systems against attack, as well as the lack of security over organization assets.

Those doing business with the organization such as contractors and vendors, as well as those who transact other business with the organization may also perpetrate external fraud. Many types of external fraud can be attributed to internal control weaknesses.

II.5.3. Collusion

This type of fraud involves two or more parties working in concert, either from within the organization, or by parties from inside and outside the organization who are working together. As with most fraud, deficiencies in internal controls can contribute to the existence of this type of fraud.

Collusion generally facilitates the commission of a fraud. However, because of the number of people that may be involved, fraud that involves collusion, once detected may sometimes be readily investigated.

III. FRAUD DETECTION BY PHILIPPINE GOVERNMENT INTERNAL AUDITORS

The detection of probable fraud by IAs during the course of an audit results from the process of planning for the identification and exploration of all fraud-indicative symptoms until sufficient audit evidence is uncovered to establish that fraud may have been perpetrated or may be currently occurring, and further audit/investigation is deemed necessary.

There are two important characteristics of fraud that help in the recognition of the symptoms. Firstly, the commission of a fraud becomes an objective fact. Once perpetrated, the fraud and evidence of the fraud is exceedingly difficult to undo. Evidence of a fraud cannot be completely expunged. It is the auditor's responsibility therefore to recognize that evidence. Because evidence of possible fraud cannot be found is no assurance that fraud has not occurred.

Secondly, fraud is generally directed at achieving financial benefit. Consequently an incident of fraud is generally related to a weakness in financial or other controls. A weakness in control indicates to the auditor the potential for fraud. Conversely, the commission of a fraud almost always indicates a weakness in controls. (See discussion of internal controls under Chapter I).

When probable fraud is detected, there are almost always facilitating weaknesses in controls that must be corrected, whether or not potential fraud is ever adjudicated.

III.1. Recognizing Red Flags

There are many general fraud symptoms and indicators, called "Red Flags", that auditors must be alert for. These include:

- a. Poor internal controls.
- b. Management override of internal controls.
- c. Missing documentation.
- d. Inappropriate and incorrect bookkeeping and poorly maintained accounting records.
- e. Active or passive resistance to audit inquiries such as denying or delaying auditor access to records or to personnel,
- f. Shortages and overages in cash.
- g. Shortages and numerous adjustments to inventories.

In addition there are also very recognizable, very specific Red Flags or fraud indicators that exist in specific activities that may indicate to the auditor the possible presence of fraud. For example:

III.1.1. Procurement and Contracting

Billions of dollars are expended annually to purchase goods and services, and on capital improvements and construction. Because of the financial enormity of these expenditures, and the widely documented propensity for fraud in this area, it is essential that auditors recognize the indicators of fraud in procurement and contracting activities.

III.1.1.1. Common Procurement and Contracting Fraud Indicators

- a. Procurement of services, goods, or work projects not needed, or in excess of what may be required.
- b. Needs assessments for services, goods, or work projects that are not adequate or are not accurately developed.
- c. Requirements that justify continuing to contract with or buy from only certain contractors or vendors.
- d. Defining requirements so that only certain contractors or vendors can supply them.
- e. Unsuccessful bidders who become subcontractors, or goods and services suppliers.
- f. Contracting or purchasing from a single source without developing alternate sources of goods and services.
- g. Work statements or material specifications that appear to fit a favored or single contractor or vendor.
- h. Releasing procurement information to preferred or selected contractors or vendors.
- i. Consulting with preferred contractors and vendors about requirements and specifications.
- j. Designing pre-qualification standards, specifications or conditions to limit competition to preferred vendors or contractors.
- k. Splitting contract requirements to so that contractors and vendors can share or rotate bids and awards.
- l. Splitting procurement requirements to avoid procurement policies.
- m. Lost or misplaced vendor or contractor bid proposals and price quotations.
- n. Questionable disqualification of a contractor or vendor.
- o. Biased proposal evaluation criteria.
- p. Award of contract or purchase order to other than lowest responsible bidder.
- q. Material changes to the contract or purchase order after the award.
- r. Awards to contractors or vendors with a history of poor or questionable performance.
- s. Incorrect certification by the contractor or vendor as to the stage of contract completion or delivery of goods and services.
- t. The delivery of services or materials that do not conform to contract or purchase order requirements.
- u. Acceptance without verification of contractor or vendor certification of service and material quality.

IAs must make a conscious effort to determine whether these conditions exist in connection with any procurement that is selected for audit. The presence of any of the foregoing conditions should indicate to the IA that the potential for possible fraud is present.

III.1.2. Treasury/Cash Functions

Cash is the focal point of most entities. Virtually every transaction involves the transfer of cash into or out of an organization. In that regard and because of its liquid nature, cash transactions pose significant inherent risk and are highly susceptible to fraud. There are many ways to misappropriate cash.

III.1.2.1. Common Petty Cash Fraud Indicators

- a. Shortages/overages in petty cash funds.
- b. Forged, fictitious or unusual vouchers in the petty cash box.
- c. Numerous, receipts for hard to verify expenditures, like postage, and office supplies.
- d. Borrowing from petty cash supported by promissory notes.
- e. Cash advances.
- f. Lack of approval for petty cash disbursements.
- g. Dummy or altered receipts

III.1.2.2. Common Cash from Bank Account Fraud Indicators

- a. Ghosts on payroll.
- b. Missing paid checks.
- c. Checks payable to employees.
- d. Endorsements on checks that do not match other writing samples.
- e. Checks that have a second endorsement.
- f. Void checks.
- g. Cash collections not deposited in the bank.
- h. Conducting cash sales and failing to record the sales.
- i. Collecting a cash sale and recording only a part of the sale.
- j. Lapping and kiting.
- k. Receiving cash and only crediting an account for a part of the sale.
- l. Receiving/ recording cash, not depositing it, and calling it deposit in Transit.
- m. Removing money from a cash bank deposit and not explaining the shortage.

III.1.3. Assets/ Inventory

Assets/inventory are very common targets of fraud. Assets/inventory have value, can be sold or converted to cash, are useful even if not sold, and often are not adequately protected.

III.1.3.1. Common Assets and Inventory Fraud Indicators

- a. Personal items purchased and charged to an asset or inventory account.
- b. Disbursement schemes charged to assets or inventory, such as other fictitious costs paid or stolen by an employee.
- c. Vendor fraud in which the customer purchases assets or inventory from a vendor and the vendor diverts the shipment to another customer, to the employee, or kicks-back money to an employee.
- d. Manipulating asset and inventory counts and inventory and asset valuations.
- e. Inflating the data on actual thefts and shortages to cover in-house thefts.
- f. Inflating asset or inventory prices.
- g. Arranged cooperative thefts with inside/outside personnel.
- h. Overstating asset or inventory counts in number and value by manipulating counts and values.
- i. Declaring assets or inventory obsolete that is not obsolete, selling it, disposing of it, or converting it for one's own use.
- j. Failing to write-down, or delete from inventory obsolete asset or inventory items after declaring them obsolete so they continue to be counted.
- k. Stealing assets or inventory by placing them in a trash container.
- l. Purchasing outdated or already-obsolete assets or inventory.
- m. Mismatching sealed containers and boxes in storage or inventory as to quantity, quality.

III.1.4. Pension And Investment Fund Operations

Frauds in the management and administration of pension and investment funds may occur in two basic ways:

- a. Poor investments tied to self-dealing or commercial bribery.

- b. Embezzlement or the conversion to one's own use or benefit the money or property of another, over which one exerts a fiduciary control.

Trustees, fund employees, employers and outsiders, may all commit this type of fraud.

III.1.5.1. Common Pension and Investment Fund Fraud Indicators

Embezzlement or the conversion to one's own use or benefit the money or property of another, over which one exerts a fiduciary control, is often evidenced by:

- a. Inadequate, incomplete, inaccurate records of, and support for transactions.
- b. The use, sale, compromise of insider and confidential information.
- c. Less than prompt communications to oversight committees, and trustees.
- d. Benefits paid to dead or otherwise ineligible beneficiaries.
- e. Unusual number of changes made to beneficiary records, including changes in addresses, amounts, and benefit computations.
- f. Signatures on benefits checks that do not match other signature samples.
- g. Multiple and unapproved changes to beneficiaries' survivor authorizations.
- h. Errors in computations made to beneficiary accounts.
- i. Complaints by beneficiaries about payments, including late payments, incorrect payments, and payments not received.
- j. Failure to reconcile balances in control accounts.

Poor investments tied to self-dealing or commercial bribery are sometimes evidenced by:

- a. Pension or investment fund personnel maintaining less than arms' length relationships with outside investment advisors and security representatives.
- b. Personal investments by pension or investment fund personnel that parallel investments made on behalf of the organization.
- c. Unqualified investment advisors, security representatives, and inept, inexperienced financial services providers.
- d. Gifts entertainment and favors from outside advisors and security representatives to pension or investment fund personnel.
- e. Privacy and confidentiality breaches connected with pension or investment fund personnel.
- f. Churning of investments, high portfolio turnover.
- g. Pension or investment fund performance that appears contrary to reliable market indicators.
- h. Failure to provide detailed, decision-critical information to pension or investment fund personnel by outside advisors and security representatives.

III.1.5. Travel Expenses

Organizations spend little time reviewing travel expenses because of the seemingly insignificant value of each item. But small infractions can add up to thousands - and ultimately millions of pesos in large organizations. According to a recent survey, respondents indicated that travel and entertainment fraud was the third greatest controllable cost in their organizations. A company can become riddled with fraud and abuse if employees believe that the top executives consider it acceptable.

Additionally, quite often travel fraud and abuse can be an indicator of much larger problems such as bribery and kickback schemes and serious conflicts of interest cases. Fraudulent travel reimbursement claims are often used to disguise or hide bribes and kickbacks. A fraudulently prepared travel reimbursement claim can be used to recover the expense incurred in buying a gift, or paying a cash bribe or a kickback.

III.1.5.1. Common Travel Fraud Indicators

- a. Falsified, altered, unusual receipts.

- b. Inflated expense amounts.
- c. Dummy receipts claiming fictitious expenditures.
- d. Unnecessary, unauthorized, unapproved travel.
- e. Claiming days of travel that were not traveled.
- f. Double-claimed expenditures.
- g. Mischaracterized expenses, for example claiming personal expenditures as business expenses.
- h. Failing to provide required documentation.
- i. Travel expenses claims that are not reviewed.
- j. Overstated expenses.

III.1.6. Fraud in a Computerized Environment

93 per cent of 503 companies recently surveyed in the United States indicated detecting security breaches in a 12-month period with 80 per cent of the companies suffering financial losses. According to another survey, 44 per cent of the companies that responded to a survey reported losses totaling almost one-half billion dollars.

The number of ways in which fraud in the computer environment is committed, is matched only by the number of ways in which systems are used, the number of systems users, and the numbers of cyber criminals. The following are fraud implications of computer technology and its related vulnerabilities:

- a. Data concentration
- b. Accessibility of storage medium
- c. Obscure audit trail
- d. Visibility of records
- e. Alteration of programs and data
- f. Tampering
- g. Networks
- h. Lack of understanding of computer systems and it technology.
- i. Inadequate security features.
- j. Lack of internal controls
- k. Circumvention of controls

III.1.6.1. Common Computer Area Fraud Indicators

- a. Missing computers, and other related assets, programs, and data.
- b. Use of computer time by employees and former employees for personal reasons.
- c. Changed or altered data by employees.
- d. Counterfeited data.
- e. Changed programs without committee approval.
- f. Altered or deleted master files.
- g. Override of internal controls.
- h. Evidence of Sabotage.
- i. Surveillance of data by unauthorized personnel.
- j. Hacking by personnel and outsiders.

While all these Red Flags may reflect the presence of possible fraud, at the same time they more than likely also indicate a condition, a deficiency that requires corrective attention by management.

III.2. Responding To the Existence of Red Flags

The presence of a Red Flag during the survey or planning stages of an audit, or while the audit is underway, requires the auditor to acknowledge its presence by recording and

documenting it. Then the auditor must develop and perform appropriate audit procedures to assess its significance and potential for evidence of probable fraud and any management weaknesses that must be corrected.

It should be remembered that all Red Flags are indicators and symptoms. And while they are not prima facie evidence of fraud, they must be:

- a. Assessed no matter how small they appear, and
- b. Carefully considered in planning and executing an audit.

III.3. Reacting to Allegations

In addition to Red Flags, allegations and anonymous tips can be a good source of leads to uncover the potential for fraud. Studies show that about 26 percent of all fraud cases result from tips or information received from employees.

While most allegations and anonymous tips do not result in uncovering potential fraud, the reasons they don't can vary. Many allegations and anonymous tips are unfounded, that is they are not based on good and sufficient information, or are based on erroneous, and incorrect information. Many of these allegations and anonymous tips however, might otherwise result in uncovering possible fraud but because they are ignored and not investigated or are improperly investigated, are never uncovered.

Therefore, it is important for IAs to remember the following when considering allegations and tips:

- a. Those making allegations usually do not know what facts and details are important to the IA and what are not, and so those making allegations usually never completely disclose all they really know.
- b. It is up to the IA or investigator when interviewing those making allegations to ask for:
 - All the details,
 - All the pertinent facts,
 - Copies of all relevant documents,
 - Names, addresses, and telephone numbers of all others that may have information regarding the allegation,
 - And any other information deemed essential to assessing the allegation.

Someone who makes an allegation can be a valuable source of important information to the IA in a possible fraud case and should be treated as a valuable asset.

As regards anonymous tips, before dismissing them as unfounded for lack of detail, the auditor or investigator should engage in discrete testing, checking, confirming, and following up on whatever information is included in the anonymous tip. In addition the auditor must also assess any information that eventually materializes from that work.

III.4. When Positive Fraud Indicators Are Identified

IAs are responsible for:

1. Someone willing to carry out the fraud.

That someone may be within the organization, someone from outside the organization, or a group of people working together from both inside or outside the organization.

2. Assets or something of value that can be fraudulently acquired.

Fraud is generally motivated by the desire to obtain something of value such as money, property, or an advantage that one is not legally entitled to.

3. Intent to commit the fraud.

For fraud to take place there must be intent to commit fraud. Fraud cannot be committed accidentally or unknowingly, it is a deliberate act.

4. The opportunity to commit fraud must exist.

When IAs ascertain that the indicators reflect the potential for the existence of possible fraud, extended audit steps and procedures must be incorporated into the audit program that will guide the collection and documentation of evidence. That evidence will ultimately allow conclusions to be drawn as to whether the *probability* of fraud exists, and whether a recommendation is appropriate that a referral to the appropriate investigative body is warranted for purposes of further investigation. Appropriate investigative bodies include an internal fraud unit or the COA's Fraud Audit and Investigation Office²³; or the filing of an administrative and/or criminal case – such as the Office of the Ombudsman²⁴; or other appropriate government agency.²⁵

When indicators reflect the potential for the existence of possible fraud, a plan of action should be developed and an auditor/investigator designated as specifically responsible for inquiring into the identified indicator to determine whether probable fraud has occurred, or may currently be taking place. It is especially important to plan and initiate audit steps as soon as possible to prevent the destruction or alteration of records, to conduct interviews while details are fresh in a potential interviewee's minds, and to gather all available evidence to demonstrate the *probability* of fraud having occurred.

The IA should be always mindful of the fact that the audit evidence collected may eventually be used for subsequent legal action and may be eventually presented to the court. Therefore, the collection of evidence and all audit work must be performed in strict accordance with prevailing audit standards. Care must be taken by the auditor to avoid jeopardizing future investigative or judicial actions.

III.5. Demonstrating the Probability of Fraud

When the fraud indicators are pursued, audit evidence must be collected by the IAs to determine whether or not the probability of fraud exists and whether the case should be referred to the appropriate agency for further investigation and prosecution.

A preponderance of evidence is the kind of evidence required to support an administrative or civil charge (which charge should, nonetheless, be proven by substantial evidence). Generally, evidence collected in accordance with relevant audit standards that is sufficient to

²³ One of the offices under the Legal Services Sector of COA is the FAIO. It has two principal divisions, the (a) Fraud Audit Investigation Division ("FAID"); and (b) the Administrative Investigation Division. The FAID is divided into the National, Local and Corporate audit services. Each of these services is headed by a Service Chief. Under COA Resolution No. 2008-12 dated October 10, 2008, each of the FAID services are mandated to: (a) evaluate requests for fraud audit; (b) conduct fraud audit; (c) prepare fraud audit reports, issue notices of disallowance ("ND") or notices of charges ("NC"); (d) institute appropriate cases based on fraud audit reports; (e) act on appeals from ND / NC; and (f) perform other assigned tasks.

²⁴ Please see Section 21 of R.A. 6770, also known as The Ombudsman Act and OMB Administrative Order No. 7, as amended.

²⁵ The growing trend in administrative regulation is for the agency concerned to adopt its own administrative investigation, adjudication and disciplinary rules and measures.

support an audit conclusion of probable fraud and convince an independent, reasonable person that fraud may have occurred, is considered adequate for a referral. A preponderance of evidence is considered sufficient to support an *audit conclusion* (as opposed to an administrative finding of liability) of probable fraud. It is that amount of relevant evidence which a reasonable mind might accept as adequate to justify a conclusion.

In civil cases, the quantum of proof required is preponderance of evidence. This refers to evidence which is of greater weight, or more convincing than that which is offered in opposition to it; at the bottom, it means that the party bearing the burden of proof must persuade the court “that the existence of the contested fact is more probable than its non-existence.”²⁶

On the other hand, to meet the standards of criminal prosecution, the evidence gathered should establish evidence that proves a criminal act beyond reasonable doubt. Proof beyond reasonable doubt does not mean such a degree of proof as, excluding possibility of error, produces absolute certainty. Only moral certainty is required, or that degree of proof which produces conviction in an unprejudiced mind (See discussion under Chapter IV).

²⁶ McCormick on Evidence (3rd ed., 1984).

CHAPTER III. FORENSIC AUDITING

I. MEANING AND SCOPE OF FORENSIC AUDITING

Forensic auditing is the application of accounting and auditing methods and techniques, other investigative skills, and a knowledge of the law to track and collect forensic evidence, that is, evidence that is admissible in a court of law, usually for the investigation and the prosecution of a criminal act.

Forensic auditing is distinguished from statutory auditing in that forensic auditing:

- a. seeks to determine the correctness of accounts or whether any fraud has actually taken place
- b. involves analysis of past trend and substantive or “in-depth” checking of selected transactions
- c. is not limited in scope of examination to a particular accounting or fiscal period
- d. involves the verification of suspected items independent of management

Forensic audit evidence is evidence collected by an auditor or investigator during the course of an investigation that will be used in an administrative tribunal or court of law or other proceeding to demonstrate that a law, a contract term, or other covenant has been violated.

Audit evidence is also used in a court of law. However, the primary purpose of audit evidence is only to support the auditor’s conclusions, in the case of fraud, a conclusion that probable fraud may exist, and whatever is contained in the reports an auditor may issue.

II. WHEN DOES THE AUDIT STOP AND A FORENSIC AUDIT/INVESTIGATION BEGIN?

Auditors are required to only employ those audit steps and procedures that will permit them to recognize the possibility of fraud, and collect sufficient, relevant, and reasonable evidence to support the work performed and the audit conclusion reached that probable fraud may have occurred.

Once the auditor has demonstrated and concluded that probable fraud may have occurred, a referral to an appropriate judicial or investigative body for follow up is generally warranted.

Accordingly, when an auditor has concluded as to the probability that fraud may have occurred and has documented that conclusion with sufficient audit evidence -- a preponderance of evidence -- the finding of probable fraud must then be quickly and systematically processed through IA management (i.e., the HoA) for review, discussion, and decision.

IA management, depending on the evidence presented, has a range of options. Prevailing law, regulation, or other related policies might require IA management to report indications of certain types of fraud, illegal acts, and violations of law to an investigative body or law enforcement immediately upon disclosure. In some cases, it may be appropriate for the IAs to work with investigators and/or legal authorities, or to withdraw from, or defer further work on the audit, or a portion of it to avoid interfering with the investigation or legal proceedings.

For example, IA management may direct the auditor to:

- Prepare the case for referral to an investigative unit or other judicial body.

- Collect more evidence of possible fraud, the evidence collected is not convincing.
- Discontinue the audit work and await further instructions.
- Complete the audit work as planned and await further instructions.
- Prepare to support investigative initiatives.

IA management has the final responsibility and authority for communicating a finding of probable fraud to either the audited entity, to other competent investigative or judicial authorities, or to both in accordance with legal and administrative protocols. IA management should be committed to cooperate with all government entities, and all investigative, law enforcement, and prosecutorial organizations. In all cases of suspected probable fraud, IAs must follow the instructions of IA management in relation to cooperation with the entity and/or other competent investigative or judicial authorities.

IT IS IMPERATIVE THAT INTERFERENCE WITH INVESTIGATIONS OR LEGAL PROCEEDINGS BE AVOIDED.

It becomes important, as soon as a conclusion of probable fraud is reached, that the auditor exercise due professional care and take no action that might possibly interfere with or prejudice a future investigation, legal processes, or other judicial or court proceeding. Significantly, continuing to collect evidence after concluding that probable fraud has occurred could:

- Result in the collection of evidence that cannot be used in a court of law because it was not collected in accordance with legal protocols established for the collection of forensic evidence.
- Alert those involved that fraud is suspected.
- Cause the perpetrators to flee.
- Precipitate the destruction of evidence.
- Put auditors in danger of bodily harm.

The finding of probable fraud now becomes a forensic audit.

A forensic audit, the results of which may ultimately be presented in an administrative tribunal, court of law or other judicial proceeding, is then conducted using a variety of evidence gathering techniques. The techniques, similar to those employed by auditors are generally supplemented with other specialized audit and investigative techniques. All evidence gathering techniques used by forensic auditors and investigators must fully comply with prevailing law in order to be admissible as evidence in a court of law or during a judicial proceeding.

II. I. WHEN FORENSIC AUDIT/INVESTIGATION BEGINS

When a conclusion, based on competent, relevant, and sufficient audit evidence is reached by the IA that the *probability* of fraud exists; the auditor/investigator must defer all further audit work and refer to the following forensic audit guidelines:

II. I. I. Jurisdiction of the Internal Auditor

In accordance with the Administrative Code of 1987,²⁷ and as reiterated in the NGICS, the functions of the IAS / IAU do not include forensic auditing or criminal investigation Internal Audit Service. Its functions are limited to the following:

²⁷ Title V, Chapter 3, Section 8.

- (1) Advising the DS/HoA on all matters relating to management control and operations audit;
- (2) Conducting management and operations performance audit of Department/Agency/GOCC/GFI activities and units and determine the degree of compliance with established objectives, policies, methods and procedures, government regulations, and contractual obligations;
- (3) Reviewing and appraising systems and procedures, organizational structure, assets management practices, accounting and other records, reports and performance standards (such as budgets and standard cost) of the Department Proper, Bureaus and Regional Offices; and
- (4) Analyzing and evaluating management deficiencies and assist top management to solve the problems by recommending realistic courses of action; and
- (5) Performing such other related duties and responsibilities as may be assigned or delegated by the DS or as may be required by law.²⁸

As such, as recommended above, a fraud/forensic audit group within, the IAS/IAU should be set up within the office concerned. Otherwise, the forensic audit should be carried out by an independent external body with the appropriate mandate to conduct such auditing.

Nonetheless, the results of an audit investigation can generally be used in a court of law or an administrative proceeding. The role of the IAS/IAU in conducting a forensic audit specifically involves the audit/investigation of a probable fraud or a presumptive fraud in order to gather evidence that can be presented to an investigative body in furtherance of a criminal investigation.

IAs, because of their expertise, may be called upon to assist government agency authorized to conduct a criminal investigation, and work under their direction in investigating cases of probable fraud.

II.1.2. Deciding to Conduct a Forensic Audit/Investigation

As soon as the IAS/IAU collect audit evidence sufficient to conclude with a preponderance of evidence that the *probability* of fraud exists, that conclusion should be reported to the internal fraud audit group or the appropriate government agency. The findings of these entities should thereafter be reported to the appropriate persons. In the case of the propriety of filing an administrative case, the reports should be forwarded to the appropriate Disciplinary Authority (depending on the position of the suspect). In the case of filing a criminal case, the reports should be placed within the context of a complaint and filed with the appropriate investigating authority which possesses jurisdiction to make a finding of probable cause to indict a person for an offense. An administrative complaint may run parallel to a criminal case.²⁹ As a general rule, there is no double jeopardy between a criminal case and an ensuing administrative case, except where the very basis of the administrative case against petitioner is conviction in a criminal case where he is acquitted, the administrative case must be dismissed.³⁰

II.1.3. Planning and Preparing For the Forensic Audit

There are no forensic audit or investigative procedures that are unique to all cases of possible fraud. Each case is different and requires its own study and analysis to plan the best approach. For example, in a case involving the theft of equipment, a physical inventory should be taken by the forensic auditors/investigators. These auditors/investigators would also be tasked to

²⁸ *Id.*

²⁹ Please see *Perez vs. Mendoza*, G.R. No. L-22006, July 28, 1975; and *Apolinario vs. Flores*, G.R. No. 152780, January 22, 2007.

³⁰ *Larin vs. Executive Secretary*, G.R. No. 112745, October 16, 1997.

conduct interviews of employees and others to obtain explanations of circumstances surrounding the irregularity detected. Cases involving contract bidding irregularities or suspicious contract change orders would be planned differently.

The auditors/investigators must rely on good professional judgment in selecting the best procedures for gathering evidence, and must also be sufficiently trained to detect such items as the falsified documents, forged signatures, and evidence of collusion.

As soon as the auditors/investigators begin investigating a fraud, the usual audit role of reviewing controls as part of routine auditing is changed. The auditors/investigators now assume duties more like that of a detective, gathering evidence to determine, among other things, whether:

- There is a probable fraud,
- Who may have committed the probable fraud,
- The extent of the loss if any, and
- Information as to how the probable fraud was perpetrated.

Auditors/investigators must investigate all discrepancies, irregularities, and unusual incidents and extraordinary observations. They should believe no explanations until they can be proven, and must routinely suspect possible collusion. Speed is essential in collecting evidence to prevent the destruction of records and to obtain evidence useful in interviewing witnesses.

Auditors/investigators should concentrate their efforts on those areas that are most likely to provide specific evidence as to the suspected fraud. To conserve time and resources, test checks should be limited, highly focused, and emphasize the specific areas of investigative concern.

As the investigation proceeds, information obtained by interviews with employees should be used to help determine investigative emphasis. Auditors/investigators should plan to obtain answers to the following questions and manage their work accordingly:

- Can the probable fraud be easily determined, or does it require extensive tracing of transactions through the records?
- What documents and evidence are needed to prove the probable fraud and the intent of the fraudulent actions?
- How far back does the fraudulent activity go?
- What assets if any been stolen, and what is the value of those assets?
- Do records indicate that there have been prior frauds that have not been thoroughly investigated or have been covered up?
- Has management been aware of any wrongdoing and taken any action?
- How many persons are involved?
- What is known or can be learned about the suspect's habits and finances?
- Do personnel files indicate employment background verification?

Those with the most impeccable credentials often perpetrate fraud. When concealment is suspected, the auditors/investigators should consider first the person with best access to a course of concealment and whose guilt would have been obvious without concealment.

- The auditors should concentrate on the weakest point in the possible fraud chain.
- Many frauds are simple and often obvious. Auditors should consider first the easiest path of the steal-convert-conceal theme. They should not overlook the obvious. They should start with the most elementary solution and, if that does not succeed, progress to the next most obvious solution and proceed systematically on that basis.
- Auditors/investigators should be keenly aware of irregular entries and be particularly wary of altered entries, amended documents, photocopies and duplicate documents, and especially addresses with only a post office box number.

Generally, a suspected employee should not be informed of the auditor's/investigator's suspicions until strong evidence has been gathered. While the matter is still under investigation, the employee may be assigned to other work. Moreover, it may be necessary to take immediate control over the employee's records to prevent their alteration or destruction.

II.1.4. An Attorney Should Be Assigned to the Fraud Audit/Investigation

Because the matter may ultimately be litigated before an administrative tribunal or the trial courts, and because matters of law are involved, an attorney should be assigned responsibility for working closely with the auditors/investigators during the forensic audit.

This access to an attorney helps assure that the auditors/investigators collect evidence in accordance with the requirements of Philippine law, and collect evidence that will demonstrate that fraud has occurred. The auditors/investigators must be charged with the responsibility for routinely conferring with the attorney and for assuring that the attorney is kept informed of the progress of the audit/investigation.

II.1.5. An Investigative Theory Must Be Developed

Each forensic audit/investigation begins with the assumption that the case will eventually be litigated in court. Accordingly, when the probability of fraud has been determined, a fraud investigation plan should be structured around the following principles:

1. Analyze available data.

The data developed in concluding that the probability of fraud has occurred must be thoroughly tested and analyzed. That analysis should result in a comprehensive understanding of the circumstances that surround the probability of fraud, and an inventory of all the factual material collected during the audit.

2. Create a hypothesis.

Based on the analysis of all the available audit evidence, the forensic auditors/investigators conducting the planning should develop a theory. The theory should encompass such elements as how the fraud may have occurred, who was involved in the fraud, when the fraud took place, what was done to facilitate it, and what additional evidence is needed to prove the fraud, and whether the evidence is available.

3. Test the hypothesis.

Based on the elements of the developed hypothesis, the forensic auditors/investigators should collect sufficient factual information to test their theory. Could the fraud have occurred as theorized? Could those theorized as capable of committing the fraud, actually have been able to commit the fraud? Could the fraud have been committed as theorized? Is there evidence available to prove the fraud?

4. Refine and amend the hypothesis.

After testing the hypothesis the auditors/investigators may conclude that the evolving facts do not fit the theory developed. This may indicate that:

- fraud was not committed,
- fraud cannot be proven, and/or
- another theory must be developed and tested.

The hypothesis testing may also reveal that the theory was valid and that a forensic audit/investigation can commence and an investigation plan prepared.

Matters to be considered, as part of the fraud audit/investigation planning process should include:

- Terms of reference for the investigation.
- Specific issues and matters to be examined in depth.
- Evidence required.
- Identification of functional areas and key staff to be involved.
- Identification of specialist expertise or support required.
- Expected costs and time period for the investigation.
- Milestones, key review points and report-back dates.
- Possible outcomes.

All audit/investigative plans should be documented in writing and retained as a part of the audit/investigative file.

III. FORENSIC AUDIT TECHNIQUES

Forensic audit techniques include the full range of audit techniques as well as enhanced audit techniques, to permit the collection of evidence that will demonstrate that a fraudulent act has been committed and should be referred to authorized officials for their disposition.

III.1. Formulating Investigative Questions

Each complete forensic audit/investigation must address certain specific issues. Formulating them as questions, and then collecting evidence through a variety of other audit/investigative techniques is a method of answering those questions. These investigative questions are:

- Were improper practices or inappropriate behaviors engaged in or otherwise carried out? Evidence must be collected to demonstrate that improper practices, such as the violation of a law or regulation, or the non-compliance with a contract's terms, were carried out.
- Were these improper practices or inappropriate behaviors carried out intentionally? Evidence must be collected to demonstrate that the improper practices were carried out intentionally and not accidentally or unwittingly.
- Were these improper practices or inappropriate behaviors carried out through the misrepresentation of material facts in order to deceive? Evidence must be collected to demonstrate that the improper practices were carried out by misrepresenting facts that influenced a decision, or modified a behavior.
- Did the victim rely on these misrepresentations? Evidence must be collected to demonstrate that the victim had the right to rely on these improper practices to make a decision or take an action.
- Did the improper practice or inappropriate behaviors result in injury or damage? Evidence must be collected to demonstrate that the improper practices caused damage, harm, or some other injury.
- Did all parties to the improper transaction benefit? Evidence must be collected to demonstrate that the improper practices benefited the perpetrators that they gained something from their improper behavior.

Answers to these investigative questions should result in the accumulation of evidence. That accumulated evidence should permit conclusions to be drawn as to the probable commission of a fraud. Specifically whether:

- A material fact or facts were misrepresented,
- The misrepresentation was made knowingly and with the intent to deceive,
- The victim relied on the misrepresentation,
- Injury or damage resulted because the victim relied on the misrepresentation, and
- Parties to the improper transaction benefited.

These determinations will support the decision as to whether a referral to a judicial body for prosecution or for further investigation is warranted, and finally, whether the matter will eventually be litigated in court.

III.2. Forensic Audit Evidence Standards

The rules of evidence to support a potential criminal investigation are different from audit evidence standards and requirements. The collection of evidence for a matter that may ultimately be litigated in a court of law must meet a higher standard of evidence than audit evidence. An auditor, when conducting an investigation into a probable fraud case, must meet this higher standard.

The evidence collected to prove fraud as a criminal matter requires a level of evidence that demonstrates *beyond a reasonable doubt* that a crime has been committed.

An auditor, when conducting a forensic audit/investigation that may eventually be referred to the judicial process and that requires the application of audit/investigative techniques, must meet forensic audit standards for evidence—whether administrative, civil or criminal.

The evidence gathered by the forensic auditor for a criminal case must convince an honest and reasonable lay person, *beyond a reasonable doubt*, that the accused is guilty of committing the offense, and for a civil case, a preponderance of evidence is required.

Forensic evidence is anything that can be weighed, evaluated, and presented in support of an action, which action will be subject to the scrutiny of the judicial system. The quantity and quality of that evidence, after being weighed and impartially evaluated by a reasonable person or body of reasonable persons, must be such in a criminal case that there is no reasonable doubt in the minds of those considering the evidence presented.

Evidence can be anything that can be perceived by the senses. For example, it can take the form of:

- Testimony of witnesses,
- Books, records and other documents,
- Recorded data on film, or in picture form, or on audio-tape, and
- Concrete or physical, tangible objects.

To be legally acceptable as evidence, all evidence including testimony, books, records and documents, recorded data on film or in picture form, or on audiotape, and concrete objects must be competent, relevant, and material to the issues being contended in court. In addition, to be used in a court of law, all the evidence must have been gathered in a lawful manner.

Evidence gathered during a forensic audit, to be legally acceptable as evidence in a court of law, must be competent, relevant and material:

Competent. The competency of evidence is judged by whether it is:

- Adequately sufficient. The evidence is complete and does not require or depend on other evidence to support it.
- Reliable. The evidence can be depended on to convey the fact or information that is intended by the introduction of the evidence.
- Presented by a qualified and capable witness. The person presenting the evidence in testimony must be qualified to present it. A person who is not qualified as an accountant may not be able to testify to accounting related issues. Generally speaking, an individual can only testify to things about which he or she has direct and personal knowledge.

Relevant. The evidence must be relevant to the issues being presented before the court. Specifically, to be relevant the evidence must have a tendency to establish a disputed fact. Some of the evidentiary matters that have been acceptable as relevant include:

- A confession
- Attempting to destroy evidence
- Physical evidence linking the accused to the crime
- The means available to commit the crime.

Material. The materiality rule requires that the specific evidence must have an important value to the issue being brought before the courts. The court may not allow repetitive or additive evidence.

CHAPTER IV. FORENSIC EVIDENCE UNDER THE CONTEXT OF PHILIPPINE LAW

There are a variety of types of forensic evidence that the auditor/investigator may collect during a forensic audit/investigation, to be eventually used in prosecution. Knowledge and application of Philippine rules on evidence is indispensable to evidence gathering, preservation and use in prosecution.

I. DEFINITION AND PURPOSE OF EVIDENCE

I.1. Definition

Evidence is understood in different contexts, and you need to ensure that you refer to evidence in either one of the following contexts:

- a. As a set of rules for proving a factual proposition or denial:
“Evidence is the means, sanctioned by these Rules, of ascertaining in a judicial proceeding the truth respecting a matter of fact.”³¹
- b. As the proof itself of the factual proposition or denial i.e, any matter, verbal or physical, to support the existence or non-existence of a factual proposition (e.g., testimonial evidence, documentary evidence, object evidence).

I.2. Purpose

The purpose of an investigator in *looking for* evidence, or of a prosecutor or defense lawyer in *presenting* evidence, or of a court in *admitting* evidence is the *same* -- to prove a factual proposition or denial. Thus, evidence addresses a factual proposition or denial. In this sense, evidence addresses a question of fact while argument addresses a question of law.

Furthermore, the specific purpose or purposes for which evidence is offered determines its admissibility. An important principle in the law of evidence is that a piece of evidence may be admissible for one purpose but not for another, or admissible against one party but not another. With respect to relevance, the relevance of a piece of evidence is determined in relation to the factual proposition to which it is directed; there is no relevance in the abstract.

I.3. Characteristics

The investigator or prosecutor should submit only evidence that the court will admit, which is evidence that is relevant and competent relative to the issue sought to be proved.³² Evidence is relevant when it has “such a relation to the fact in issue as to induce belief in its existence or non-existence.”³³ Evidence is competent when it is not excluded by the law or the Rules of Court.³⁴

With respect to object evidence and documentary evidence, they must be “authenticated” before they can be admitted. It means that the object or writing must be shown to be what its

³¹ Rule 128, Section 1, Rules of Court.

³² Rule 128, Section 3, Rules of Court.

³³ *Id.*, at Section 4.

³⁴ *Id.*, at Section 3.

proponent claims it to be. Thus, as regards real evidence, authentication consists of showing that the object is the object that was involved in the underlying event or transaction. And with respect to a document or writing, authentication will consist of showing who its author is.

Authentication and identification of evidence “are merely aspects of relevancy which are a necessary condition precedent to admissibility.”³⁵ For instance, suppose that in a murder prosecution, the prosecution offers into evidence a gun. Without a showing that the gun has at least some connection to the crime (e.g., that it was found at the scene), the gun is simply irrelevant – it does not make any proposition of fact more or less probable than it would be without the gun. Thus, the requirement of authentication is a requirement that there be a logical nexus between the evidence and the point on which it is offered.”³⁶

II. STANDARD OF PROOF IN CRIMINAL CASES

The standard of proof is that quantum of evidence needed to prove the fact in issue. In criminal cases, this standard varies, depending upon the context in which the standard is applied. There are two relevant evidentiary standards in criminal cases.

II.1. Probable Cause

- a. To make a warrantless arrest;³⁷
- b. To obtain a search and seizure warrant;³⁸
- c. To obtain a freeze order in money laundering cases;³⁹ and
- d. To file an information after preliminary investigation⁴⁰

II.2. Guilt Beyond Reasonable Doubt

- a. To convict; and
- b. To affirm a conviction⁴¹

III. TYPES OF EVIDENCE

III.1. Based on the Form of the Evidence

III.1.1. Objects

Objects include things that the court can observe (i.e., things that it can see, hear, smell, taste, or feel).⁴²

³⁵ 5 Weinstein’s Evidence, Section 901 (a)(02).

³⁶ Lempert, R. and Saltzburg, S., A Modern Approach to Evidence, p. 997 (2nd ed., 1982).

³⁷ Article III, Section 2, Constitution; Rule 113, Section 5, 2000 Revised Rules of Criminal Procedure (2000 Rules).

³⁸ Rule 126, Section 4, 2000 Rules.

³⁹ Republic Act or “R.A.” No. 9160, Section 10; as amended by R. A. No. 9194.

⁴⁰ Rule 112, Section 4, 2000 Rules.

⁴¹ Rule 120, Section 2, 2000 Rules.

⁴² Rule 130, Section 1, Rules of Court.

III.1.2.1. Real Evidence

Refers to tangible items that actually played a role in the matter in dispute (e.g., marked money in a bribery case, substandard road or combat boots in a case under Paragraph 3(e) of R.A. No. 3019, a luxury vehicle, house or condominium unit in a lifestyle check case).

Regarding the probative value of real evidence, the Supreme Court has, in one recent case, ruled that physical evidence is a mute but eloquent manifestation of truth, and it ranks high in our hierarchy of trustworthy evidence. Physical evidence is evidence of the highest order. It speaks more eloquently than a hundred witnesses.⁴³ The reason is that the judge can perceive first-hand the real or physical evidence without a witness as intermediary or regardless of any contrary testimony of a witness. Testimonial evidence, on the other hand, always requires the judge to assess the credibility of the witness.

III.1.2.2. Demonstrative Evidence

- (1) Refers to tangible evidence that illustrates a matter of importance in the litigation (e.g., photograph, map, skeleton, model).
- (2) Helps explain, clarify or illustrate testimony to facilitate understanding by the court, especially technical or difficult issues of fact (e.g., flow chart, mock-up, modals, computer simulation).
- (3) Must be shown to be a fair and accurate representation of what it purports to depict.
- (4) Has no independent substantive force but serves merely as a visual aid to the judge's understanding of the testimony.

III.1.2. Documents

Documents include writings or any material containing letters, words, numbers, figures, symbols or other modes of written expression offered as proof of their contents.⁴⁴ They are further classified into:

III.1.2.1. Public Documents

- (1) Written official acts, or records of the official acts of the sovereign authority, official bodies, and public officers of the Philippines and of a foreign country;
- (2) Documents acknowledged before a notary public, except, last wills and testaments; and
- (3) Public records, kept in the Philippines, of private documents required by law to be entered therein.

III.1.2.2. Private documents – ALL other writings that are not public.

III.1.2.3. Electronic documents

III.1.3. Testimony

Testimony refers to statements given by witnesses during the trial or at depositions that are, in accordance with the rules, adopted by the party presenting the deponent.⁴⁵ This is evidence in itself; and it is also a medium for introducing other evidence.

⁴³ Pelonia vs. People of the Philippines, G.R. No. 168997, April 23, 2007.

⁴⁴ Rule 130, Section 2, Rules of Court.

⁴⁵ Rule 130, Sections 20-51, Rules of Court.

III.2. Based on the Connection to the Factual Issue

III.2.1. Direct Evidence

This is evidence which, if believed, resolves a matter in issue;⁴⁶ it asserts the existence of the fact to be proven or in the case of object evidence, embodies or represents that fact.⁴⁷ Direct evidence when offered to help establish a material fact can never be irrelevant.⁴⁸

III.2.2. Circumstantial Evidence

This is evidence which, even if believed, does not resolve the matter at issue unless additional reasoning is used to reach the proposition to which the evidence is directed.⁴⁹ Circumstantial evidence does not actually assert or represent the fact to be proven but from which the judge can infer an increased probability that the fact exists.⁵⁰ Circumstantial evidence, even if offered to prove a material fact, is irrelevant if the evidence has no probative value, i.e., it does not affect the probability of the proposition to which it is directed.

Rule 133, Section 4 of the Rules of Court delineates when circumstantial evidence is sufficient for conviction:

Circumstantial evidence, when sufficient. —

Circumstantial evidence is sufficient for conviction if:

- (a) There is more than one circumstance;*
- (b) The facts from which the inferences are derived are proven; and*
- (c) The combination of all the circumstances is such as to produce a conviction beyond reasonable doubt.*

III.2.3. Substitute for Evidence

In certain instances, a fact can be established without formal evidentiary proof.

III.2.3.1. Mandatory judicial notice

This covers the existence and territorial extent of states, their political history, forms of government and symbols of nationality, law of nations, admiralty and maritime courts of the world and their seals, political constitution and history of the Philippines, laws of nature, the measure of time, and the geographical divisions.⁵¹

III.2.3.2. Discretionary judicial notice

These are matters that:

- (1) are of public knowledge
- (2) are capable of unquestionable demonstration
- (3) ought to be known to judges because of their judicial functions⁵²

⁴⁶ McCormick on Evidence, p. 543 (3rd ed., 1984).

⁴⁷ Mueller & Kirkpatrick, Modern Evidence, section 4.1 (1995).

⁴⁸ Id.

⁴⁹ Id.

⁵⁰ Mueller & Kirkpatrick, Modern Evidence, section 4.1 (1995).

⁵¹ Rule 129, Section 1, Rules of Court.

⁵² Rule 129, Section 2, Rules of Court.

III.2.3.3. Judicial admissions

These are verbal or written statements of a party regarding the truth or falsity of a fact in issue made in the course of the proceedings in the same case which may be contradicted only by showing that they were made through palpable mistake or that they were never made.⁵³ Judicial admissions are not evidence at all but are formal admissions in the pleadings in the case or stipulations, oral or written, by a party or his counsel which have the effect of withdrawing a fact from issue and dispensing wholly with the need for proof of the fact.⁵⁴

III.2.3.4. Conclusive presumptions⁵⁵

III.2.3.5. Disputable presumptions⁵⁶

IV. RULES OF ADMISSIBILITY OF EVIDENCE

In general, there are only two requirements for evidence to be admitted, namely, *relevancy and competency*. Relevancy is determined by the rules of logic and human experience.⁵⁷ Evidence is admissible, according to Rule 128, Section 3 of the Rules of Court, when it is “not excluded by the law or these rules.” Illegally obtained evidence, although otherwise competent evidence under the Rules of Evidence, is inadmissible because it is excluded by the Constitution or statute.

Evidence will be presumed to have been legally obtained, unless challenged through a timely objection. The party who objects to the admissibility of evidence on the ground that it was obtained in violation of constitutional rights (e.g., through an invalid search) or illegally (e.g., through an illegal wiretap) must support his objection. Unless the objection is overcome, the illegally seized or procured evidence must be excluded, notwithstanding that it is relevant. This illustrates the requirement of competency for admissibility – i.e., “not excluded by the law or these rules.”

With respect to object evidence and documentary evidence, even if relevant and not otherwise excluded by the law or the rules of evidence, they must be “authenticated” before they can be admitted – i.e., that the object or writing is what its proponent claims it to be.

IV.I. Authentication

All object and documentary evidence must be “authenticated” before they can be admitted. Authenticity refers to the genuineness of the evidence (i.e., that the evidence before the court is what it purports to be). In other words, the question to be answered by proof of authenticity is this: *Is the evidence being presented the very same object or document that is the subject matter of the fact in issue?* If so, then it is said to be authentic and the court may proceed to admit and consider it. If not, then it is said to be inauthentic, and will not be admitted because it cannot serve the purpose of evidence, which is to ascertain the truth.

Authentication represents a more specific application of the requirement of relevancy. If an object is not supported by evidence significant to support a finding that it is what its proponent claims, it lacks relevance and is subject to exclusion.

⁵³ Rule 129, Section 4, Rules of Court.

⁵⁴ McCormick on Evidence, p. 776 (3rd ed., 1984).

⁵⁵ Rule 131, Section 2, Rules of Court.

⁵⁶ Rule 131, Section 3 Rules of Court.

⁵⁷ II Regalado, F., Remedial Law Compendium, p. 673 (10th ed., 2004).

IV.1.1. Real Evidence

To prove that an object played some actual role in the underlying event or transaction, there are two methods of authenticating it:

IV.1.1.1. Ready identifiability

If the object has distinctive characteristics, appearance, or identifying marks, it may be authenticated by a witness with personal knowledge to identify it by such distinctive marks.

IV.1.1.2. Chain of custody

Identification by showing the chain of custody is particularly required for evidence that is fungible, lacking in distinctive means of identification, or likely to deteriorate or change in condition. Establishing a chain of custody requires calling each of the persons who had custody of the item from the time of the relevant event until trial and offering testimony showing: (1) when (date, time, place) they took custody and from whom; (2) the precautions they took to preserve the item; (3) the item was not changed, substituted, or tampered with while they had it; and (4) when (date, time, place) they relinquished custody and to whom. Each witness should also testify that the item offered appears to be in the same condition as when they had custody of it.⁵⁸

As a mode of authenticating evidence, the chain of custody rule requires the presentation of evidence be preceded by evidence sufficient to support a finding that the matter in question is what the proponent claims it to be. This would ideally cover the testimony about every link in the chain, from obtaining the evidence up to the time it is offered in evidence, in such a way that everyone who touched the evidence would describe how and from whom it was received, to include, as much as possible, a description of the condition in which it was delivered to the next in the chain.⁵⁹

IV.1.2. Demonstrative Evidence

Authentication basically involves a showing that the object fairly represents or illustrates what it is claimed to represent or illustrate. It may be proved by the testimony of the person/s who produced, and was/were in possession of, the evidence. For example, a photograph may be authenticated by a witness with knowledge who testifies that the photograph accurately represents the scene depicted at the relevant time. The authenticating witness need not be the photographer; the authentication can be done by any competent witness who can testify that the photograph is an accurate or faithful representation of what is depicted.⁶⁰

Photographs can also be authenticated under the “silent witness” doctrine. Reliance on this doctrine is necessary for photographs such as those taken by bank surveillance cameras and automatic teller machines where there is no authenticating witness available who saw the scene depicted or where the witness to the event lacks sufficient memory to authenticate the photograph. The “silent witness” doctrine is also used in other cases where a camera captures the defendant in the act of committing a crime or engaging in other activity relevant to the matters at issue. To authenticate such photographs under the “silent witness” doctrine, they are introduced by showing the “process” by which the photograph was taken (and of course the time and place) and that it produces an accurate result.⁶¹

⁵⁸ Mueller & Kirkpatrick, *Modern Evidence*, Section 9.5 (1995).

⁵⁹ Prieto vs. People, G.R. No. 180870, January 22, 2010.

⁶⁰ Sison vs. People, G.R. Nos. 114931-33, November 16, 1995.

⁶¹ Mueller & Kirkpatrick, *Modern Evidence*, Section 9.15 (1995).

IV.1.3. Challenging the Authenticity of Object Evidence

The authenticity of object evidence which is not uniquely identifiable may be challenged by proving a “reasonable probability” that a tampering occurred because of a “break” in the chain of custody. Thus, in a case where the alleged bribe money was not marked, the serial numbers not noted before the supposed entrapment, and there was no direct proof of receipt by the accused, the charge of bribery was dismissed.

IV.1.4. Documents

IV.1.4.1. Best Evidence Rule

I. General Rule⁶²

“When the subject of inquiry is the contents of a document, no evidence shall be admissible other than the original document itself.”

Before the onset of liberal rules of discovery, and modern techniques of electronic copying, the best evidence rule was designed to guard against incomplete or fraudulent proof and the introduction of altered copies and the withholding of the originals. But the modern justification for the rule has expanded from the prevention of fraud to the recognition that writings occupy a central position in the law. The importance of the precise terms of writings in the world of legal relations, the fallibility of human memory as reliable evidence of the terms, and the hazards of inaccurate or incomplete duplicates are the concerns addressed by the best evidence rule.⁶³

The core concept in the best evidence rule is “when the subject of inquiry is the contents of a document”. Thus, testimony about the making, execution, existence, or delivery of a document does not violate the best evidence rule.

Even though the contents of a document or writing are in some sense being “proved”, if the document is only of tangential importance or not closely related to a controlling issue, the requirement that the original document must be produced may be dispensed with. This is known as the “collateral writings” exception.

The “original” includes:

- (a) Document whose contents are the subject of inquiry

“Original” does not necessarily mean the first or earlier – created document but rather the document that is at issue in the litigation. Thus, a photocopy can qualify as the “original” if it is the document of significance in the litigation. For example, a defendant types an original of a libelous document; he then makes a photo-static copy, but he publishes only the latter. The copy is the operative document under the substantive law and, as such, constitutes the original with respect, to the best evidence rule.⁶⁴

In other words, if the issue is the genuineness of a signature on a letter, then the original document itself must be presented.

However, if the issue is the receipt of the letter by its addressee, then even a mere photocopy that bears an original stamp of receipt is the “original” and therefore is the best evidence to prove the

⁶² Rule 130, Section 3, Rules of Court.

⁶³ Lee vs. People of the Philippines, G.R. No. 159288, October 19, 2004, citing Seiler vs. Lucas Films, Ltd. 808 F.2nd. 1316 (1989).

⁶⁴ Lilly, G., An Introduction to the Law of Evidence, p. 530 (2nd ed., 1987).

factual issue. Thus, it has been held that the rule has no application to proof of facts collateral to the issues such as the nature, appearance or condition of physical objects or to evidence relating to a matter which does not come from the foundation of the cause of action or defense; or when a party uses a document to prove the existence of an independent fact, as to which the writing is merely collated or incidental.⁶⁵

- (b) All copies that have identical contents and were executed at or about the same time. Examples are carbon copies.
- (c) Entry repeated in the regular course of business, one being copied from another at or near the time of transaction. Examples are accounting entries.

2. Exceptions; Proof of contents by secondary evidence

In certain instances, and by way of exception to the Best Evidence Rule, secondary evidence of the original document may be introduced. The original of a document need not be produced as the best evidence when, in any of the following instances, the original:

(a) Is lost, destroyed, or cannot be produced in court⁶⁶

In some cases, the original is no longer available because it has been lost, destroyed, or cannot otherwise be presented in court. In such instances, the Rules allow for the presentation of secondary evidence, subject to compliance with certain requirements.

The offeror of the secondary evidence should not be in bad faith (e.g., he should not have maliciously caused the loss, destruction, or unavailability of the original document). *Only after* proof of the document's existence, execution, and subsequent loss, destruction, or unavailability of *all* originals without fault of the offeror, may its contents be proved by a copy, by a recital of its contents in an authentic document, or by testimony of a witness, in that order.⁶⁷

Thus, proof by secondary evidence requires a 3-stage process of presentation, as follows:

First, establish the prior existence and due execution of the document. This may be done by the testimony of a party who signed the document or a witness to its execution.

Second, evidence of its loss, destruction, or unavailability must be presented. This can be accomplished by the testimony of the custodian or possessor of the lost document (who must testify on the earnest, albeit unsuccessful, efforts to locate the document), or, in the case of old records, of the person who actually shredded the document following the standard and accepted practice of the office. If the policy or procedure for destroying old records is in writing, then this should also be presented. Note that, in case of multiple copies, the evidence must show the loss, destruction, or unavailability of *all copies*.

Third, only after satisfactory completion of the first two steps may the secondary evidence be introduced. Note that secondary evidence must be presented in the following order:

- a. Copy;
- b. Recital of contents in an authentic document; or
- c. Testimony of a witness.

⁶⁵ United States vs. Gonzales-Benitez, 537 F. 1051.

⁶⁶ Rule 130, Section 3(a), Rules of Court.

⁶⁷ Rule 130, Section 5, Rules of Court.

This means that, if a copy of a document is available, a recital of its contents or testimony will not be admissible, and that testimony of the document's contents will be allowed only if both a copy and a recital in an authentic document are not available.

(b) Is in the custody of the adverse party⁶⁸

In some cases, the original is unavailable because it is in the possession of the adverse or opposing party. In those cases, the Rules allow secondary evidence of the document. However, the Rules require that *only after* the adverse party fails to produce the original document despite reasonable notice and opportunity to do so may secondary evidence be presented, as in lost documents.⁶⁹

Thus, the procedure for introducing secondary evidence is as follows:

First, evidence must be presented of the notice to the adverse party to produce the original document. This may consist of a *subpoena duces tecum* issued by the court or even a simple notice in writing, provided proof of receipt of the written notice is shown.

Second, evidence of the adverse party's unjustified refusal or failure to produce the evidence. This implies that the adverse party admits possession but, without valid reason, fails or refuses to present the original document. If the adverse party denies possession, you must produce evidence of possession in order to move forward with the secondary evidence.

Third, you may then introduce the secondary evidence as in the case of lost or destroyed documents (i.e., a copy, a recital in an authentic document, or testimony, in that order).

(c) Consists of numerous accounts⁷⁰

There are instances when the original documents consist of numerous separate documents and books, most common accounting records that may include ledgers, journals, receipts, vouchers, inventory lists, sales records, and other audit papers, but what you want to prove is, "only the general result of the whole" and not the detailed contents of the records. It would therefore be pointless and inconvenient, not to mention a waste of valuable time and resources, to produce in evidence each and every piece of document or page of an accounting book. The Rules therefore allow another exception to the Best Evidence Rule for such numerous accounts. The requirements are that:

- a. The voluminous character of the records must be established;
- b. It is inconvenient to produce such voluminous records in court; and
- c. The original records must be made accessible to the adverse party so that their correctness may be tested on cross-examination.⁷¹

Note that, unlike lost or destroyed originals, the requirement for numerous accounts is "inconvenience" and not necessarily impossibility. Therefore, the basis that must be laid consists of:

First, proof of the voluminous character of the original documents. For example, if the audit consists of an examination of various accounts covering an extended period, then expectedly the number of original documents would be quite large.

⁶⁸ Rule 130, Section 3 (b), Rules of Court.

⁶⁹ Rule 130, Section 6, Rules of Court.

⁷⁰ Rule 130, Section 3(c), Rules of Court.

⁷¹ *Cia. Maritima vs. Allied Free Workers Union, et. al.*, G.R. No. 28999, May 24, 1977.

Second, a statement of the purpose limiting the inquiry to only the general result of the examination. For example, if there is an accusation that some entries were falsified or fictitious, then it would be necessary to produce the original falsified document.

Third, introduction of secondary evidence. This may consist of a summary of the accounts or an audit report.

(d) Is a public record⁷²

This exception provides that, where the original copy is under custody of public officer or recorded in a public office, its contents may be proved by a certified true copy issued by the custodian.⁷³

Examples include the original copy of a Torrens Certificate of Title or the Deed of Sale filed with the Register of Deeds, the Vehicle Certificate of Registration in the LTO, or a person's Birth Certificate on file with the Office of the Civil Register.

The purpose for this exception is public interest. It would be risky for valuable, oftentimes irreplaceable original documents, to be repeatedly taken out of their official repository for presentation in court. Since the custodian is a public officer, the Rules regard a certified true copy by that custodian as the equivalent of the original.

IV.1.5. Testimony

IV.1.5.1. Qualifications

Any person who can perceive and make known his perception to others may be a witness.⁷⁴

The Rule requires two capacities: the ability to perceive, which is physical, and the ability to communicate one's perceptions, which is mental. Thus, an infant can perceive but cannot communicate his perceptions to others. Similarly, a person suffering from certain psychological illnesses, such as severe psychosis, cannot perceive reality, and is, therefore, also disqualified as a witness.

Since all persons are presumed sensate and sane, it follows that, under this rule, every person is *presumed* qualified to testify, and that, unless the witness is proven to be covered by any disqualification, he may testify. Corollary to that, the party who alleges disqualification has the burden of proving that the witness lacks one or both capacities of perception and communication.

IV.1.5.2. Disqualifications

1. Mental condition

This disqualification includes persons whose mental status at the time of the examination prevents them from intelligently making known their perception to others⁷⁵ (e.g., a raving or incoherent witness).

2. Immaturity

Children are presumed competent to testify. A child's competency to testify may be challenged in order to determine the child's ability to perceive, remember, communicate,

⁷² Rule 130, Section 3 (d), Rules of Court.

⁷³ Rule 130, Section 7, Rules of Court.

⁷⁴ Rule 130, Section 20, Rules of Court.

⁷⁵ Rule 130, Section 21 (a), Rules of Court.

distinguish truth from falsehood, or appreciate the duty to tell the truth. The burden of proving incompetence is on the party challenging the presumption.⁷⁶

IV.1.5.3. Testimonial Privilege

Under the adversarial system of litigation prescribed by the Rules, a witness is required to respond truthfully to questions propounded by counsels and the court. However, on grounds of public policy, the Rules allow for exceptions wherein a witness may be excused from testifying or responding to certain questions.

I. Self-incrimination

“No person shall be compelled to be a witness against himself.”⁷⁷

This privilege applies to a defendant in a criminal proceeding and to a witness other than a defendant giving testimony in a case. The accused in a criminal trial may invoke this right and refuse to take the stand at all. That is, the accused has complete immunity from even being called to testify and questioned, let alone being forced to answer. But with respect to a witness other than a defendant giving testimony in a case, he may refuse to answer any question put to him on the ground that it may tend to incriminate him, but he must take the stand and assert the privilege question-by-question.

As the Supreme Court explained in *Secretary Of Justice vs. Lantion*⁷⁸ citing *Pascual vs. Board of Medical Examiners*,⁷⁹ the right against self-incrimination, which is ordinarily available only in criminal prosecutions, extends to administrative proceedings which possess a criminal or penal aspect, such as an administrative investigation of a licensed physician who is charged with immorality, which could result in his loss of the privilege to practice medicine if found guilty.

Also, in *Cabal vs. Kapunan*,⁸⁰ which involved an administrative charge of unexplained wealth against a respondent that was filed under the Anti-Graft and Corrupt Practices Act, the Court ruled that since the investigation may result in forfeiture of property, the administrative proceedings are deemed criminal or penal, and such forfeiture partakes of the nature of a penalty. Therefore, the right against self-incrimination is available to respondent. Following the above rule, the right against self-incrimination should likewise be available to the respondent in an administrative case, because the resolution thereof may result in a penalty upon him, including dismissal.

2. Marital Privilege

Neither spouse may, during their marriage, testify for or against the other without the consent of the affected spouse, except in a civil case by one against the other, or a criminal case for a crime committed by one against the other or the latter’s direct descendants or ascendants.⁸¹

Either spouse, during or after the marriage, cannot be examined as to any communication received in confidence during the marriage, except in a civil case by one against the other, or a criminal case for a crime committed by one against the other or the latter’s direct descendants or ascendants.⁸²

⁷⁶ Section 6, Rule on Examination of Child Witness, A.M. No. 00-4-07 SC.

⁷⁷ Article III, Section 17, Constitution.

⁷⁸ G.R. No. 139465, January 18, 2000.

⁷⁹ G.R. No. L-25018, May 26, 1969.

⁸⁰ G.R. No. L-19052, December 29, 1962.

⁸¹ Rule 130, Section 22, Rules of Court.

⁸² Rule 130, Section 24 (a), Rules of Court.

3. Parental or Filial Privilege

*No person may be compelled to testify against his parents, other direct ascendants, children, or other direct descendants.*⁸³

The public policy behind this exception is the primacy given to the family as a social unit, and is, therefore, similar to the marital privilege. However, under Article 215 of the Family Code, the descendant may be compelled to testify against his parents and grandparents if such testimony is indispensable in prosecuting a crime against the descendant or by one parent against the other.

4. Attorney-Client Privilege

This privilege prohibits the examination of a lawyer, without his client's consent, on any confidential communication made by the client to him, or his advice in the course of, or with a view to, professional employment.⁸⁴

In order for a lawyer to provide effective legal representation, the client should not be inhibited from making a full and candid disclosure of the relevant facts bearing upon his case. The privilege manifests the societal respect for the importance of confidentiality and trust in the attorney-client relationship. Otherwise, clients would be deterred from seeking legal assistance or making full disclosure to their lawyers.

The privilege extends to the lawyer's secretary, stenographer, or clerk. However, the privilege does not extend to a third person, such as the adverse party, who comes into lawful possession of the communication.⁸⁵ For example, if a waiter at a restaurant or a taxi driver overhears a conversation between a lawyer and client, they cannot be prevented from testifying on what they heard.

The phrase, "*in the course of, or with a view to, professional employment,*" requires that the information should have been received by the lawyer in his professional capacity or for the purpose of facilitating the rendition of legal services to the client. Thus, where a client consults a lawyer on whether he had violated any law, the lawyer cannot be examined in order to elicit proof of any admission made by the client.

On the other hand, the privilege excludes a situation where the lawyer's involvement is that of a co-conspirator, accomplice, or accessory in an illegal activity. Thus, where a lawyer delivered bribe money to a judge, or committed falsification for a client, neither he nor his client can invoke the privilege against questions relating to those illegal acts. Also, the privilege does not apply where the client asks for assistance in carrying out or defending against future crimes or wrongs.

Note that the privilege is in favor of the client and not the lawyer, such that if the client waives the privilege, the lawyer has no right to refuse to disclose the information.

5. Doctor-Patient Privilege

A physician cannot be examined in a civil case, without his patient's consent, on any advice or treatment given by him or any information acquired in a professional capacity, which information was necessary to enable him to act in that capacity, and which would blacken the reputation of the patient.⁸⁶

⁸³ Rule 130, Section 25, Rules of Court.

⁸⁴ Rule 130, Section 24 (b), Rules of Court.

⁸⁵ Barton vs. Leyte Asphalt & Mineral Oil Co., G.R. No. 21237, March 22, 1924.

⁸⁶ Rule 130, Section 24(c), Leyte Asphalt & Mineral Oil Co.

Respect for privacy is the public policy behind this privilege. Note that the privilege belongs to the patient, not the physician, and like any privilege, it may be waived by the patient.

6. Priest-Penitent Privilege

This prohibits examination of a priest or minister without the consent of the person making the confession as to any confession made to, or any advice given by him, in his professional character in the course of discipline enjoined by the church to which the priest or minister belongs.

This exception recognizes the long-held tradition of the sanctity of the confessional. The Rules accept that the vow of confidentiality that priests take for confessions made by them is superior to the oath they take as witnesses, and that it is unrealistic to expect any priest to give up the former for the latter. After all, he makes his vow before God while the witness' oath is before man.

7. State Secrets

This privilege prohibits the examination of any public officer, during or after his term, as to communications made to him in official confidence when, the court finds that, the public interest would suffer by the disclosure.⁸⁷

Again, the dictates of public policy compel the subordination of the search for the truth in a specific case to the larger public interest. Note that the privilege is not automatic, and that it is for the court to determine whether or not public interest will be adversely affected by the disclosure. Thus, whenever invoked, the judge must ascertain the nature of the testimony, the public interest involved, as well as the effect of one on the other. If necessary, the judge may hear the proposed testimony in chambers and off the record, in order to determine whether or not he will allow the testimony.

8. Editorial Privilege

This privilege prevents the publisher editor, columnist, or duly accredited reporter of any newspaper, magazine, or periodical of general circulation from being compelled to reveal the source of any news report or information appearing in said publication which was related in confidence to him. It is based on the public policy recognizing the vital role that the media plays in society, and the importance of protecting confidential sources of information in order for the media to fulfill that role; the concern is that these sources will “dry up” if their identities may be subject to compulsory disclosure.

However, as an exception to the exception, courts or Congress can compel disclosure in the interest of national security. The privilege does not, however, exempt journalists from civil or criminal liability (e.g., for libel or sedition, for any of their public statements).⁸⁸

IV.1.5.4. Admissions and Confessions

Admissions and confessions constitute valuable evidence in any litigation. A court will accord full evidentiary weight to an accused's extra-judicial admission or confession unless he comes forward with an explanation or counterproof. Thus, to rebut an admission or confession, a defendant will be forced to take the stand and risk impeachment. Therefore, be mindful of the adverse party's admissions in public statements, affidavits, media interviews, etc. With respect to an extra-judicial confession, take note of Rule 133, Section 3 of the Rules of Court, which provides that an extra-judicial confession made by an accused is not a sufficient ground for conviction without proof of the corpus *delicti*.

I. Inadmissible Acts or Declarations

⁸⁷ Rule 130, Section 24(e), Rules of Court.

⁸⁸ R.A. No. 53, as amended by R.A. No. 1477.

The following acts or declarations are inadmissible:

- a. An offer of compromise in a civil case;⁸⁹
- b. A plea of guilt later withdrawn, or an unaccepted offer of a guilty plea to a lesser offense;⁹⁰ and
- c. An offer to pay for the medical, hospital or other expenses occasioned by an injury.

2. Party Admissions

The following acts, declarations, and omissions of a party are *binding on him or her* and are therefore *admissible* in evidence, subject to the requirements specified below:

a. As to a relevant fact ⁹¹

These are admissions made by a party extra-judicially or out of court.

A defendant's answer in the administrative proceedings may be given in evidence against him in the criminal proceedings as an admission of a party.⁹²

b. Offer of compromise by the accused

Except in quasi-offenses and those allowed by law to be compromised, an offer of compromise by the accused is considered an implied admission of guilt.⁹³

For example, the ruling in a rape case that an offer to pay-off the complainant is admissible as an implied admission of guilt may be cited by analogy in a corruption case.⁹⁴

c. Silence

Silence requires that: *i) an act or declaration is made in the presence and within the hearing or observation of a party; ii) who does or says nothing; iii) when the act or declaration is such as naturally to call for action or comment if not true; and iv) when proper or possible for him to do so.*⁹⁵ Admission by silence:

- Requires that the party understood the meaning of the act or declaration.
- Assumes that he was aware of the truth, or conversely the falsity of the act or declaration.
- Requires that he must have an interest to object such that he would naturally have done so, if the statement was not true. The occasion and nature of the statement should be such that he would likely have replied if he did not mean to accept what was said.
- Silence is not protected by the constitutional right to remain silent.

d. Confessions

The declaration of an accused acknowledging his guilt of the offense charged, or of any offense necessarily included therein, may be given in evidence against him.⁹⁶ If the accused admits having committed the act in question but alleges a justification therefor, the same is merely an admission.⁹⁷

However, any confession or admission obtained through torture, force, violence, threat, intimidation, or any other means which vitiate the free will, or while the accused was held in

⁸⁹ Rule 130, Section 27, Paragraph 1, Rules of Court.

⁹⁰ Rule 130, Section 27, Paragraph 3, Rules of Court.

⁹¹ Rule 130, Section 26, Rules of Court.

⁹² Perez vs. People, G.R. No. 164763, February 12, 2008.

⁹³ Rule 130, Section 27, Paragraph 2, Rules of Court.

⁹⁴ People vs. Viernes, G.R. No. 136733-35, December 13, 2001.

⁹⁵ Rule 130, Section 32, Rules of Court.

⁹⁶ Rule 130, Section 33, Rules of Court.

⁹⁷ U.S. vs. Tolosa, G.R. No. 2650, February 16, 1906.

secret detention places, solitary, or *incommunicado*, or in violation of the person's so-called Miranda rights, is *inadmissible* in evidence for any purpose.⁹⁸

3. Third parties

The rights of a party cannot be prejudiced by an act, declaration or omission by another,⁹⁹ *except* by the following:

a. Co-partner, agent, joint owner, joint debtor, or other person jointly interested with the party –

The act or declaration must be:

- Within the scope of the partner's or agent's authority
- Made during the existence of the partnership, agency, or joint interest
- The partnership, agency, or joint interest is shown by evidence other than such act or declaration¹⁰⁰

b. Conspirator

The act or declaration must be:

- Related to the conspiracy
- During its existence
- The conspiracy is shown by evidence other than such act or declaration¹⁰¹

The foregoing requisites are not required with respect to admissions by a conspirator on the witness stand because the co-accused can cross-examine the witness.¹⁰²

c. Privies

Requires that:

- A party is the holder of title to property
- Title to the property was acquired from another
- Previous title holder makes an act or declaration or omits to do something
- While holding the title
- Act or declaration is in relation to the property¹⁰³

IV.1.5.5. Conduct as Evidence

1. Evidence that one did or did not do a certain thing at one time is not admissible to prove that he did or did not do the same or a similar thing at another time, but it may be received to prove a specific intent or knowledge, identity, plan, system, scheme, habit, custom, usage, and the like.¹⁰⁴

Thus, evidence of another crime was held admissible in a prosecution for robbery to prove the identity of the accused or his presence at the scene of the crime.¹⁰⁵ Similarly, previous acts of negligence were held admissible to show knowledge or intent.¹⁰⁶

⁹⁸ Article III, Section 12(3), Constitution.

⁹⁹ Rule 130, Section 28, Rules of Court.

¹⁰⁰ Rule 130, Section 29, Rules of Court.

¹⁰¹ Rule 130, Section 30, Rules of Court.

¹⁰² *People vs. Serrano, et. al.*, G.R. No. L-7973, April 27, 1959.

¹⁰³ Rule 130, Section 31, Rules of Court.

¹⁰⁴ Rule 130, Section 34, Rules of Court.

¹⁰⁵ *People vs. Irang*, G.R. No. 45179, March 30, 1937.

¹⁰⁶ *U.S. vs. Pineda*, G.R. No. 12858, January 22, 1918.

2. A written offer to pay a particular sum of money or deliver a written instrument or specific personal property is, if rejected without valid cause, equivalent to the actual production and tender of the money, instrument, or property.¹⁰⁷

This rule is merely an evidentiary complement to the rule on tender of payment,¹⁰⁸ by providing that said offer of payment must be made in writing.

IV.1.5.6. Testimonial Knowledge

IV.1.5.6.1. Hearsay Rule

As a general rule, a witness may testify only to facts known to him of his own personal knowledge (i.e., those that are derived from his own perception).¹⁰⁹ Briefly defined, hearsay is “a statement or assertive conduct which was made or occurred out of court and is offered to prove the truth of the facts asserted. The purpose for which the statement is offered is dispositive. An out-of-court declaration may be offered into evidence for many purposes other than to prove the truth of the matter asserted in the declaration. In that event, the declaration is not hearsay. Thus, independently relevant statements are non-hearsay. As explained by the Supreme Court in *Estrada v. Desierto*, independently relevant statements are those which are relevant independently of whether they are true or not. They belong to two classes: (1) those statements which are the very facts in issue and (2) those statements which are circumstantial evidence of the facts in issue. The second class includes the following:

- (a) Statement of a person showing his state of mind, that is, his mental condition, knowledge, belief, intention, ill will and other emotions;
- (b) Statements of a person which show his physical condition, and illness and the like;
- (c) Statements of a person from which an inference may be made as to the state of mind of another, that is the knowledge, belief, motive, good or bad faith, etc. of the latter;
- (d) Statements which may identify the date, place and person in question; and
- (e) Statements showing the lack of credibility of a witness.¹¹⁰

I. Declaration against Interest

This includes any declaration:

- Made by a person deceased, or unable to testify;
- Against his own interest.

Basis: If the fact asserted in the declaration was, at the time it was made, so far contrary to the declarant’s own interest that a reasonable man in his position would not have made the declaration, unless he believed it to be true.

It may be received in evidence against himself or his successors in interest and against third persons.¹¹¹ The interest embraced by the exception may be pecuniary, proprietary or penal. A statement fits the exception only if the defendant knew that what he said was against his interest at the time.

¹⁰⁷ Rule 130, Section 35, Rules of Court.

¹⁰⁸ Article 1256, Civil Code.

¹⁰⁹ Rule 130, Section 36, Rules of Court.

¹¹⁰ *Estrada vs. Desierto*, G.R. Nos. 146710-15 and 146738, April 3, 2001.

¹¹¹ Rule 130, Section 38, Rules of Court.

2. Part of the *res gestae*

These are statements made by a person while a startling occurrence is taking place or immediately prior or subsequent thereto.¹¹²

The rule on *res gestae* includes statements accompanying an equivocal act material to the issue and giving it legal significance.¹¹³

2.1. Excited utterances

There are three independent requirements that must be satisfied for the excited utterances exception to apply:

- a. The event giving rise to the statements must be sufficiently startling to eliminate the declarant's capacity to reflect before speaking;
- b. The statements must be made while the declarant is still under the influence of the startling event – i.e., the statements were made before the declarant had the opportunity to contrive; and
- c. The statements refer to the occurrence in question and its attendant circumstances.¹¹⁴

2.2. Verbal acts

For verbal acts to be admissible, it is required that: (a) the *res gestae* or principal act to be characterized must be equivocal; (b) such act must be material to the issue; and (c) the statements give a legal significance to the equivocal act. For example, D hands money to X, a friend who happens to be the town mayor. It is not clear whether the transfer was a loan, gift, or bribe. Therefore, the testimony of a witness who overhears D's statement to X at the time of the transfer, "This is to repay you for the money you lent me last year," is the verbal part of the act of transferring the money. In the United States, verbal parts of acts are considered non-hearsay.

2.3. Entries in the Course of Business

These are entries in business records that were made:

- By a person deceased, or unable to testify;
- At or near the time of the subject transaction;
- By a person who was in a position to know the facts stated in the entries;
- Made the entries in his professional capacity or in the performance of a duty; and
- In the regular course of business or duty.¹¹⁵

In a case where the accountant who made the entries was presented in court, and testified that she made the entries on the basis of the bills given to her but she did not have personal knowledge of the truth of the facts stated in the bills, the Supreme Court ruled that the exception to the hearsay rule did not apply.¹¹⁶

2.4. Entries in Official Records

Rule 130, Section 44, of the Rules of Evidence provides:

Entries in official records made in the performance of his duty by a public officer of the Philippines, or by a person in the performance of a duty specially enjoined by law, are prima facie evidence of the facts therein stated.

The Supreme Court summarized the requisites for this exception as follows:

¹¹² Rule 130, Section 42, Rules of Court.

¹¹³ Id.

¹¹⁴ II Regalado, F., Remedial Law Compendium, p. 747 (10th ed., 2004).

¹¹⁵ Rule 130, Section 43, Rules of Court.

¹¹⁶ Canque vs. Court of Appeals, G.R. No. 96202, April 13 1999.

- a. The entries were made by a public officer in the performance of his duty or by a person in the performance of a duty specially enjoined by law;
- b. The public officer or person who made the entries had personal knowledge of the facts stated by him or such facts were acquired by him from reports made by person under a legal duty to submit the same; and
- c. Such entries were duly entered in a regular manner in the official records.

This exception is based on the presumption that public duty has been faithfully performed. It is important since corruption cases often include official records as evidence. For example, in a malversation case where an entry is made of a short delivery, the record may be used as evidence of the truth of the fact of delivery and the corresponding figures depicting the volume or number of goods delivered, even if the official who made such record is not available, provided the above requisites are proven.

Note, however, that the entries constitute only *prima facie* evidence of the truth of the facts stated in the entries. Hence, contrary evidence may be admitted to refute the entries.

2.5. Commercial Lists

A document is a commercial list if it is a statement:

- Of matters of interest to persons engaged in an occupation;
- Contained in a list, register, periodical, or other published compilation;
- Published for use by persons engaged in that occupation; and
- Generally used and relied upon by persons in that occupation.

A supplier's price list is an example of a commercial list that is very useful evidence in cases of overpricing or rigged bidding under Paragraph 3(e) or 3(g) of R.A. 3019, or in appraising property in lifestyle-check cases. It has been held, however, that price quotations from various suppliers do not qualify under the exception; if the suppliers do not testify, the price quotations are objectionable on the ground of hearsay.¹¹⁷

2.6. Testimony or Deposition at a Former Proceeding

This refers to the testimony or deposition:

- Of a person deceased or unable to testify;
- Given in a former case or proceeding, judicial or administrative;
- In a case involving the same parties and subject matter;
- The issue testified to by the witness in the former trial is the same issue involved in the present case; and
- The adverse party had the opportunity to cross-examine the witness.

Subsequent failure or refusal to appear at the second trial, or hostility since testifying at the first trial, does not amount to inability to testify. Such inability should proceed from a grave cause, almost amounting to death, as when the witness is old and has lost the power of speech.¹¹⁸

IV.1.5.6.2. Opinion

As a *general rule*, opinions are *inadmissible*.¹¹⁹ The rationale is that the process of making inferences from the underlying facts properly belongs to the judge, not to the witness. However, the following are recognized *exceptions*:

¹¹⁷ PNO Shipping & Transport Corporation vs. Court of Appeals, G.R. No. 107518, October 8, 1998.

¹¹⁸ Tan, et. al. vs. Court of Appeals, L-22793, May 16, 1967.

¹¹⁹ Rule 130, Section 48, Rules of Court.

- a. An expert witness may express opinions on a matter requiring special knowledge, skill, experience or training.¹²⁰
- b. Ordinary witnesses may express opinions on:
 - Identity of a person known to him;
 - Familiar handwriting;
 - Mental sanity of a person known to him; and
 - Impressions of the emotion, behavior, condition or appearance of a person.¹²¹

IV.1.5.6.3. Character Evidence

As a *general rule*, character evidence is *not admissible*, save in the following *exceptions*:

1. In criminal cases:

- a. Accused may prove his good moral character, which is pertinent to the moral trait involved in the offense charged:¹²²
- b. Prosecution cannot prove the accused’s bad moral character, except in rebuttal;¹²³
- c. Good or bad moral character of the offended party may be proved if it tends to establish in any reasonable degree the probability or improbability of the offense charged.¹²⁴

The character evidence that may be presented by the accused must be “pertinent to the moral trait involved in the offense charged – e.g., in prosecutions for *estafa*, perjury or false testimony, it is the accused’s moral trait for honesty or probity that is involved.

2. In civil cases

Evidence of a party’s good or bad moral character is admissible only when pertinent to the issue of character involved in the case.¹²⁵

3. Evidence of the good character of a witness is not admissible until it is impeached.¹²⁶

Settled is the principle that evidence of one’s character or reputation must be confined to a time not too remote from the time in question. In other words, what is to be determined is the character or reputation of the person at the time of the trial and prior thereto, but not at a period remote from the commencement of the suit.¹²⁷

IV.2. Relevance

Evidence is admissible when it is relevant to the issue.¹²⁸ *Evidence must have such a relation to the fact in issue as to induce belief in its existence or non-existence. Evidence on collateral matters shall not be allowed, except when it tends in any reasonable degree to establish the probability or improbability of the fact in issue.*¹²⁹

Relevance has two aspects:

¹²⁰ Rule 130, Section 49, Rules of Court.

¹²¹ Rule 130, Section 50, Rules of Court.

¹²² Rule 130, Section 51 (a) (1), Rules of Court.

¹²³ Rule 130, Section 51 (a) (2), Rules of Court.

¹²⁴ Rule 130, Section 51 (a) (3), Rules of Court.

¹²⁵ Rule 130, Section 51 (b), Rules of Court.

¹²⁶ Rule 130, Section 51 (c), in relation to Rule 132, Section 14, Rules of Court.

¹²⁷ Civil Service Commission vs. Alysson Belagan, G.R. No. 132164, October 19, 2004.

¹²⁸ Rule 128, Section 3, Rules of Court.

¹²⁹ Rule 128, Section 4, Rules of Court.

I. Probative value

There must be a probative relationship between the piece of evidence and the factual proposition to which it is addressed. Evidence must have such a relation to the fact in issue as to induce belief in its existence or non-existence.¹³⁰ To assess probative value, a judge applies his “own experience, his general knowledge, and his understanding of human conduct and motivation.”¹³¹

2. Materiality

Evidence is said to be material when it is directed to prove a fact in issue as determined by the rules of substantive law and the pleadings.¹³² Consequently, evidence may have probative value but may be immaterial in the case.

IV.3. Competency

In addition to relevance, evidence to be admissible must be competent (i.e., “not excluded by the law or these rules.”).¹³³ Thus, any evidence that is obtained in violation of any constitutional or statutory proscription cannot be admitted by the courts, even if that evidence is otherwise admissible under the Rules of Evidence. Public policy dictates that such illegally obtained evidence and any evidence referred to as the “fruit of the poisoned tree,” cannot be used for any purpose in any proceeding¹³⁴ in order to protect the rights of persons and to discourage law enforcement officers from violating those rights.

V. WEIGHT AND SUFFICIENCY OF EVIDENCE

Differentiating between admissibility, on the one hand, and weight and sufficiency of evidence, on the other, the Supreme Court, in a recent case, emphasized the distinction between admissibility of evidence and its probative value. According to the Court, the absence of any objection to a piece of evidence does not *ipso facto* mean that it conclusively proves the fact in dispute. The admissibility of evidence should not be confused with its probative value. Admissibility refers to the question of whether certain pieces of evidence are to be considered at all, while probative value refers to the question of whether the admitted evidence proves an issue. Thus, a particular item of evidence may be admissible, but its evidentiary weight depends on judicial evaluation within the guidelines provided by the rules of evidence.¹³⁵

V.I. Direct Evidence

This refers to evidence, which, if believed, resolves a matter in issue.¹³⁶ Examples include:

- a. Eyewitness account of the commission of the felony;
- b. Falsified document; and
- c. Marked money.

¹³⁰ Rule 128, Section 4, Rules of Court.

¹³¹ McCormick on Evidence, p. 340 (3rd ed., 1984).

¹³² People vs. Bautista G.R. No. L-49778, January 27, 1981.

¹³³ Rule 128, Section 3, Rules of Court.

¹³⁴ Article III, Section 2, Paragraph (1), Constitution.

¹³⁵ Licomcen vs. Foundation Specialists, Inc., G.R. Nos. 167022 and 169678, August 31, 2007, citing Heirs of Sabanpan vs. Comorposa, G.R. No. 152807, August 12, 2003.

¹³⁶ McCormick on Evidence (3rd ed., 1984).

V.2. Circumstantial Evidence

This refers to evidence which, even if believed, does not resolve the matter at issue unless additional reasoning is used to reach the proposition to which it is directed.¹³⁷ Examples include:

- Testimony of relationship, unexplained wealth, deviation from established practice, to prove bribery;
- Unexplained deposits into personal accounts of money in the same amounts and on the same dates, to prove malversation; and
- A pattern of behavior.

Circumstantial evidence is sufficient for conviction if:

- a. There is more than one circumstance;
- b. The facts from which the inferences are derived are proven; and
- c. The combination of all the circumstances is such as to produce a belief in guilt beyond reasonable doubt.

V.3. Probable Cause

Probable cause is the quantum of evidence required in the following proceedings:

- a. Preliminary investigation;
- b. Applications for warrants of arrest or search and seizure; and
- c. Application for an asset preservation order.

In preliminary investigation, probable cause signifies a reasonable ground of suspicion supported by circumstances sufficiently strong in themselves to warrant a cautious man's belief that the person accused is guilty of the offense charged.¹³⁸ In the language of Rule 112, Section 1 of the Rules of Court, the quantum of evidence is such evidence sufficient to "engender a well-founded belief that a crime has been committed and the respondent is probably guilty thereof, and should be held for trial."

V.4. Preponderance of Evidence

Preponderance of evidence is the quantum of proof required in *civil cases*. Preponderance of evidence refers to evidence which is of greater weight, or more convincing than that which is offered in opposition to it; at the bottom, it means that the party bearing the burden of proof must persuade the court "that the existence of the contested fact is more probable than its non-existence."¹³⁹

In determining where the preponderance or superior weight of evidence on the issues involved lies, the court may consider all the facts and circumstances of the case, the witnesses' manner of testifying, their intelligence, their means and opportunity of knowing the facts to which they are testifying, the nature of the facts to which they testify, the probability or improbability of their testimony, their interest or want of interest, and also their personal credibility so far as the same may legitimately appear upon the trial. The court may also consider the number of witnesses, though the preponderance is not necessarily with the greater number.

¹³⁷ Ibid.

¹³⁸ Tetangco vs. Ombudsman, G.R. No. 156427, January 20, 2006.

¹³⁹ McCormick on Evidence (3rd ed., 1984).

V.5. Proof beyond Reasonable Doubt

In *criminal cases*, the quantum of evidence required to establish the guilt of an accused is *proof beyond reasonable doubt*.

Proof beyond reasonable doubt does not mean such a degree of proof as, excluding possibility of error, produces absolute certainty. Only moral certainty is required, or that degree of proof which produces conviction in an unprejudiced mind.

V.6. Substantial Proof

Substantial proof is the quantum of evidence required to establish culpability in administrative cases. In cases filed before administrative or quasi-judicial bodies, a fact may be deemed established if it is supported by substantial evidence, or that amount of relevant evidence which a reasonable mind might accept as adequate to justify a conclusion.

VI. RULE ON ELECTRONIC EVIDENCE¹⁴⁰

Electronic evidence is a recognized form of evidence. Advances in technology are such that the traditional rules of evidence do not easily, or in some instances do not at all, apply.

It is important to emphasize, however, that while it may be a special form of evidence, electronic evidence must still adhere to the general principle that evidence must be relevant and competent in order for it to be admissible. The E-Commerce Act provides that it “does not modify any statutory rule relating to the admissibility of electronic/data messages or electronic documents, except the rules relating to authentication and best evidence.”¹⁴¹ In other words, an electronic document must still meet the requirements for admissibility prescribed by the rules on evidence.

The E-Commerce Act is basically a rule of non-discrimination. By itself, it does not make an electronic document legally effective, valid and enforceable.¹⁴² Section 7 of the Act provides that, “Information shall not be denied validity or enforceability solely on the ground that it is in the form of an electronic data message purporting to give rise to such legal effect, or that it is merely incorporated by reference in that electronic data message.” And Section 12 further states that: “In any legal proceedings, nothing in the application of the rules on evidence shall deny the admissibility of an electronic data message or electronic document in evidence: (a) on the sole ground that it is in electronic form; or (b) on the ground that it is not in the standard form...”

VI.1. Defined Terms under the E-Commerce Act

- a. “Certificate” means an electronic document issued to support a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair.¹⁴³

¹⁴⁰ A.M.No. 01-7-01-SC, effective August 1, 2001; Originally applicable only in civil cases, these Rules were amended on October 24, 2002 and made applicable as well to criminal cases.

¹⁴¹ Section 7, R.A. No. 8792.

¹⁴² Amador, V., *The E-Commerce Act and Other Laws & Cyberspace*, p. 256 (2002).

¹⁴³ Rule 2, Section 1 (c).

- b. “Computer” refers to any single or interconnected device or apparatus, which, by electronic, electro-mechanical or magnetic impulse, or by other means with the same function, can receive, record, transmit, store, process, correlate, analyze, project, retrieve and/or produce information, data, text, graphics, figures, voice, video, symbols or other modes of expression or perform any one or more of these functions.¹⁴⁴
- c. “Digital Signature” refers to an electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem such that a person having the initial untransformed electronic document and the signer’s public key can accurately determine:
 - whether the transformation was created using the private key that corresponds to the signer’s public key; and
 - whether the initial electronic document had been altered after the transformation was made.
- d. “Digitally signed” refers to an electronic document or electronic data message bearing a digital signature verified by the public key listed in a certificate.¹⁴⁵
- e. “Electronic data message” refers to information generated, sent, received or stored by electronic, optical or similar means.¹⁴⁶
- f. “Electronic document” refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically. It includes digitally signed documents and any print-out or output, readable by sight or other means, which accurately reflects the electronic data message or electronic document. For purposes of these Rules, the term “electronic document” may be used interchangeably with electronic data message.”¹⁴⁷

The Supreme Court has ruled that a photocopy is not considered an electronic document.¹⁴⁸ According to the Court, “(t)he rules use the word “information” to define an electronic document received, recorded, transmitted, stored, processed, retrieved or produced electronically. This would suggest that an electronic document is relevant only in terms of the information contained therein, similar to any other document which is presented in evidence as proof of its contents. However, what differentiates an electronic document from a paper-based document is the manner by which the information is processed; clearly, the information contained in an electronic document is received, recorded, transmitted, stored, processed, retrieved or produced electronically.

A perusal of the information contained in the photocopies submitted by petitioner will reveal that not all of the contents therein, such as the signatures of the persons who purportedly signed the documents, may be recorded or produced electronically. By no stretch of the imagination can a person’s signature affixed manually be considered as information electronically received, recorded, transmitted, stored, processed, retrieved or produced. Hence, the argument of petitioner that since these paper printouts were produced through an electronic process, then these photocopies are electronic

¹⁴⁴ Rule 2, Section 1 (d).

¹⁴⁵ Rule 2, Section 1 (e).

¹⁴⁶ Rule 2, Section 1 (g).

¹⁴⁷ Rule 2, Section 1 (h).

¹⁴⁸ NPC vs. Codilla, Jr., et al., G.R. No. 170491, April 3, 2007.

documents as defined in the Rules on Electronic Evidence is obviously an erroneous, if not preposterous, interpretation of the law. Having thus declared that the offered photocopies are not tantamount to electronic documents, it is consequential that the same may not be considered as the functional equivalent of their original as decreed in the law.

The term “electronic data message” as used in the E-Commerce Law has been held to exclude telexes or faxes, except computer-generated faxes.¹⁴⁹

- g. “Electronic signature” refers to any distinctive mark, characteristics and/or sound in electronic form representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedure employed or adopted by a person and executed or adopted by such person with the intention of authenticating, signing or approving an electronic data message or electronic document. For purposes of these Rules, an electronic signature includes digital signatures.¹⁵⁰
- h. “Ephemeral electronic communication” refers to telephone conversations, text messages, chat-room sessions, streaming audio, streaming video, and other electronic forms of communication the evidence of which is not recorded or retained.¹⁵¹

The admissibility of text messages as part of ephemeral electronic communication has been recognized by the Supreme Court.¹⁵²

The admission of text messages does not violate the right to privacy of the sending party.¹⁵³

VI.2. Electronic Documents

VI.2.1. Electronic documents as functional equivalent of paper-based documents.

Whenever a rule of evidence refers to the term of writing, document, record, instrument, memorandum or any other form of writing, such term shall be deemed to include an electronic document as defined in these Rules.

This provision of the Rule on Electronic Evidence¹⁵⁴ restates the functional equivalent rule in Section 7 of the E-Commerce Act which states, in relevant part, that, “for evidentiary purposes, an electronic document shall be the functional equivalent of a written document under existing laws.”¹⁵⁵

VI.2.2. Admissibility

An electronic document is admissible in evidence if it complies with the rules on admissibility prescribed by the Rules of Court and related laws and is authenticated in the manner prescribed by these Rules.

¹⁴⁹ MCC Industrial Sales Corporation vs. Ssangyong Corporation, G.R. No. 170633, October 17, 2007.

¹⁵⁰ Rule 2, Section 1(j).

¹⁵¹ Rule 2, Section 1(k).

¹⁵² Vidallon-Magtolis vs. Salud, A.M. No. CA-05-20-P, September 9, 2005; Nuez vs. Cruz-Apao, A.M. No. CA-05-18-P, April 12, 2005.

¹⁵³ Vidallon-Magtolis, supra.

¹⁵⁴ Rule 3, Section 1.

¹⁵⁵ Amador, supra, at p. 535.

VI.2.3. Privileged communication

The confidential character of a privileged communication is not lost solely on the ground that it is in the form of an electronic document. Note use of the term “solely,” which means that if there are other circumstances showing that the communication is not intended to be confidential, then it may lose its privileged character.¹⁵⁶

VI.3. Best Evidence Rule

VI.3.1. Original of an electronic document

An electronic document shall be regarded as the equivalent of an original document under the Best Evidence Rule if it is a printout or output readable by sight or other means, shown to reflect the data accurately.

Note that the printout or output readable by sight is treated as the equivalent of an original document only if it is “shown to reflect the data accurately.”

VI.3.2. Copies as equivalent of the originals

When a document is in two or more copies executed at or about the same time with identical contents, or is a counterpart produced by the same impression as the original, or from the same matrix, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original, such copies or duplicates shall be regarded as the equivalent of the original.

Notwithstanding the foregoing, copies or duplicates shall not be admissible to the same extent as the original if:

- a. A genuine question is raised as to the authenticity of the original; or
- b. Under the circumstances, it would be unjust or inequitable to admit a copy in lieu of the original.

VI.4. Authentication of Electronic Documents

VI.4.1. Burden of proving authenticity

The person seeking to introduce an electronic document in any legal proceeding has the burden of proving its authenticity in the manner provided in the Rules.

VI.4.2. Manner of authentication

Before any private electronic document offered as authentic is received in evidence, its authenticity must be proved by any of the following means:

- a. By evidence that it had been digitally signed by the person purported to have signed the same;
- b. By evidence that other appropriate security procedures or devices as may be authorized by the Supreme Court or by law for authentication of electronic documents were applied to the document; or
- c. By other evidence showing its integrity and reliability to the satisfaction of the judge.

In one case, the Supreme Court ruled that mere testimony of the plaintiff that a computer print-out of an electronic document signed and handed to him by an employee of a travel agency that his credit card was blacklisted is not sufficient authentication of said electronic document.¹⁵⁷

¹⁵⁶ Amador, *supra*, at p. 537.

¹⁵⁷ Aznar vs. Citibank, N.A. (Phil), G.R. No. 164273, March 28, 2007.

E-mail messages which were unsigned were denied admissibility by the Supreme Court for lack of proper authentication. The print-outs were not certified or authenticated by any company official who could properly attest that these came from IBM's computer system or that the data stored in the system were not and/or could not have been tampered with before the same were printed out.¹⁵⁸

VI.5. Electronic Signatures

VI.5.1. Definition

An electronic signature or a digital signature authenticated in the manner prescribed hereunder is admissible in evidence as the functional equivalent of the signature of a person on a written document.

A digital signature consists of an encrypted or mathematically scrambled document that appears as a string of characters appended to the message and serves to identify the sender and establish the integrity of the document. Only someone with the proper software can decode the signature.

Digital signatures are typically generated using a public key or an asymmetric cryptosystem. An asymmetric cryptosystem is based on the use of two software codes, or a "public-private" key pair. The "private" key is kept secret by its owner and used to encode the digital signature. The "public" key is made available to persons who need to decode the transmission. The public and private keys are mathematically related, but the relationship is so complicated that it is "computationally infeasible" to deduce one key solely from knowledge of the other key. The keys are such that the digital signature created by one key can only be decrypted by the other key. Public key infrastructure ("PKI") provides the foundation for deploying, using and managing the encryption keys and digital certificates that enable digital signatures.¹⁵⁹

VI.5.2. Authentication of electronic signatures

An electronic signature may be authenticated in any of the following manner:

- a. By evidence that a method or process was utilized to establish a digital signature and verify the same;
- b. By any other means provided by law; or
- c. By any other means satisfactory to the judge as establishing the genuineness of the electronic signature.

VI.5.3. Disputable presumptions relating to electronic signature

Upon the authentication of an electronic signature, it shall be presumed that:

- a. The electronic signature belongs to the person to whom it correlates;
- b. The electronic signature was affixed by that person with the intention of authenticating or approving the electronic document to which it is related or to indicate such person's consent to the transaction embodied therein; and
- c. The methods or processes utilized to affix or verify the electronic signature operated without error or fault.

The presumption in Section 3(c) is based on practical necessity. Without said presumption, authenticating a digital signature could be very tedious and time-consuming as the proponent has to prove that the process operated without any hitch or error. The presumption is called

¹⁵⁸ IBM Philippines, Inc, et al. vs. NLRC, et al., G.R. No. 117221, April 13, 1999.

¹⁵⁹ Amador, op. cit. supra, at pp. 545-546.

for because the digital signature process or system is an accepted technology. The same presumption holds true for other appropriate security procedures or devices that may be developed in the future.¹⁶⁰

VI.5.4. Disputable presumptions relating to digital signatures.

Upon the authentication of a digital signature, it shall be presumed, in addition to those mentioned in the immediately preceding section, that:

- a. The information contained in a certificate is correct;
- b. The digital signature was created during the operational period of a certificate;
- c. The message associated with a digital signature has not been altered from the time it was signed; and
- d. A certificate had been issued by the certification authority indicated therein.

These presumptions, which are based on commercial experiences, are necessary to help abbreviate the proceedings. Without these presumptions, the process of approving or verifying digital signatures becomes tedious and time-consuming.¹⁶¹

VI.5.5. Evidentiary Weight of Electronic Documents

In assessing the evidentiary weight of an electronic document, the following factors may be considered:

- a. The reliability of the manner or method in which it was generated, stored or communicated, including but not limited to input and output procedures, controls, tests and checks for accuracy and reliability of the electronic data message or document, in the light of all the circumstances as well as any relevant agreement;
- b. The reliability of the manner in which its originator was identified;
- c. The integrity of the information and communication system in which it is recorded or stored, including but not limited to the hardware and computer programs or software used as well as programming errors;
- d. The familiarity of the witness or the person who made the entry with the communication and information system;
- e. The nature and quality of the information which went into the communication and information system upon which the electronic data message or electronic document was based; or
- f. Other factors which the court may consider as affecting the accuracy or integrity of the electronic document or electronic data message.

Rule 7, Section 1 of the Rules on Electronic Evidence clarifies that matters relating to the reliability of the manner in which the electronic document was generated, stored or communicated, the integrity of the computer in which it is recorded or stored and other factors enumerated therein go into the evidentiary weight of the electronic data message or electronic document and not to its admissibility.¹⁶²

VI.5.6. Integrity of an Information and Communication system

In any dispute involving the integrity of the information and communication system in which an electronic document or electronic data message is recorded or stored, the court may consider, among others, the following factors:

- a. Whether the information and communication system or other similar device was operated in a manner that did not affect the integrity of the electronic document, and there are no other reasonable grounds to doubt the integrity of the information and communication system;

¹⁶⁰ Id., at p. 547.

¹⁶¹ Id., at p. 548.

¹⁶² Id., at p. 550.

- b. Whether the electronic document was recorded or stored by a party to the proceedings with interest adverse to that of the party using it; or
- c. Whether the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not act under the control of the party using it.

VI.5.7. Business Records as Exception to the Hearsay Rule

A memorandum, report, record or data compilation of acts, events, conditions, opinions, or diagnoses, made by electronic, optical or other similar means at or near the time of or from transmission or supply of information by a person with knowledge thereof, and kept in the regular course or conduct of a business activity, and such was the regular practice to make the memorandum, report, record, or data compilation by electronic, optical or similar means, all of which are shown by the testimony of the custodian or other qualified witnesses, is excepted from the rule on hearsay evidence.

Note that there is no requirement that the entrant has personal knowledge of the matter recorded or that he must be deceased or unable to testify.

VI.5.8. Overcoming the presumption

The presumption provided for in Section 1 of this Rule may be overcome by evidence of the untrustworthiness of the source of information or the method or circumstances of the preparation, transmission or storage thereof.

VI.6. Method of Proof

VI.6.1. Affidavit evidence

All matters relating to the admissibility and evidentiary weight of an electronic document may be established by an affidavit stating facts of direct personal knowledge of the affiant or based on authentic records. The affidavit must affirmatively show the competence of the affiant to testify on the matters contained therein.

Rule 9, Section 1 of the Rule on Electronic Evidence recognizes that the requirements for admissibility and the factors to be considered by the court for weight and sufficiency of electronic evidence require time and effort to be presented. To expedite proceedings, Rule 9, Section 1 allows affidavit evidence – which shall constitute the direct examination of the affiant.¹⁶³

VI.6.2. Cross-examination of deponent

The affiant shall be made to affirm the contents of the affidavit in open court and may be cross-examined as a matter of right by the adverse party.

VII. AUDIO, PHOTOGRAPHIC, VIDEO, AND EPHEMERAL EVIDENCE

VII.1 Audio, video and similar evidence

Audio, photographic and video evidence of events, acts or transactions shall be admissible, provided it shall be shown, presented or displayed to the court and shall be identified,

¹⁶³ Id., at p. 555.

explained or authenticated by the person who made the recording or by some other person competent to testify on the accuracy thereof.

VII.2 Ephemeral electronic communication

Ephemeral electronic communications shall be proven by the testimony of a person who was a party to the same or has personal knowledge thereof. In the absence or unavailability of such witnesses, other competent evidence may be admitted.

A recording of the telephone conversation or ephemeral electronic communication shall be covered by the immediately preceding section. If the foregoing communications are recorded or embodied in an electronic document, then the provisions of Rule 5 shall apply. It is not essential that the person who took the photograph, audio or video be the testimonial sponsor; any person who is competent to testify on the accuracy of such pieces of evidence can act as the authenticating witness.

VIII. TECHNIQUES FOR COLLECTING FORENSIC EVIDENCE

There are numerous techniques for collecting forensic audit evidence. These techniques build on contemporary audit techniques and include nuances and characteristics that especially enable them to acquire evidence that can be used in a judicial proceeding.

VIII.1. Document Examination and Analysis Techniques

Obtaining, reviewing, and carefully analyzing files or other records can uncover information that can shorten the audit/investigative work. An audit/investigation requires a thorough professional examination and analysis of all specific records and other documents associated with the suspected fraud. The purpose is to:

- a. Prove the extent of the loss.
- b. Establish the cause of the loss and the methods used, and
- c. Identify responsibility and possible knowledge of guilt.

This examination and analysis should cover all:

- a. Records of movements of assets or information during the period under investigation.
- b. The correspondence relating to these movements.
- c. Formal records handled by suspects.
- d. Private or informal records within the control of the suspects.

VIII.2. Examining Documents for Alterations

All relevant documents should be reviewed and analyzed by the auditors/investigators for irregularities. Documents are routinely altered to cover up or facilitate the commission of a fraud. Accordingly, the process of analyzing all relevant documents and records should focus on uncovering possible evidence of document alteration, manipulation, and forgery. Document alteration, manipulation, and forgery can take many recognizable forms including:

- a. Changed numbers, and erased or crossed out figures,
- b. Inconsistent inks, typefaces, and handwriting,
- c. The re-use, duplication, and writing-over of old documents,
- d. Edited and retyped pages in documents,

- e. Defaced documents,
- f. Forged approvals and signatures.

VIII.3. Detecting Forged Documents

Every auditor or investigator is not expected to be an expert in document examination. Audit organizations that conduct forensic audits should have access to the services of an expert document examiner, or include someone on the staff that is trained in that expertise. However, all auditors should be familiar with the techniques for recognizing documents that may have been forged, altered, or manipulated. The most common techniques used to detect documents that may have been forged include:

- a. Signature forgeries. Signature forgeries are recognized by irregularities in the written letters and differences in size from a genuine signature.
- b. Free-hand forgeries. Free-hand forgeries occur when the subject signs the name of another person without ever having seen a sample of the other's signature.
- c. Auto-forgeries. Auto-forgeries occur when an individual disguises his or her signature so that he or she, the one who signed the document, can attempt to deny having signed the questioned document. This type of forgery may be detected by examining each of the letters in the auto-forgery for similarities with the subject's signature, as well as the positioning, slant, or angling of the signature, and the pressure applied when the document was signed.
- d. Simulated and traced forgeries. Simulated and traced forgeries can be detected by superimposing two signatures in front of a light. If they are identical it is likely a forgery. Indentations and ink transfers from the tracing may be present.
- e. Substitute pages. Substitute pages can be recognized by holding the suspect pages in front of a bright light and observing differences in whiteness, density, thickness, opacity, and fiber patterns.
- f. Ink differences, alterations, and erasures. Ink differences, alterations, and erasures on paper can be recognized by holding paper in front of a bright light, or holding a light over the writings at differing angles. Reducing the light in a room and then holding a narrow-beam light low and parallel to the page surface can reveal indentations and other irregularities.
- g. Counterfeit documents. Counterfeit documents can almost always be recognized by comparison with the genuine documents.

The very act of altering a document may be sufficient evidence to demonstrate intent on the part of the individual suspected of committing fraud.

VIII.4. Document Analysis Techniques

There are a variety of analytic techniques that forensic auditors/investigators can use in examining documents and other evidence collected. They include:

VIII.4.1. Link analysis

This type of analysis analyzes the relationships or connections among people, businesses and organizations commonly used to detect bid-rigging.

VIII.4.2. Telephone records analysis

A branch of link analysis shows linkage between people and organizations through telephone numbers.

VIII.4.3. Flow analysis

Flow analysis documents the flow of events, of commodities, or of activities that occur when a fraudulent action is committed. The series of events that led up to a fraudulent action being committed can be analyzed to determine how the actions were planned, and executed.

VIII.4.4. Behavioral analysis

Behavioral analysis is used to determine a perpetrator's psychological profile as well as a perpetrator's motivations and potential victims. It provides the auditor or investigator with information about the type of person likely to commit a particular act. The auditor or investigator can compare such profiles with the profiles of those who could have committed the fraud, or use these profiles as guidance in identifying fraud-vulnerable situations.

VIII.4.5. Financial analyses

Net worth analysis, source and application of funds, bank record analysis, business record analysis, trend analysis, proportional analysis, and critical point analysis are some of the techniques used to analyze financial data.

- a. A *net worth analysis* uses proof of income from tax records, and other proofs of income and expenses, usually for three consecutive years, to determine if someone is living beyond their income limits.
- b. The *source and application of funds* technique is similar to net worth analysis in that it requires the auditor to collect data for four consecutive years to determine what someone's actual income was (source) and what that income was spent on (application.)
- c. A *bank record analysis* examines summaries of financial information from the bank to identify evidence of transactions needed to corroborate other evidence, or an individual or pattern of transactions that must be investigated.
- d. A *business record analysis* is essentially a focused, very specifically targeted audit of an organization's books and records. Unlike a typical audit however, it is a highly concentrated effort to uncover fraud in a very specific area. Accordingly, every aspect of all the analyses performed includes a determination as to whether evidence of fraud exists.
- e. A *trend analysis* is a diagnostic audit tool. Projections of future performance are analyzed and compared with previous performance. The technique is to chart the operating data for the period under examination against that of a previous period. Individual items of cost are compared and all variances investigated. It often reveals the first indication of inflated or depressed figures. It is important when using this tool that all evidence is fully corroborated by testing and inspection. This technique is particularly useful when applied to short periods of risk such as holiday periods and when applied to periods of high activity when controls would normally be expected to be under strain.
- f. *Proportional Analysis* is also an audit tool. The auditor/investigator seeks to establish the relationship between one set of costs and another, for example between freight and shipment of products, or between material used and product produced. The technique is to compare the relationship for the period under examination with that for a selected prior period. It can also be used to examine the relationship of what is happening with what should be happening, calculated on a standard basis. The

technique can also be used to measure performance in the period under examination against that of comparable organizations in the same sector.

- g. *Critical point analysis* is the process of isolating for detailed examination those transactions most vulnerable to fraud or manipulation. The technique is to filter out from the transactions passing through the organization, those with characteristics that identify them as being most vulnerable to irregularities so that these can be re-examined in detail. The filtration process examines all information in monetary or statistical terms and looks at particular risk areas. The technique examines specifically those areas that could be expected to arise from incorrectly handled or suppressed debits or credits and the areas where these would show discrepancies in the individual account statements.
- h. *Mail and trash covers* involves the accumulation and analysis of information obtained by the auditor/investigator from a suspect's mail and a suspect's refuse. Referred to as Mail Covers and Trash Covers, the auditor/investigator monitors the mail received by a suspect, and/or the trash disposed of by a suspect and then analyzes it for evidence.
 - A Mail Cover requires the auditor/investigator to intercept a suspect's mail, either at the suspect's home or at the suspect's place of employment and before the suspect receives it, and to determine the type of mail the suspect receives and who the suspect is receiving mail from. The mail is not opened, but the front and back of the missives are copied. That information is analyzed for use as evidence, or as leads to other sources of evidence. In no case should the auditor/investigator open the mail, delay the delivery of the mail, or otherwise interfere with the receipt of the mail by the suspect.
 - A Trash Cover requires the auditor/investigator to intercept a suspect's trash, either at home or at the suspect's place of employment and before it can be collected or disposed of. The trash is then analyzed for use as evidence, or as leads to other sources of evidence. Trash can be retained by the auditor/investigator as evidence.

The auditor/investigator must make certain, generally through advice from an attorney, that prevailing privacy laws will not be violated before using either of these two techniques, and /or that the evidence obtained can be used in court.

VIII.5. Laboratory Analysis Techniques

Laboratory analysis usually requires access to laboratory facilities and professional laboratory technicians. Few audit organizations have either the facilities or the expertise to perform a laboratory analysis. In that regard they must depend on the services of independent laboratories and technicians, or in the case of the government, access to government laboratories and technicians.

Laboratory analyses conducted by competent laboratories have been used successfully in testing the quality of vendor's products, in testing construction materials, and in food, water, and air quality testing. Laboratory analysis is often used to test disputed documents to determine whether they were forged or otherwise altered.

In computer fraud cases, forensic evidence may be required from expert witnesses in testifying to the intricacies of computer hardware or software and the forensic techniques used to gather computer related evidence.

VIII.6. Observations and Surveillance Techniques

The objective of any observation or surveillance is to visually see and hear precisely what occurs or what exists at a given point in time, and to record what happens, what does not happen and what is seen and heard or not seen or heard. It can be tedious and boring and, sometimes can be dangerous. These techniques can be an effective manner of collecting physical evidence.

VIII.6.1. Observations

An observation is a usual forensic audit technique. The auditor/investigator selects or determines the activity or location that must be observed and then arranges to observe it in an inconspicuous and in an unobtrusive manner as is possible. Care must be taken to assure that the presence of the observing auditor/investigator does not interfere with the way the activity being observed is being conducted.

The auditor/investigator then records and documents the observations made exactly as they took place and as they were being observed. Time, length of observation, place, weather conditions, the manner of observation, and any other pertinent information that would be a part of the documented observation. Photographs, drawings, and video and audio recordings help enhance and document observations.

So for example the auditor/investigator may decide that an observation of construction activities, specifically the number of construction workers working at the site, is appropriate. Or, the auditor/investigator may decide that the manner in which a particular construction technique is being performed should be observed.

VIII.6.2. Surveillance

Similar to observations, there are many techniques available to match varying surveillance requirements. Many of the basic techniques are simple, are not especially dangerous and can be adopted without specific training or prior experience. The more sophisticated techniques involving remotely controlled video recorders, and infrared cameras may require specialist skills.

It is critical to select participants for surveillance with great care, particularly for their suitability for a particular surveillance. It is important to define precisely the area or the activity or person that will be placed under surveillance, why the surveillance is necessary, and the length of time the surveillance will take place.

So for example an auditor/investigator may decide that surveillance should be conducted of the activities of someone responsible for inspecting construction materials to determine how inspections are carried out. Or the auditor/investigator may decide that a surveillance should be conducted, not only of the way inspections are being carried out, but also to determine the nature of the relationship the inspector has with the supplier of the materials, as well as the inspector's lifestyle. Each surveillance objective requires different surveillance techniques and different resources.

As with an observation, the results of each surveillance must be carefully and accurately documented.

VIII.6.3. Undercover Investigation Techniques

An undercover operation is a law enforcement technique, not generally used during forensic audits, whereby an operative, acting under an assumed identity is placed inside the suspected criminal enterprise or at a location where suspected criminal behavior is taking place. The perpetrators of the criminal enterprise are not aware that they are dealing with an operative. The primary purpose in utilizing this technique is to detect and expose the criminal activity by acquiring direct, relevant evidence for a criminal prosecution.

The undercover technique is generally used only in criminal investigations. Only special trained operatives should be authorized to participate in undercover activities. They should all be required to undergo specialized training.

The operative's assignment as to anonymity and the length of the undercover period must be scrupulously observed. Cover, including a past work history, an assumed name, a driver's license, an identity card, a passport, and other such identifying documentation must be established for the undercover operative. Any departure from the agreed assignment or any attempt to make contact with the undercover investigator can frustrate the investigation and could endanger the investigator.

This is specialized surveillance technique and should not be attempted by anyone who is not specifically trained in the technique. It should only be adopted when there are well-founded suspicions of a major fraud involving a number of people and a significant risk to the organization.

VIII.6.4. Modified Undercover Techniques

Auditors, especially forensic auditors, sometimes use a modified undercover technique, sometimes called a ruse or a form of subterfuge, to obtain evidence. This form of undercover technique requires little training but does require extensive preparation and planning.

For example, a modified undercover operation could require a forensic auditor/investigator to assume the role of an applicant for a license to determine whether a bribe is required for the approval of the application or the granting of the license. Or a forensic auditor/investigator could assume the role of a participant in a training program to determine whether the participants were encouraged by the instructors to violate laws or regulations, or a forensic auditor/investigator, acting as a prospective supplier, contractor, or vendor, can attempt to determine whether a procurement official is amenable to a kickback.

It is important in preparing and planning for the use of a ruse, or this *modified undercover technique*, that the forensic auditor/investigator receives legal advice from the attorney as to the manner in which the technique can be carried out so as to assure that the evidence obtained can be used in a court of law.

VIII.7. Interviewing Techniques

All the evidence needed to demonstrate that a fraud may have been perpetrated will not necessarily be in documentary, physical, or analytic form. Testimonial evidence obtained from subjects, witnesses, and others can contribute substantially to the investigation. Information will usually be required from witnesses, subjects, and others to place the documentary, physical, and analytic evidence in an appropriate perspective. In addition testimonial evidence is vital in corroborating and verifying the integrity of the other forms of evidence already obtained.

Auditors/investigators must be familiar with the interview technique and highly proficient in its use. A successful audit, especially a forensic audit cannot usually be conducted without the extensive use of interviews. Much of the evidence gathered in a forensic audit/investigation originates with interviews.

VIII.7.1. General Interviewing Guidelines

There are some general rules that should serve to guide all interviews and the collection of testimonial evidence by auditors/investigators:

- Interviews are generally conducted in a non-custodial setting. Interviewees must voluntarily consent or agree to be interviewed. While they may be asked by the auditor /investigator to agree to be interviewed, an interviewee always has the option of not consenting.
- Interviewees are always generally free to terminate the interview; they are not in custody. Care should be taken by the auditor /investigator to assure that the interviewee understands that his or her freedom is not being restricted. During phases of a criminal investigation interviews are often conducted in a custodial setting. This means that the interviewee is in custody, the interviewee's freedom is restricted, the interviewee is not free to terminate the interview, and the interviewee may have the right to legal counsel and afforded other constitutional protections...
- Interviews should not be conducted by more than two auditors /investigators. Interviewees are often intimidated by the interview itself and the presence of more than two auditors /investigators tend to exacerbate that feeling of intimidation.
- All interviews must be thoroughly planned. The auditor /investigator should know well in advance of the interview as much as possible about the interviewee and about the subject of the interview, and should know the specific questions that will be asked during the interview.
- The auditor /investigator must not unnecessarily disclose the identity of their information sources. Often witnesses and other interviewees are reluctant to provide information or even consent to an interview unless they believe that the information they are providing and their identity will be kept confidential. The auditor /investigator must take great care in assuring interviewees that the information they are providing will not be unnecessarily associated with them. It may be necessary to seek legal advice to confirm the extent of anonymity that the auditor/investigator may grant.
- Auditors/investigators should not rely on volunteered and uncorroborated information, but should not ignore it either. Volunteered information can sometimes provide the auditor /investigator with leads that might otherwise have not been discovered. Cooperative interviewees can often be the source of valuable information. Uncorroborated information may also be useful in developing leads to evidence that may contribute to the auditor/investigator's case. Evidence, before it can be completely relied on, should always be corroborated to the extent possible.
- An interviewee's first response to a question should never usually be accepted. When something sounds wrong or implausible, the auditor/investigator should discretely persist until a satisfactory answer is obtained, or until it is believed that an answer will not be forthcoming. When something sounds right, the auditor/investigator should confirm the response with additional questions asked in a different manner.

- The skilled interviewer should get to know the witness or subject over one or more interviews. Knowing the interviewee enables the interviewer to assess the reliability of the answers being provided and facilitates an assessment of the integrity of the testimonial evidence.
- A note conveying the auditors'/investigators' professional observations should be included in the record of the interview. Observations such as the witness's or subject's character, reliability, and likely performance in court may assist the attorney who ultimately presents the case in court.

VII.7.1.1. Interviews with Witnesses

Witnesses should always be interviewed in complete privacy. If the witness is an employee and the interview is being conducted in the work place, the interview should always be conducted well away from fellow employees. No one but the interviewee and the auditors /investigators should know that the interview is taking place. Many interviews of witnesses take place outside the workplace, but the same general rule applies as to privacy regardless of where the interview takes place.

Care must be taken to ensure that the interview is not interrupted. If the interview is being conducted in the work place it should be carried out in a quiet place away from all distracting sounds of normal office activity. Telephones should be ignored or even disconnected.

The witness must have the opportunity to tell his or her own story and respond to questions in his or her own way. The forensic auditor/investigator must be alert to the possibility of distorted or false information from a witness with a prejudiced or biased viewpoint precipitated by jealousy, spite, or some other self-serving motivation. It is not uncommon for a witness to view the interview as an opportunity for a vindictive attack or to promote his or her own agenda.

VII.7.1.2. Interviews with Suspects

In preparing for an interview with someone suspected of perpetrating a fraud, the auditor/investigator should always confer with the attorney assigned to the case. In addition, an outline of the questions to be asked can also be discussed with the attorney.

The interviewer should be prepared for both affirmative and negative responses to key questions and should avoid creating the impression that the purpose of the interview is to seek a confession or admission of guilt. Remember that the suspect is not under custody and should be allowed to terminate the interview, or have the assistance of his private counsel if he requests it.

It is preferable for the interviewer to assume the role of one seeking the truth, essentially the facts as the interviewee knows them. The interviewer should be tactful when replies to questions do not agree with the facts as the interviewer knows them and should avoid emphasizing any inconsistencies noted during the interview. The interviewer should continue to ask for additional information in such cases.

The auditor/investigator conducting an interview should listen carefully to whatever the interviewee has to say and then relate questions to specific transactions and documents of interest. The skill of the interviewer is a determining factor in obtaining information useful to the investigation.

VII.7.1.3. Choosing Question Types for Interviews

The key to a successful forensic audit interview is to use one or more interview techniques, relying on the auditors/investigators ability to size up the interviewee, and determine the

approach that will work best. auditors/investigators when interviewing witnesses, suspects, or anyone else should carefully organize their interviews following some very well phrased question types.

For example:

- a. **Open-Ended Questions**-This type of question is broad and unstructured, letting interviewees give answers as they see fit. Open-ended questions are intended to establish good communications and obtain the viewpoints of the interviewee.
- b. **Restatement Questions**- The purpose of a restatement question is to verify and understand what was said and to encourage the interviewee to continue to respond. The interviewer takes a statement that the interviewee has just made and rephrases it as a clarifying question.
- c. **Probing Questions**- The purpose of a probing question is to obtain more specific information about an answer that has been given in response to an interviewer's question. The interviewee is asked to explain in more detail the response given to a specific question.
- d. **Closed-Response Questions**- This type of question is used when the interviewer wants to limit an interviewee's options in responding to a question. For example an interviewer may ask, "Do you record transactions daily or wait until the end of the month?" The use of closed questions requires the interviewer to have background knowledge of the subject. This method is useful when it is desired to have the interviewee think through alternatives and arrive at a response.
- e. **Yes-No Response Questions**- This is a form of a closed ended question that allows the interviewee to answer either "Yes," "No", or "I don't know." This type of question does not elicit much detailed information, but is useful in obtaining very specific information.

VII.7.1.4. Confessions and Admissions of Wrongdoing During an Interview

It is advisable for the auditor/investigator to be guided by competent legal advice from the attorney regarding the conduct of any interview with an individual suspected of involvement in fraudulent activities. This is especially important if it is anticipated that a confession or an admission of wrongdoing might be forthcoming.

It is particularly important to ensure privacy, absence of distractions and interruptions and for the interviewer to maintain control of the interview. All admissions, to be admissible as evidence in court, must be freely made, with no indication of coercion, pressure, or threats. Subsidiary aims when interviewing a suspect may include establishing the method used to commit the fraud, identifying accomplices, and the part played by accomplices and others.

It is important to remember to document and authenticate confessions or admissions of wrongdoing. One way is to request the interviewee to write down his confession and swear by it before an officer with authority to administer oaths. Another way is to record statements by means of an audio or audio-visual recorder, provided that the consent of the interviewee is categorically explained. The auditor may accomplish this by activating the recorder and, on record, categorically asking the interviewee whether he agrees to the recording and its disclosure to lawyers and courts and other relevant third parties such as other investigators. If the response is in the negative, the recorder must immediately be switched off. Failure to do this will expose the auditor/investigator to liability for violation of R.A. 4200, as amended, also known as the Philippine Anti-Wire Tapping Act. The interview may then continue if the

interviewee wishes, and documented by written means discussed above. Otherwise, the recorded interview may continue. The auditor/investigator would have to testify later on before an administrative tribunal or trial court as to the circumstances of the recorded interview (i.e., the time, place and the conduct of the interview).

Another way to document and authenticate the confession and/or admission is for the auditor/investigator to execute a sworn statement as to the circumstances and substance of the interview. This will again require the auditor/investigator to testify before an administrative tribunal or trial court (see discussion under Section 8.8 under this Chapter).

VIII.7.2. Preliminary Interview

There will usually be a preliminary interview, or a series of preliminary interviews with any suspected party, conducted much like a witness interview. At this interview, the activities for which the interviewee is responsible should be identified. The interviewer should seek to obtain an original explanation of events for comparison with known facts and subsequent statements.

VIII.7.3. Final Interview

If conducted, the purpose of this final interview is to attempt to ultimately obtain an admission of guilt (see discussion above regarding interviewing a “suspect” and documentation and authentication of confessions / admissions). In most cases, the evidence needed for referral to a prosecutorial body or criminal investigative organization should have already been developed. It is particularly advisable to conduct this interview on a one-to-one basis and only with the advice of an attorney.

The auditor/investigator must emphasize that the sole objective of the interview is to discover the truth. The interviewer should remain calm and polite at all times and avoid any manifestation of emotion. The interviewer must be particularly careful to use language that is simple, direct and unambiguous. Care must be taken to ensure that the suspect understands what is being asked. It is especially important not to use emotive words or phrases. Provocative words like “fraud, lie, steal, or thief” are likely to be perceived as assertions of guilt and must be avoided. Again, the suspect or any other interviewee for that matter is not under custodial investigation and should be allowed to terminate the interview, or have the assistance of his private counsel if he requests it.

VIII.8. Records of all Interviews Must be Prepared

A standard format should be used by auditors/investigators for documenting all interviews and for preparing a record of all interviews that take place. This will assist in the analysis and collation of testimonial evidence and prepare the records for examination by an administrative tribunal or trial court. A written record should include the following information about the interview:

- The time of the day it took place,
- How long it lasted,
- Where it took place—the location,
- The date it was conducted,
- Who was present at the interview,
- The reason the interview was conducted, and
- Any follow up issues that must be addressed by the auditor/investigator.

IX. ORGANIZING AND DOCUMENTING THE WORK PERFORMED

Forensic auditors/investigators must take extreme care to carefully document and organize all the work performed and the evidence collected and to handle records in an appropriate manner in accordance with the requirements for establishing a chain of custody for evidence. (See discussion under Section 9.2. of this Chapter on the Chain of Custody And The Care Of Forensic Evidence)

If a matter does eventually come before the court, defense attorneys can destroy an otherwise well-constructed body of evidence by pointing out, for example, that some audit working paper notes are neither signed nor dated and not prepared in accordance with prevailing audit standards, or that a computer file was not properly copied or tested for completeness or accuracy, raising the question of the possible alteration or lack of reliability of the records.

Every investigation eventually results in a written report. It may be a report to management on the causes and methodology of the probable fraud with recommendations to management for preventing recurrence. Alternatively, it may be a statement of the evidence uncovered supporting a full and detailed description of what happened, intended as a brief to be used by a prosecuting attorney for legal presentation during a criminal proceeding.

It is essential, both for the security of the investigation and for a successful outcome that all the evidence collected be maintained in an orderly and sequential fashion and in accordance with the protocols established for the evidence, i.e. chain of custody. This will facilitate preparation of the final report and ensure that nothing of importance is overlooked. It also enables the work to continue if for any reason there has to be a change in the audit/investigative team.

Spiral-bound index books are suitable for making a permanent record of all interviews in sequence as they occur, with appropriate references to all relevant documentary evidence. All audit working papers, including those that reflect the initial conclusion of probable fraud, must be prepared in accordance with prevailing audit standards.

IX.1. Collecting and Maintaining Documents

The collection and maintenance of documents collected, as evidence is an essential aspect of any audit/investigation. The following should be used as guidance:

1. The first rule in a forensic audit/investigation is to obtain all the documents that might possibly be relevant to the audit/investigation. Any documents subsequently found not to be required can be returned. Documents not collected but later needed may by then have been destroyed, mutilated or removed, and valuable evidence lost.
2. As with the preparation of working papers, a system must be devised by the audit/investigative team for cataloging and classifying all documents collected. (See Section 9.2 of this Chapter on Chain of Custody.) At a minimum all documents collected should be listed, stating the place where the document was found, the name of the person who removed it, and the date of removal.
3. Documents already bound in binders or bundles should not be separated, but the contents of each bundle should be listed, identifying each separate document.

4. All documents collected should be copied front and back and only the copies used as working documents. The originals should not be marked or written on or fastened together. They should be kept secure and separate from the copies and beyond the reach of suspects.
5. Detailed notes of document examination should be compiled as a permanent record in an investigation notebook. No original document that is relevant to the investigation should be returned until after the investigation and after the resulting proceedings have been completed.
6. Documents are generally admissible as evidence if properly authenticated. The authentication requirement is met by offering proof that the document is in fact what the person offering it says it is. Courts routinely allow the use of copies of routine documents as evidence. However, the originals of critical documents, essential to the fraud case, should be produced in their original form for the court.

IX.2. The Chain of Custody and the Care of Forensic Evidence

Generally forensic evidence collected during a forensic audit takes the form of documents, photos, or other objects. That evidence should be marked, identified, inventoried, preserved, and safeguarded in a controlled location, such as a safe or double locked file cabinet with access restricted and controlled.

This process will serve to maintain the evidence in its original condition and establish a clear chain of custody until the evidence is introduced into a judicial proceeding as evidence. Any gaps in the chain may cause the evidence to be challenged by the defense on the basis of its susceptibility to compromised authenticity and integrity. The courts may allow a document as evidence for which a chain of custody has not been established. If a document, such as a business letter or contract, is readily recognizable by the witness without having to account for its storage and handling.

A seized document, to be used as evidence, must be proven to be the same document that was seized and in the same condition. In addition, the custody of the seized document must be established from the time of seizure to the time it is placed in evidence in the court.

IX.2.1. Marking seized documents

When a document is seized, the investigator must identify the document with an appropriate marking:

- a. The investigator or auditor's name /initials, and date of seizure can be placed in the margin, on a page corner, or on the back of the document, or
- b. The document can be copied for use and reference during the investigation. The original can be placed in an envelope, the investigator or auditor's name /initials, and date of seizure on the envelope should be written on the envelope, the envelope should be sealed, and the envelope secured in a custodial, controlled environment.

In collecting forensic evidence the auditor/investigator should remember:

- a. To always keep in mind the legal admissibility of the evidence. Can the evidence be absolutely validated and attested to as original, unaltered, and not compromised evidence?
- b. Photographic evidence requires special care. The photographer should be identified, the time and place each photo was taken should be recorded, a log should be maintained as to the transfer of the film to the developer, the identity of the developer

of the photos must be a matter of record, and the secure custody of the photographs maintained.

- c. A log must be maintained of how and where all evidence was obtained.
- d. Notes should be hand-written.
- e. Verbatim transcripts of important discussions with key officers should be prepared.
- f. Original documents should be protected and secured.
- g. Photocopies of seized key documents can be annotated and placed in official files if they are needed for the conduct of regular business.
- h. Originals of key documents should not be marked in any way, except to record their seizure.

CHAPTER V. INTERIM AND FINAL INVESTIGATION REPORTS; TESTIFYING IN COURT

In addition to conducting routine oral status briefings for the head of the forensic audit/investigation team, and legal counsel who is a member of the team, an interim report should always be ready and up-to-date depending on the status of the audit/investigation. The interim report can provide an up to date synopsis of the case and provide a useful opportunity for the head or the legal counsel to provide advice on the direction and/or form of the investigation. It will also ensure continuity and currency of the audit/investigation despite death, resignation or termination of any member of the audit/investigation team.

All fraud reports should be organized according to the elements of proof. For example, in bribery case the report should contain clear and convincing evidence beyond a reasonable doubt that the perpetrators:

- Gave or received,
- Something of value,
- With corrupt intent,
- To influence a decision,
- Without disclosure to the recipient's employer.

I. INTERIM REPORT PREPARATION GUIDANCE

As a guide in preparing an interim report, the evidence collected to answer the following investigative questions should be highlighted in the report:

- a. What were the improper, illegal practices or inappropriate behaviors that were engaged in or otherwise carried out? Evidence must show that illegal, improper practices were carried out.
- b. Were these practices or behaviors intentional? Evidence must show that the practices were carried out intentionally.
- c. Were these illegal, improper practices or inappropriate behaviors carried out through the misrepresentation of material facts in order to deceive? Evidence must show that the practices were facilitated by misrepresenting fact.
- d. Did the victim rely on the misrepresentations? Evidence must show that the victim relied on these misrepresentations.
- e. Did the illegal, improper practices or inappropriate behaviors result in injury or damage? Evidence must show that the practices caused damage or injury.
- f. Did all parties to the transaction benefit? Evidence must show that the practices benefited the perpetrators.

To help in the understanding and appreciation of the magnitude of the fraud, and assess the likelihood of a referral to other investigative agency/ies, interim reports could also include such information as:

- a. Nature of the fraud
- b. Actual or estimated amounts of money involved
- c. Location where the fraud occurred

- d. Type of activity
- e. Means by which the fraud was identified
- f. Formal history of the matter within the Ministry
- g. Name(s) and details of the individual (s) involved
- h. Explanation of the circumstances of the fraud
- i. Action taken (including method of investigation), facts uncovered, present status of employee and steps taken to protect company assets from further loss
- j. Indications whether the most recent audit of the location uncovered any circumstances that might have indicated that a fraud was in progress
- k. Further action or investigation required to complete the investigation
- l. Expected investigation completion
- m. Final reporting and referral to appropriate investigating authority time-frame

Care should be taken to ensure that any interim reporting practices do not cause delays in the audit/investigation or cause premature conclusions to be reached. Oral interim reporting arrangements may be suitable in some situations.

II. FINAL REPORTS

A final report should be forwarded to the head of the audit/investigation team, the legal counsel, and, especially, the appropriate Disciplining Authority / Investigation Authority, as the case may be. It is recognized that a realistic standard in this regard may depend on a number of factors. The reporting format for final reports is a matter for the auditors/investigators to determine. However, the information provided in the final report could include:

- a. Who carried out the investigation? And when?
- b. Existence of confirmed fraud and its location
- c. Amount involved
- d. Name and position of employee(s) and non-employee(s) involved
- e. Personnel information
- f. Methods used to detect the fraud
- g. Time period over which the fraud occurred
- h. How the fraud was disclosed
- i. A statement as to whether there was:
- j. An absence of internal control
- k. A circumvention of internal control through collusion
- l. Effective internal control
- m. Steps taken to prevent recurrence
- n. The names of the insurance companies and other persons from whom recoveries were made and amounts recovered
- o. Copy of any statement made by employees'
- p. Current employment status of those involved.
- q. Property and/or funds recovered
- r. Any arrangements made for restitution
- s. Disciplinary action taken or proposed
- t. Probable result of any police action or planned prosecution
- u. Overall costs and time frame to conduct and finalize the investigation.

It is also imperative that a follow up review at some future point in time is conducted to ensure recommendations have been implemented and are working effectively to prevent any reoccurrence of fraud.

Ultimately, a forensic audit can result in a conclusion that fraud may have occurred and referred in report form to the appropriate persons. The final report should be carefully organized, and should clearly present the evidence collected according to each element of proof, especially knowledge and intent. The report should not be cluttered with minor details, unnecessary information, or charts, graphs or audit work papers unless absolutely essential.

All final reports should be thoroughly reviewed by an attorney familiar with Philippine law and the case. The attorney's review should include a determination that the evidence has been collected in accordance with the law and that it is sufficient to demonstrate evidence of wrongdoing. The final report should generally be confined to the following components:

- a. What were the improper, illegal practices or inappropriate behaviors that were engaged in or otherwise carried out? Evidence must show that illegal, improper practices, that is, practices that are contrary to laws and regulations were carried out.
- b. Were these practices or behaviors intentional? Evidence must show that the practices were carried out intentionally.
- c. Were these illegal, improper practices or inappropriate behaviors carried out through the misrepresentation of material facts in order to deceive? Evidence must show that the practices were facilitated by misrepresenting facts.
- d. Did the victim rely on the misrepresentations? Evidence must show that the victim relied on these misrepresentations.
- e. Did the illegal, improper practices or inappropriate behaviors result in injury or damage? Evidence must show that the practices caused damage or injury.
- f. Did all parties to the transaction benefit? Evidence must show that the practices benefited the perpetrators.

III. TESTIFYING IN COURT

Auditors' working papers, prepared during the course of an audit, are often used in a court of law as evidence. The auditor who prepared the working papers can also be required to testify as an expert witness. In addition, the forensic auditor/investigator who conducted the forensic audit/investigation may also be required to provide testimony as an expert witness. Unless the court acknowledges that the witness is testifying as an expert witness, all testimony by the auditor/investigator should be limited to facts, and based on direct knowledge. Only an expert witness can provide an opinion based on the witness's expert knowledge of the subject.

To be an effective witness the forensic auditor/investigator must be prepared to respond successfully with the defense attorney's questioning. There are some basic rules that the auditors/investigators should observe that will help them withstand any attempts to discredit their testimony and the evidence they provide. The auditor/investigator should:

- a. Rely on the strength of your direct testimony; do not contradict your direct testimony. Make certain that you have reviewed all pertinent documents, and are thoroughly familiar with all the evidence before testifying
- b. Not give the defense attorney any new or additional defensive theories or ideas when responding to questions.
- c. Not give the defense attorney any reason to cast doubt on your testimony or on the evidence you have presented. Listen carefully and fully to the defense attorney's questions and assure that you understand them before you answer. Leading questions by defense attorneys sometimes include assumptions that, if answered, imply an acceptance with those assumptions. Make certain if that question format is used, that

you carefully consider whether or not you agree with those assumptions before answering.

- d. Not argue with a defense attorney. Defense attorneys argue for a living and are good at it. If a witness engages in argumentative dialogue with a defense attorney, the witness has a very good chance of losing. Ignore any attempts by a defense attorney to draw you into an argument.
- e. Answer only the question that is asked and stop. Provide the defense attorney with only the answer to the question asked and no more. Providing more information than is asked for, may jeopardize your testimony and create doubts about your evidence.
- f. Control the pace of your testimony. There is no need to adopt the defense attorney's pace and respond immediately to a question. Defense attorneys often attempt to string together long statements, position, and arguments and then immediately ask a question that requires a "yes" or "no" answer. Take the time to completely understand the question and to slowly and carefully think about the answer before you respond. If you do not understand the question, ask the attorney to repeat, re-ask, or rephrase the question. When a question requires more than a "yes" or "no" answer, think carefully about your response and take all the time you need to reply.
- g. Examine all the documents and the other tangible evidence that a defense attorney may refer to when asking a question. Do not rely on your memory or your recollection of any evidence being used by the defense attorney to ask a question. Examine the evidence and make sure it is what the attorney says it is and that it is relevant to the attorney's question before you answer.
- h. Never guess or speculate to provide an answer even if the attorney asks you to. It is perfectly permissible to say you do not know.
- i. Never provide an answer to a question beyond your level of expertise. Every question asked by a defense attorney is designed to cast doubt on both your testimony and the evidence.
- j. Pay careful attention to the actions of the State's attorney during your testimony. The State's attorney or prosecutor may only have limited ability to object to the questions raised by the defense attorney. When the State's attorney does raise an objection or makes a statement during your testimony, listen carefully to those statements. The statements will usually have some instructional information for you or a warning about the defense attorney's line of questioning.
- k. Be mindful at all times that you are in a court of law. Your conduct and demeanor should be professional at all times. A relaxed and casual attitude can have a negative impact on your persuasiveness, as well as on your ability to focus on the testimony that you are delivering.
- l. Practice and prepare for your testimony. In anticipation of providing testimony, you should become thoroughly familiar with all the documents and all the evidence that will be presented. In addition, a good practice technique is to arrange to have several attorneys with differing styles question you about the important aspects of your testimony and the evidence that will be presented in court.