**THE INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS OF PAKISTAN (ICPAP)**

**(Suggested Solution)**

| | | | |
|---|---|---|---|
| Stage | **Specialization** | Course Code | **SP-612** |
| Examination | **Summer-2012** | Course Name | **Fraud Investigation and Audit** |
| Time Allowed | **03 Hours** | Maximum Marks | **100** |

**NOTES:**

1) Attempt 5 out of 6.
2) Answers are expected to the precise, to the point and well written.
3) Neatness and style will be taken into account in marking the papers.

Question No 1:-

What you mean by Opinion Testimony. Also explain the Exceptions to the opinion Rule.

Answer:-

Opinion Testimony

Generally, lay (i.e., non-expert) witnesses are only allowed to testify about what they have actually experienced firsthand, and their factual observations. Witnesses provide a report on what they know, and keep their opinions and conclusions to themselves.

Exceptions to the Opinion Rule

NON; EXPERT WITNESSES

Despite the general rule, there are ways to get a non-expert witness's opinion into the record. For example, an employee at a securities f1rtn blows the whistle on his superiors for a high- level stock fraud. Defense suggests the investigation was an invasion of privacy, Prosecutors are justifying their secret eight month investigation on the basis of the whistleblower's tip, the prosecution will enter the whistler's "opinion" and his suspicions of fraud to show that the government was justified in conducting its investigation. In this case, the opinion is admissible; however, the reason it is allowed in is not to show that management is guilty, but to show what prompted the investigation.

Opinions are admissible if they pass a three-part test:

Does the witness have direct personal knowledge of the facts to which the opinion pertains?

Is the opinion of the common, everyday sort, i.e." does not involve specialized knowledge or tests?

Is the opinion NOT part of a level judgment, reserved for the jury or judge to decide?

Opinions from ordinary witnesses must be based on personal experience and have some bearing on the facts (as opposed to the judgment of the case. This distinction is further refined in situations involving hearsay and personal judgment, discussed below. Expert witnesses are exempt from the opinion rule, since experts are hired to render a professional opinion.

## EXPERT WITNESSES

Expert witnesses are allowed to give opinion testimony because they possess education, training, skill, or experience in drawing conclusions from certain types of data or information that lay witnesses do not possess. However, expert testimony may be excluded if it embraces a legal conclusion. Therefore, expert opinions addressing or innocence will likely be excluded in criminal cases.

### Exhibits

Exhibits are the tangible objects presented as evidence. Therefore, both real evidence and demonstrative evidence are entered into the record as exhibits. This includes documents like contracts, letters, and receipts; plus photographs, X-rays, baseball bats, knives, fountain pens. In short, anything that is not testimony is an exhibit Testimony is what people say. Exhibits are the "props."

### Demonstrative Exhibits

An exhibit used for purely "illustrative purposes" is a type of demonstrative evidence. Demonstrative evidence includes charts, and summaries that help to simplify complicated evidence for the jury. Such evidence is admissible if the court decides that it presents a fair and balanced summary or picture of the evidence and is not unduly prejudicial.

In complex fraud cases, such evidence is extremely useful, but care should be taken to keep the charts and exhibits simple. The evidence that is summarized must be made available to the other party, and the court may order that the underling document may be produced to the court.

### Authenticating Typical Exhibits

At the most basic; level, evidence must be established as reliable or authentic. Thus, evidence, other than testimonial evidence, must be properly authenticated; that is, the party offering the document must produce some evidence to show it is, in fact, what the party says it is. If a piece of real evidence cannot be authenticated, the evidence Will not be admitted, even if it is plainly relevant.

Similar to the authentication requirement for evidence, there is a sinlilarsort of "credibility test' for witnesses. If testimony is to become admissible evidence, the witness must demonstrate that the knowledge being communicated is believable and made by personal experience.

Question No 2:-

How successful Investigation is performed? Also explain the steps of Investigation process.

Answer:-

Guidance for Conducting a Successful Investigation

1. Do not 'go it alone' if you can avoid it. Good investigation requires discussion and it is all too easy to agree with yourself! Different type's people see things from different perspectives and in investigation you want to make use of this.

2. Remember to think things through before you begin. Do not rush in to interview witnesses or walk the site until you have decided what should come first and who is going to do what.

Gather your thoughts. Discuss with your 'team.' Find witnesses and make arrangements to interview them properly. Decide carefully when you will do the various necessary tasks.

3. Organise who will be responsible for all the information you will collect and which you will need for your analysis. If this is yourself, then set up a simple but effective system for storing and keeping it safe. Make sure none of your data is lent out or left lying around.

4. Set up your 'investigation headquarters' right away. This may sound 'over the top' but it isn't; you need somewhere to put up your Storyboard and Analysis charts so that you can come back to your investigation each day in an orderly way. Even small incidents or near misses (hits) could have been much bigger events; the reason you are investigating is to identify actions which could prevent a much more serious occurrence. Your investigation is extremely IMPORTANT no matter what size the incident.

5. As you gather your data, put it right away onto Post-its and then the Timeline chart. That way you can see in front of you what is emerging. And you can discuss your findings so far with your colleague/team. Using Post-its like this allows flexibility; nothing is fixed. You can move them around– or take them off the chart altogether.

6. Make sure that everyone feels able to input information. TOP-SET® has 'difference' at its core. Make use of this. Be open and accepting. What seems obvious is rarely the answer.

7. Do not discount the apparently naive idea. The non-expert too can have a very valuable contribution just because they can see with fresh eyes. Is there anyone in your office/establishment whom you have not thought of who could contribute well to the investigation?

8. Arrogance and bullishness have no place in investigation; each individual has equal value in this process. Often the quieter individual, the one who is listening, comes up with the gem.

9. Listen to others. Sometimes someone else's idea triggers something in your own mind. It's OK to piggy-back on the ideas of others.

10. Be open minded; it is dangerous to be fixated on any idea. Use the TOP-SET® indicators to direct you in different directions. Allow them to stimulate your own thinking. Remember, you are looking for truth, not convenient coat-hangers. And sometimes you just have to live with uncertainty. A good investigator can do that and can base their recommendations on what they have found without needing A SINGLE ANSWER.

## Steps for Investigation process

### Planning

Effective planning is a key component of any successful investigation: it will help you define the parameters of your investigation and keep you focused on what is relevant. We recommend drawing up a standard investigation plan at the start of every investigation, capturing the key issues and structuring your actions.

Of course, you cannot ever predict with certainty what direction an investigation will take.

During the course of the investigation, you may uncover issues that require further research and consideration, and could result in significant revisions to your plan. Even so, a good initial plan will help to reduce the disruption of unforeseen circumstances and keep your investigation focused.

The sample plan at the back of this guide might give you some ideas. At its most fundamental, the plan should include the following sections.

### The allegation

A good investigation plan starts with a precise definition of the allegation. Knowing exactly what you are trying to establish will help you focus. Ambiguity about the exact nature of the allegation may cause difficulties later on in the investigation.

If you need clarification on any facts of the allegation you can approach the complainant.

You are required to tell the complainant that you have received the matter for local investigation, so this might be a good time to check any details

### Relevant parts of the Code

It is useful to list the parts of the Code of Conduct that may have been broken, to help you focus the investigation in the right areas. We have found that one of the greatest dangers is becoming distracted by issues that only serve to muddy the waters and increase the amount of time and effort spent on an investigation.

### Information

The complaint sometimes comes with a great deal of documentary information which you will need to sift through, recording the relevant parts on your plan.

From this, you should be able to work out what further information or evidence is needed to determine whether the alleged conduct occurred. Be as focused and precise as possible: being clear about what you need to know at this stage will help you avoid delays and distractions later on. You may find it helpful to produce a checklist of the elements that need to be proved.

### Action plan

Set out how you intend to obtain the information you need. Your plan should include the witnesses you intend to interview, the order in which the interviews will be conducted, the questions you need to ask and the areas you need to cover. It should also include any documents, you need to obtain and any site visits you think would be useful.

It is usually best to secure all relevant documents before beginning the interviews as they may have an impact on the questions you want to ask. You should also consider what documents if any, you may wish to give to the interviewee before the interview.

### Resources and targets

At this stage, you should have a reasonable idea about the resources needed to complete the investigation, such as time and expenses. Record them on your plan and make sure they are available to you.

We also recommend that you include target dates for completion of the various stages of your investigation and an overall target date for completion of the final report.

### Establishing facts

In the vast majority of investigations, you will need to gather documents and conduct interviews to establish the facts of a case. This section considers how to go about it.

## Gathering documents and background information

You will need to obtain the background information and other documentary evidence you have identified as relevant to the investigation. You may also wish to get written statements from witnesses, although these are usually only successful where the information you are seeking is very straightforward. They will not be helpful where you need to probe the answers given for further information, test an individual's responses, or where there is some doubt about the credibility of an individual's account of events.

## Requests for information should:

- be made in writing
- explain the reasons for your request
- be precise about the information you need
- set a deadline for responding

You may wish, at this stage, to ask people to let you know if they are likely to be late responding. Ask them to explain any delays and agree a new deadline. It may also be helpful to give a copy of the letter to your chief executive, in case you need their help persuading people to co-operate.

It's important you contact anyone who missed the deadline straight away to ask them when the information will be provided. Do not accept vague promises; insist on a precise date. You may even want to offer to have it collected and agree a date and time for this.

Getting information from your own authority and other local authorities should be quite straightforward. These bodies have a statutory duty to provide the information you require and ethical standards officers are unlikely to refer cases to you for local investigation if they believe you will need information from other sources.

## Conducting interviews

You should already have identified the people you need to interview and the areas you need to cover for your investigations plan, and considered the order in which they should be approached.

As a rule, you should plan the order of your interviews so that each witness is interviewed only once, although repeat interviews are sometimes unavoidable.

Interviewing the member who is the subject of the investigation first may save you a lot of time if, for example, they admit to the alleged breach of the Code of Conduct. It may also help you establish which facts, if any, are disputed. However, you may learn things during other interviews that you need to discuss with the subject member, requiring a second interview. If you think this is likely, you may wish to leave the subject member's interview until last. Alternatively, to help manage the subject member's expectations, you could explain at the start of the first interview that there may be a need for further interviews.

You also need to consider whether to conduct the interview in person or over the telephone. With face-to-face interviews, you should agree a time, date and venue for the interview in advance, and confirm these details in writing. You can also use this letter to remind members being investigated that they may wish to have legal representation, and advise interviewees if the interview is to be recorded. Some interviewees may prefer to be accompanied by a friend or colleague. This should not present a problem as long as the companion is not connected with the investigation in any way — for example, someone the member is accused of trying to secure an advantage for.

For telephone interviews, people may be happy to talk when you first call, but you should realise that it might not be convenient or they may need time to prepare. It might also be seen as unfair to spring an interview on someone without warning. Always check with the interviewee first, and where appropriate agree a convenient time to call them back. Ensure you keep the appointment as punctually as you would a face-to-face interview. Again, it might be a good idea to confirm the details of the interview in writing and explain if it will be recorded.

### Recording interviews

If you intend to tape record an interview, you must ask permission of the person being interviewed in advance of the interview. You should never start to record and then ask permission. Once you begin recording, we recommend you get the interviewee to confirm for the record that they have given their permission to be recorded.

In face-to-face interviews, you may wish to ask a colleague to take notes for you if you are unable to record it. This will enable you to maintain eye contact with the interviewee and concentrate on their responses to your questions. The interview will also take a little less time. For telephone interviews, you might want to consider using a headset to keep both hands free for taking notes.

At the end of an interview, the interviewee should be offered a copy of any tapes made and told that they will be given the chance to approve or dispute the transcript or notes of the interview. We recommend you supply the tape straight away unless you have a specific reason not to — for example, if you are concerned it may be passed to other interviewees or the press. All statements should be confirmed promptly with the person who gave it, while the interview is still fresh in their mind.

## Confidentiality

The statutory guidance asks you to treat the information you gather during an investigation as confidential, to ask interviewees to maintain confidentiality, and remind members of their obligations around confidentiality under the Code of Conduct. We suggest you do this both before and after the interview. However, it should be made clear to the person you are investigating that they are allowed to discuss the case with a friend, adviser or solicitor.

## Evaluating

You need to review all the evidence you gather to determine if there are any gaps in it.

You must be able to take a view on all disputed relevant matters. Absolute certainty is desirable, of course, but not necessary. It is sufficient to form your opinion based on the balance of probabilities. If you cannot do this, you may need to seek further information.

You then need to weigh up all the evidence and decide if the alleged conduct occurred.

Again, you do not need absolute certainty — it is acceptable to come to your conclusion based on the balance of probabilities. If you decide that the subject member acted as alleged, you will need to consider whether his or her conduct involved a failure to comply with the Code of Conduct.

## Reporting

When you have concluded your investigation, you need to write up your findings in a report to the standards committee. The statutory guidance includes detailed advice on this aspect of the investigation process but key points are summarized here.

You have the option of producing a draft version of your report first, giving key parties opportunity to review and comment on your findings and enabling you to check facts and ensure all aspects of the case have been explored sufficiently. A draft report may be particularly suitable

if the facts are complex, ambiguous or disputed, or if the parties expect one. But it is not always necessary, and going straight to a final report will save considerable time.

Draft reports should be sent for comment to the complainant and the member who is the subject of the allegation. Ordinarily you should not need to send the draft to other witnesses or parties interviewed but you should have confirmed their statement. However, there will be occasions when you will need to disclose extracts of a draft report to any potential witnesses, especially if the report is critical of their actions.

Members may respond in whatever manner is most convenient for them. Responses to your draft may reveal the need for further investigation, or they may add nothing of relevance. There may be occasions when responses reveal a need for further investigation and result in such significant changes to the report that you may wish to consider whether to issue a second draft.

Once you have considered whether the responses add anything of substance to the investigation, you will be able to make your final conclusions and recommendations. For more information on producing reports and directions on issuing your final report, refer to the statutory guidance.

### Confidential information

Before issuing draft or final reports, consider whether the report contains any confidential information that should not go into the public domain, such as financial or medical details.

All information of this kind should be deleted from any copies of the report before they are made public. Your authority will be able to advise you further on this process, known as redaction

### Question No 3:-

### What are important cautions while going to seize Computer for investigation?

### Answer:-

**Considerations when Conducting the Seizure**

There are a number of practical considerations and procedures to employ when the decision is made to go forward with a computer seizure. One of the primary considerations that is often neglected is the subject debriefing, when the subject is asked for passwords and whether any encrypted data exists on the target computer.

Procedurally, it is important to identify any destructive processes that maybe running on the machine before beginning the seizure. If such a process appears to be running, unplug the machine immediately.

Before beginning to disconnect the system, make certain to isolate it from any outside connections, such as a phone modem or a CATS network connection; another consideration to be aware of is a wireless connection, which may not be immediately apparent.

Be certain to document the scene with photographs or a diagram, depending on the complexity of the setup, remembering that it may be a year or longer before testimony about what the office looked like on the day of the seizure will be asked for in a !egal proceeding. Additionally, it is important to document what is on the screen if the system is on, as well as what processes are currently running. Many people have a habit of Writing down or recording their passwords near their computer, so examiners should look around for notes that may appear to be passwords. This practice may aid in the discovery of passwords needed to access encrypted data in the event the subject of the investigation is being uncooperative.

The second golden rule when securing a computer is, don't peek through the fues. This also applies to disks. If a system is running, the examiner may be tempted to click on the My Computer icon to look for evidence and/or copy filestoa flash or optical storage device. This should never be done, because each file the investigator touches will have its original time stamps changed; once this is done the original time stamps cannot be recovered. It will be obvious to the forensic examiner that this has occurred.

There are two methods for shutting down a running system, a hard shutdown and a graceful shutdown. Generally, the hard shutdown is preferred. There may be extenuating circumstances that would lead the investigator to perform a graceful shutdown, so it is important to evaluate the best shutdown option based on the type of data being preserved and the possible ramifications of a hard shutdown based on the type of operating system installed. A hard shutdown is basically pulling the power cord from the back of the PC.

Laptop computers present additional considerations. When seizing a laptop, it is important to remove the battery first and then pull the plug. It is essential when seizing a laptop to recover all of the comp9nents that belong to the laptop such as zip drives, CD- and DVD- ROMs, and power supply. Often laptop computers must be imaged with their drives installed and because of the proprietary nature of the laptops themselves, they will only function with their own components.

Once a computer is seized, it is necessary to secure it in such a way that will allow the investigator to testify, if need be, that no unauthorized access to the suspect system occurred.

**What Can the Computer Forensic Examiner Locate?**

A computer-forensic examiner is a trained professional who is capable of analyzing digital media at the hexadecimal level. The hexadecimal level means that every sector and all the bytes in those sectors are available for viewing. This includes deleted files, both purposefully deleted and those that were deleted through various Windows-automated processes. This can also include temporary auto-save files, print.; spool files, deleted emails, and link files. The hexadecimal level also contains various items found in restore points and registry files that define hardware, such as external drives and websites visited, in addition to the document revisions and files created and maintained by the user.

The increased sophistication of Windows allows the computer system to store more information about how people use their computers. The forensic examiner will be able to uncover a large amount of data that relates to the use of a computer, what is or has been stored on it, and the details about the user. In Microsoft's effort to "be all" to the user, it has incorporated ways to make computer use more secure, such as offering encryption and other methods to protect data from unwanted access. In the future, these types of innovations will stall the examiner arid will sometimes successfully prevent system access. However, these encryption packages are not always foolproof. The Encrypted File System offered by Microsoft has in fact been cracked bya number of password-cracking software makers.

Computer-forensic examiners have special tools and software designed to facilitate a thorough and legally sufficient analysis of items that contain digital evidence. It is important to allow a trained examiner to conduct a proper seizure and examination on a piece of evidence so the investigator will have the best chance of using that evidence in a legal proceeding. Whether an agency or company is defending against an unlawful termination suit or filing a criminal complaint, it is vital that the digital evidence is handled properly.

**Handling the Evidence**

One of the major differences between investigating computer-related crimes and conventional criminal activities is the volatility of the evidence that reside~ in the computers themselves. Indeed, the evidence of a computer intrusion might be erased or altered as part of the intrusion itself. It is therefore very important for the organisation and/or law enforcement personnel to deal quickly and decisively with evidence of suspected computer- related criminal activities.

Supported by a foundation for its introduction into court .Legally obtained .Properly identified .Properly preserved

In the handling of computer data in criminal investigations, the examiner *or* investigator must be aware of some of the vulnerabilities of computer evidence:

The investigator must ensure that turning off power to computer equipment will not destroy or erase evidence that is required for the investigation.

The read/write heads of hard disk drives must be parked in a retracted position so that powering down the disk drive will not cause the read/write head to contact the surface: of the disk platter.

Be aware that magnetic storage media are vulnerable to magnetic fields. Evidence might be erased without the investigator being aware of the erasure if the media are brought close to a magnetic field.

Be aware that other equipment attached to the computer might be: needed to complete the investigation into the data that resides in the computer.

The investigator should write-protect all disks that are being used in the investigation so that they cannot be written upon inadvertently.

**Integrity of Evidence**

There are certain issues that must be considered when processing computer evidence. These areas should be considered regardless of whether the incident will be processed criminally or civilly. Even if the organization decides not to take action, the way the investigation is conducted can have potential civil-liability implications for both the organization and the fraud examiner.

Should the fraud examiner discover evidence on a computer system, he must be able to state unequivocally that the evidence was not changed in any way by his actions. This requires that strict forensic methodologies be followed to satisfy the stringent evidentiary standards necessary to ensure the integrity o(the evidence "beyond a reasonable doubt" for possible court presentation. Therefore, fraud examiners must be aware of the following issues that relate to the gathering of computer evidence.

Privacy Issues Regarding Computer Seizure Without Warrant

In every case where it becomes necessary to seize a computer or other device capable of storing digital evidence, the investigator should consult with legal counsel. It is imperative that legal counsel be involved in the seizure process and knowledgeable of case law pertaining to seizures in the workplace. Case law governing workplace seizures in the corporate community is different from case law governing seizures in the government workplace.

When conducting all internal investigation or inquiry into allegations of misconduct or illegal activities in both the private and governmental sector, it is important to be aware of what the

employee policy protects against and what it allows. It should also be determined whether steps have been taken to nullify any expectations of privacy.

It should also be noted that personal devices are becoming more common in the workplace. Employees often carry PDAs, thumb drives, or MP3 players into the office. Each of these devices is capable of storing large amounts of data and can easily be used to steal a company's intellectual property.. Because these devices are often purchased by the employee for personal use, a search warrant may be needed to seize or search these devices because employees may have a "reasonable expectation of privacy" in these types of personal devices. Therefore, it is extremely important to include such devices in the company's search policy.

**Law Enforcement Assistance**

There may be occasions when a fraud examiner will be called upon to assist law enforcement or to request the assistance of law enforcement in a particular case. Fraud examiners who are involved in law enforcement already understand the importance placed on proceeding with the search and seizure pursuant to a search warrant. Under these conditions, the law enforcement officer will prepare an affidavit for the search warrant, which will detail the probable cause or legal reasoning behind the request for the warrant. Only a judge can issue a search warrant and only law enforcement can seek and serve a search warrant. Often law enforcement personnel will need guidance from the fraud examiner as they conduct pre- search preparation.

## Pre-Search Preparation

Obtaining as much intelligence as possible regarding the location of the potential evidence is very desirable before writing the search warrant affidavit. Considerations for fraud examiners include:

Determine the type of computer systems that will be involved in the search. What operating system is used? Are the computers networked together?

Determine how many people will be needed to conduct the search. In one case, approximately 17 networked file servers were involved, with multiple routers and dial-up modems. A team of only two investigators would need at least four to six hours to complete a seizure of this magnitude.

If expert witnesses with a specific expertise are required during the search, identify and clear them before the search warrant is written. Depending on the circumstances, their credentials should possibly be included in the warrant affidavit before they are approved by the magistrate issuing the search warrant~ The time to discover that an "expert witness" has a criminal conviction is before the search warrant affidavit has even been written, not when the witness takes the stand to testify in a criminal proceeding.

## Search Warrant Affidavit Construction

Law enforcement personnel may seek the advice of the fraud examiner when constructing the search warrant affidavit. It is important to prepare an affidavit that includes all of the pertinent information, which will allow for a proper and legal search.

Question No 4:-

How organization should respond to different risks.

Answer:-

**Response to Fraud Risks:**

Regardless of the framework used to conduct the fraud risk assessment, management will need to address to the identified risks. Larry Cook, CFE, who is the principal author of the ACFE Fraud Risk Assessment Tool, suggests that management can use one or a combination of the following approaches to respond to the organization's residual fraud risks:

**Avoid the Risk**

Management may decide to avoid the risk by eliminating an asset or exiting an activity [the control measures required to protect the organisation against an identified threat are too expensive. This approach requires the fraud risk assessment team to complete a cost-benefit analysis of the value of the asset or activity to the organisation compared to the cost of implementing measures to protect the asset or activity.

**Transfer the Risk**

Management may transfer some *or* all *of* the risk by purchasing fidelity insurance or a bond. The cost to the organizations the premium paid for the insurance or bond. The covered risk of loss is then transferred to the insurance company, less any deductible payment included in the contract.

**Mitigate the Risk**

Management can help mitigate the risk by implementing appropriate countermeasures, such as prevention and detection controls. The fraud risk assessment team should evaluate each countermeasure to detertnine if it is cost effective andreasonib1e given the probability of occurrence and impact Qf.1oss.

**Assume the Risk**

Management may choose to assume the risk if it determines that the probability of occurrence and impact of loss are low. Management may decide that it is more cost effective to assume the risk than it is to eliminate the asset or exit the activity, buy instance to transfer the risk, or implement countermeasures to mitigate the risk.

**Combination Approach**

Management may also elect a combination of the above approaches. For example, if the probability of occurrence and impact of loss are high, management may decide to transfer part of the risk through the purchase *of* insurance, as well as implement preventive and detective contro1s to mitigate the risk.

Question No 5:-

Discuss the criminal Investigator Responsibilities and also explain the crime scene priorities.

Answer:-

## Criminal Investigators' Responsibilities

Criminal investigators should arrive at the crime scene as quickly as possible because:

- The suspect may still be at or near the scene.
- Injured persons may need emergency care.
- Witnesses may still be at the crime scene.
- A dying person may have a confession or other pertinent information to give.
- Weather conditions may change or destroy evidence.
- Someone may attempt to alter the crime scene.

## Crime Scene Priorities

Although circumstances at the crime scene may dictate the criminal investigator's priorities, the first priority generally is to handle emergencies: save life, apprehend suspects, and request assistance. The second priority is to secure the scene. The third priority is to investigate.

## Preliminary Investigations: Basic Considerations

The initial response is usually by a patrol officer assigned to the area where a crime has occurred.

During the preliminary investigation, criminal investigators measure, photograph, videotape, and sketch the scene. They then proceed to search for evidence. If the investigators find physical evidence, they identify, collect, examine, and process it. Victims, witnesses, and suspects are questioned, and statements and observations are recorded in notes.

## Following are the steps in the investigative process:

- Determine if a crime has been committed.
- Verify jurisdiction.
- Discover all facts and collect physical evidence.
- Recover stolen property.
- Identify the perpetrator or perpetrators.
- Locate and apprehend perpetrators.
- Aid the prosecution by providing evidence of guilt admissible in court.
- Testify effectively as a witness in court.

It is not enough to just collect and analyze evidence. Investigators need to apply the logic of reasoning or the methodology of scientific research investigation. They need what can only be called working theories, which are sufficiently flexible to allow for new information while still demonstrating clear patterns of inference or cause and effect.

A hypothesis is an if-then statement that implies a variable level of certainty, as in "if the victim was mutilated, the perpetrator is most likely disturbed." Steps in the scientific method of investigation include:

- Identifying the questions and define the key variables.
- Specifying the simplifying assumptions.
- Formulating a hypothesis.
- Testing the hypothesis with data.

- Retesting the hypothesis with additional data to validate.

Question No 6:-

How to develop an Anti-Fraud Program. Also discuss the typical types of Fraud and Fraud Tests.

Answer:-

## Seven Steps to Jump Start Your Anti-Fraud Program

Fraud whether it occurs in the form of carefully crafted Ponzi schemes, fudging financial reports or theft from one's own employer, is reaching alarming proportions and is not without its costs. Businesses and government agencies worldwide suffer hundreds of billions in lost or misused funds, diminished value, and irreversible damage to company reputation and customer trust.

Consider the alarming stats from the 2010 Report to the Nations on Occupational Fraud and Abuse from the Association of Certified Fraud Examiners (ACFE). According to the study, organizations worldwide lose an average of 5% of revenues to fraud each year for an average of $160,000.

Making matters worse (and no thanks to the economic downturn), many organizations have been forced to cut staff, freeze spending and skimp on internal controls and process assurance, which has left organizations more vulnerable to risk and fraud.

Now is the time for Internal Audit teams to step up fraud prevention and detection measures. Here is a quick list of priorities to kick start your program.

**1. Build a profile of potential frauds**

Take a top-down approach to your risk assessment, listing the areas in which fraud is likely to occur in your business and the types of fraud that are possible in those areas. Then qualify the risk based on the overall exposure to the organization. Focus on risks that have the greatest chance of reducing shareholder value.

**2. Test transactional data for possible indicators of fraud**

You must test 100% of the data, not just random samples. Fraudulent transactions, by nature, do not occur randomly. Transactions may fall within boundaries of certain standard testing and not be flagged.

**3. Improve controls by implementing continuous auditing and monitoring**

Strengthen controls over transaction authorizations and use continuous auditing and monitoring to test and validate the effectiveness of your controls. This method can drastically improve the overall efficiency, consistency and quality of your fraud detection processes

**4. Communicate the monitoring activity throughout the organization**

A big part of fraud prevention is communicating the program across the organization. If everyone knows there are systems in place that alert to potential fraud or breach of controls, and that every single transaction running through your systems is monitored, you've got a great preventative measure.

**5. Provide management with immediate notification when things are going wrong**

It is better to raise any issues right away than explain why they occurred later. Create audit reports with recommendations on how to tighten controls or change processes to reduce the likelihood of recurrence. And, don't forget to quantify the impact to the business.

**6. Fix any broken controls immediately**

Segregation of duties is important. If you can initiate a transaction, approve the transaction, and also be the receiver of the goods from the transaction, there is a problem.

**7. Expand the scope and repeat.**

Re-evaluate your fraud profile, taking into account both the most common fraud schemes and those that relate specifically to the risks that are unique to your organization, and move your investigative lens.

## Typical Types of Fraud and Fraud Tests

Knowing what to look for is critical in building a fraud detection program. The following examples are based on descriptions of various types of fraud and the tests used to discover the fraud as found in Fraud Detection: Using Data Analysis Techniques to Detect Fraud.

| Type of Fraud | Tests Used to Discover This Fraud |
|---|---|
| **Fictitious vendors** | ➢ Run checks to uncover post office boxes used as addresses and to find any matches between vendor and employee addresses and/or phone numbers<br>➢ Be alert for vendors with similar sounding names or more than one vendor with the same address and phone number |

| | |
|---|---|
| **Altered invoices** | ➢ Search for duplicates<br>➢ Check for invoice amounts not matching contracts or purchase order amounts |
| **Fixed bidding** | ➢ Summarize contract amount by vendor and compare vendor summaries for »»several years to determine if a single vendor is winning most bids<br>➢ Calculate days between close for bids and contract submission date by vendor »»to see if the last bidder consistently wins the contract |
| **Goods not received** | ➢ Search for purchase quantities that do not agree with contract quantities<br>➢ Check if inventory levels are changing appropriate to supposed delivery of goods |
| **Duplicate invoices** | ➢ Review for duplicate invoice numbers, duplicate date, and invoice amounts |
| **Inflated prices** | ➢ Compare prices across vendors to see if prices from a particular vendor are »»unreasonably high |
| **Excess quantities purchased** | ➢ Review for unexplained increases in inventory<br>➢ Determine if purchase quantities of raw materials are appropriate for production level<br>➢ Check to see if increases in quantities ordered compare similarly to previous contracts or years or when compared to other plants |
| **Duplicate payments** | ➢ Search for identical invoice numbers and payments amounts<br>➢ Check for repeated requests for refunds for invoices paid twice |
| **Carbon copies** | ➢ Search for duplicates within all company checks cashed; conduct a second search for gaps in check numbers |
| **Duplicate serial numbers** | ➢ Determine if high value equipment a company already owns is being repurchased by checking serial numbers for duplicates and involvement of same personnel in purchasing and shipping processes |
| **Payroll fraud** | ➢ Find out if a terminated employee is still on payroll by comparing the date of termination with the pay period covered by the paycheck and extract all pay transactions for departure date less than date of current pay period |
| **Accounts payable** | ➢ Reveal transactions not matching contract amounts by linking Accounts Payable files to contract and inventory files and examining contract date, price, ordered quantity, inventory receipt quantity, invoice quantity, and payment amount by contract |

**********