Quest Masterclass

Leading The Risk Based Internal Audit Function

How to Create An Effective Risk Based Internal Audit System?

According to the ACFE (Association of Certified Fraud Examiners), fraud and corruption is costing corporations and government 5% of revenue or spend. This equates to US$4 trillion per year. This is a worldwide epidemic and can only be tackled by effective Fraud Risk Management. The most effective way to manage and combat Fraud is to train fraud fighters and employees in identifying key indicators of fraud and in the latest techniques for identifying, investigation and managing fraud risk. This ebook will equip you to manage and fight fraud and be a part of the process to reduce the impact on organisations.

2 Key Pain Points for Developing A Fraud Risk Management Programme

An efficient Fraud Risk Management Programme involves a sound understanding of human behaviour, why people obey law, what encourages them to commit crimes, laws related to frauds etc. Along with the above stated important topics, one should also note down the international and regional initiatives that are being taken against fraud and corruption, worldwide trends in frauds, and departments and high risk industries that are most prone to frauds. Below are 2 main pain points for developing a Fraud Risk Management programme:

1. Profiling The Fraudster

2. Digital Forensics

1. Profiling The Fraudster

The first and foremost objective is to understand the underlying reasons why people commit fraud so we can educate others and help business owners prevent fraud from happening to their businesses. Trust violators are often trusted persons who do illegal trade frauds when they conceive of themselves as having a financial problem which is non-shareable, and are aware that this problem can be secretly resolved by violation of the position of financial trust. The fraud triangle defines this in the simplest sense.

The Fraud Triangle

Opportunity	Rationalization	Pressure

The Fraud Triangle consists of 3 components that together lead to fraudulent behaviour:

a. Pressure:

This is the first component of the fraud triangle that motivates crime in the first place. This indicates that only by the use of legitimate means, the individual's financial problems cannot be solved, so he begins to consider committing an illegal act, such as looting cash or falsifying a financial statement, in order to solve his problem. He may suffer from either personal or professional financial problems like he may be in great debt or suffering from financial losses in business respectively.

Reasons why this type of fraud occur:

- **Gambling or narcotic addiction**
- **Not able to pay personal bills**
- **To meet the set output at work**
- **Aspiring a better lifestyle such as a stylish car or a bigger house**
- **To sustain investor confidence**

b. Opportunity:

This is the first component of the fraud triangle that motivates crime in the first place. This indicates that only by the use of legitimate means, the individual's financial problems cannot be solved, so he begins to consider committing an illegal act, such as looting cash or falsifying a financial statement, in order to solve his problem. He may suffer from either personal or professional financial problems like he may be in great debt or suffering from financial losses in business respectively.

- **This is the second component of the fraud triangle that motivates crime at the second place.**
- **This indicates a perceived opportunity, using which the person can commit the crime.**
- **The person searches for ways through which he can solve his financial problems without any/low perceived risk of getting caught.**
- **The fraudster always looks out for ways through which he can solve his problems using secretive ways. For maintaining their social status, many people commit white-collar crimes. For example, for concealing a drug problem, paying off debts, or enjoying a better lifestyle some people might indulge in stealing.**
- **If a perpetrator is caught falsifying financial information, this will not only hurt his status but he will also not be able to conceal his theft. So the fraudster not only has to be able to steal funds, but he has to be able to do it in such a way that he will likely not be caught and the crime itself will not be detected.**

c. Rationalization:

- **Rationalization is the third component of the Fraud triangle.**
- **Most violators think that they were actually not criminals.**
- **This is because they had rationalized to themselves that the misdeed was ok. Moreover, they thought that this was an act of general irresponsibility and not only them but everyone was responsible for it.**
- **For example, some fraudsters think that their fraud is justified because they find themselves as otherwise morally upright. Also a lot of other people think that they are justified in doing so because they are either underpaid or feel overworked.**

2. Digital Forensics

As law enforcement and legal entities realize how valuable information technology (IT) professionals are when it comes to investigative procedures, they are heavily investing in the field of computer forensics investigation. For protecting private citizens, national security, government and law enforcement, tracking malicious online activity has become very important. Digital forensics allows investigators to connect cyber communications and digitally-stored information to physical evidence of criminal activity. This helps to curb future cybercrimes. Let's take a detailed analysis of the most important steps involved in digital forensics:

Digital Forensics

1. Development of Policies & Procedures:

- Cybersecurity professionals understand that if not held responsibly, information can be easily leaked out.
- To protect such leak outs, strict procedures and guidelines are made for computer forensic investigations such as when to recover potential digital evidence, how to prepare systems for evidence retrieval, where to store any retrieved evidence, and how to document these activities to help ensure the authenticity of the data.
- Codification of a set of explicitly-stated actions such as a proper definition of evidence, its constituents, where to look for it, and how to handle it once it has been retrieved.
- Before solving any case at hand, all permissions and authorizations regarding the case should be taken, case briefs should be read, and warrants must be thoroughly understood.

2. Assessment of Evidence:

- First of all it's important to classify the cybercrime in consideration including specific platforms and data formats.
- Computer forensics investigators sift through email accounts, hard drives, social networking sites etc. to search for any information that can serve as evidence of the crime.
- Then Computer forensics investigators should check the source and integrity of such data before taking it as evidence.
- A clear perception as to how to protect and preserve the collected evidence is also a must.

According To A Report by Transparency Market Research, The Global Digital Forensics is Estimated To Reach

US$4.9 bn till 2021

This Market is Projected to Grow Significantly At A

12.50% CAGR between 2015 & 2021

3. Evidence Acquisition:

- Acquisition of evidence is the most critical factor in the success of a Computer forensic investigation.
- Investigation must contain detailed analysis of everything involved including software and hardware specifications and other systems in the investigation process.
- After acquisition, preservation is the key area of focus. This includes guidelines such as physical removal of storage devices, retrieval of sensitive data using controlled boot discs to retrieve sensitive data etc.

4. Evidence Examination:

- Various methods are used to examine the evidence such as:
  - a. Data tagged with times and dates.
  - b. Analyzing file names for knowing where specific data was created, downloaded, or uploaded.
  - c. Analysis software to search massive archives of data for specific keywords or file types.
- In this stage, computer forensic investigators work in close collaboration with criminal investigators, lawyers, and other qualified personnel to ensure a thorough understanding of the nuances of the case.

Major Pain Point of Risk Based Auditing

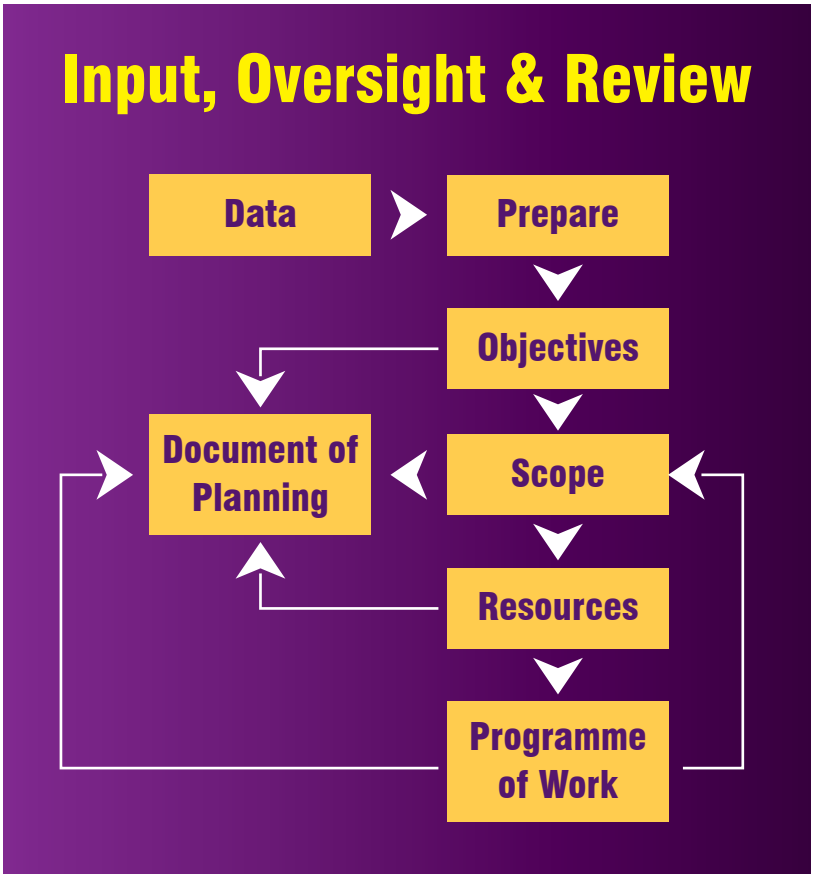
The risk based internal audit function and strategy consists of not just internal audit frameworks, but also strategies, policies and procedures established by the chief audit executive (CAE). CAE need to take care of best standards relating to strategy, planning and reporting, and the key elements that will make the internal audit strategy effective, risk-based and value-add.

How to Efficiently Plan Internal Audit

A. Opportunity:

First and foremost the internal auditors need to comprehend the area under review. This needs careful research across organisational documents and internet. This not only help Internal Auditors build good relationships with managers but also assists in knowing the activities that the former manage. Following are some of the activities:

- i. What kind of activities occur?
- ii. Who is assigned with what task?
- iii. What purpose do such task/tasks serve?
- iv. What information is available to whom?
- v. What are the risks and responses?



B. Objectives:

For each engagement, Performance Standard 2210 demands internal auditors to establish objectives for each engagement. Here are few guidelines:

i. To determine the implementation standards, it is important to know whether the purpose of engagement is assurance or consulting.

ii. For any internal audit work, Performance Standard 2100, will set an objective. It amounts to evaluating and contributing to the up gradation of the subject matter.

iii. The Performance Standards 2100 series describes the objectives on risk management, control processes, and governance. It comprises of a stable coordination between IT governance and the board, including the auditors and management of an organization.

iv. The assurance implementation standards include observing reliability and integrity of financial and operational information. Moreover, whether the organization is able to safeguard the assets, and comply with laws and regulations is of vital importance.

Explanatory Business Objectives, Risks & Audit Objectives

	1. Business Objective	2. Business Risk	3. Audit Objective
a. Strategic	Execution of creative and new customer relationship database.	A delay in execution of database will lead to loss of market share and business.	Monthly affirmation that the company is achieving its set goals.
b. Operational	Aim to solve customer complaints at the earliest.	Inability to solve customer concerns will lead to loss of reputation and camouflage future revenue streams.	Confirming that all customer complaints have been successfully resolved by the concerned authorities.
c. Reporting	Monthly performance is accurately reported.	Impeded and deficient reports will often provide a deceptive review of operational performance.	Assuring that monthly reports were reliable and were produced on time.
d. Compliance	Personal data is kept secret as per data protection acts and privacy laws.	A violation in data security resulting in loss of data leading to legal punishments and fines.	Ensuring that the rules and regulations set for data privacy are adequate and effective.

C. Scope:

It revolves around the extent of the subject matter with which the engagement deals.

i. Scope sets boundaries and expectations and allows to identify records and systems. It also clarifies the period under review and the complete subject matter to the managers.

ii. The Performance Standard 2200 clearly mentions that the objectives of the engagement must be duly satisfied by the established scope. Thus, it is better to identify all the relevant people, business areas and systems.

iii. Root cause analysis guarantees that biases are curtailed, presumptions are challenged, and evidence is completely assessed. This technique is more effective when deliberations with stakeholders take place around the scope of the audit engagement.

D. Resources:

It's important to implement enough resources and also the right resources. Let's see what the internal auditor needs to take into consideration while allotting resources:

a. Sufficient: The internal auditor must take into consideration about the planned engagement days in organization. And also about the estimated start and finishing dates and the complexity of the engagement. However this is just the preliminary allocation of resources which is subject to change at later stages.

b. Appropriate: Appropriate resources are a function of their objectivity, competency and independence.

E. Programme of Work:

i. According to Performance Standard 2240, internal auditors should formulate and document work programmes that accomplish the engagement objectives.

ii. Internal Auditors should prepare a formal project plan to coordinate activities such as surveys, data gathering, interview etc.

iii. Internal Auditors need to take care not to provide notices relating to meetings, visits, and information requests in some engagements.

iv. Internal Auditors should note that the work programme must consist of procedures for discerning, scrutinizing, assessing, and documenting data during the engagement.

Quest ontheFRONTIER

People- Knowledge- Success

Consulting/
Interim Management

Executive Search

Master Class &
Conference

Incorporated in 2002 and head quartered in Singapore, **Quest ontheFRONTIER** is an established international consulting, executive search and training company operating in Asia, the Middle East and Africa with 7 offices including China, India, Vietnam and Indonesia. We provide implementation consulting wherein our consultants with deep industry knowledge help organizations develop and execute business initiatives. The same philosophy guides our training services including Quest Master Class; our Master trainers are seasoned industry executives with leading global companies who share their insights and facilitate interactive learning among the participants. Quest conferences provides a platform for industry leaders to exchange ideas, interact and network.
We help individuals and organizations succeed through knowledge and insights.

Quest Masterclass

Quest Conferences

Quest Learning & Development

Quest Consulting

www.questonthefrontier.com

Singapore l Hong kong l China l Vietnam l India l Indonesia l Dubai UAE l Myanmar

for More Details Contact upendra@questmasterclass.com