



E - NEWS LETTER



Tuticorin Branch of Southern India Regional Council of The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)

May 2010

Chairman Writes



Dear Friends,

After the hectic bank audits' season, this month we can find some time to relax with our family and friends. We should take good care of ourselves especially in summer to avoid unnecessary complications. Let me discuss an interesting topic with you...

How to improve our memory?

Sometimes we find difficult to remember names, numbers or any important piece of information. Memorizing especially for students may seem like a dull task and this idea makes accomplishing it all the more difficult. But there is always a way. Here are a few tips...

i) Look for pattern: When we have to remember long phrases or numbers, we can look for pattern. For example, 38101517222429. Look at this number, it may appear random but it has a pattern. Adding 5 to the first number gives the second and adding two to the second gives the third and so on. To remember such a series it is enough if we know the first number and the pattern.

ii) Associate: Break down the numbers into smaller portions and associate them with something else. For example take the number 36552101, 365 – No. of days in a year, 52 – a deck of cards or the No. of weeks in a year, 101 – Phone No. for ambulance. Also imagine an image or a situation incorporating separate ideas formed above into a single idea. It makes us think creatively.

iii) Use the alphabetical order: In case of listing all the states in India, pick out all those beginning with A, then B and so on. Sounds easy isn't it!

iv) Categorize them: In case of shopping, just put them into groups or heads and keep in mind the groups and the number of items under each head.

v) Chunk numbers: We use this strategy almost everyday. To memorise a phone number we just put them into chunks of 2, 3 or 4 digits and likewise.

vi) Assign images: Names, places or words can be related to images, so that we almost picturise them and they are better stored in our memory.

vii) Make up a story: It is fun to make up a story that includes all things we need to remember on a particular occasion. The story has to be more ridiculous to be more effective.

viii) Apply mnemonic codes: All of us would have come across the code VIBGYOR which denotes the seven colours of a rainbow. Another example is the difference between the words desert and dessert. The sweet one has two sugars (S). Search for such codes.

We can use these tips singly or in combination as appropriate. These are some tips that energise the brain. To conclude as the saying goes, "Wit beyond measure is man's greatest treasure".

Best Wishes and regards,

CA H.Raman

Effects of Global Warming on India



Lakshadweep, comprising tiny low-lying islands, are at risk of being inundated by sea level rises associated with global warming.

The effects of **global warming on the Indian subcontinent** vary from the submergence of low-lying islands and coastal lands to the melting of glaciers in the Indian Himalayas, threatening the volumetric flow rate of many of the most important rivers of India and South Asia. In India, such effects are projected to impact millions of lives. As a result of ongoing climate change, the climate of India has become increasingly volatile over the past several decades; this trend is expected to continue.

Greenhouse gases in India

Elevated carbon dioxide emissions contributed to the greenhouse effect, causing warmer weather that lasted long after the atmospheric shroud of dust and aerosols had cleared. Further climatic changes 20 million years ago, long after India had crashed into the Laurasian landmass, were severe enough to cause the extinction of many endemic Indian forms.^[1] The formation of the Himalayas resulted in blockage of frigid Central Asian air, preventing it from reaching India; this made its climate significantly warmer and more tropical in character than it would otherwise have been.^[2]

Effects of global warming on India and Bangladesh

Several effects of global warming, including steady sea level rise, increased cyclonic activity, and changes in ambient temperature and precipitation patterns, have affected or are projected to affect India. Ongoing sea level rises have submerged several low-lying islands in the Sundarbans, displacing thousands of people.^[3] Temperature rises on the Tibetan Plateau, which are causing Himalayan glaciers to retreat.

Environmental

Increased landslides and flooding are projected to have an impact upon states such as Assam.^[4] Ecological disasters, such as a 1998 coral bleaching event that killed off more than 70% of corals in the reef ecosystems off Lakshadweep and the Andamans, and was brought on by elevated ocean temperatures tied to global warming, are also projected to become increasingly common.^{[5][6][7]}

The first among the countries to be affected by severe climate change is Bangladesh. Its sea level, temperature and evaporation are increasing, and the changes in precipitation and cross boundary river flows are already beginning to cause drainage congestion. There is a reduction in fresh water availability, disturbance of morphologic processes and a higher intensity of flooding and other such disasters. Bangladesh only contributes 0.1% of the world's emissions yet it has 2.4% of the world's population. In contrast, the United States makes up about 5 percent of the world's population, yet they produce approximately 25 percent of the pollution that causes global warming.^[8]

Economic

The Indira Gandhi Institute of Development Research has reported that, if the predictions relating to global warming made by the Intergovernmental Panel on Climate Change come to fruition, climate-related factors could cause India's GDP to decline by up to 9%; contributing to this would be shifting growing seasons for major crops such as rice, production of which could fall by 40%. Around seven million people are projected to be displaced due to, among other factors, submersion of parts of Mumbai and Chennai, if global temperatures were to rise by a mere 2 °C (3.6 °F).^[9]

Villagers in India's North Easter state of Meghalaya are also concerned that rising sea levels will submerge neighbouring low-lying Bangladesh, resulting in an influx of refugees into Meghalaya^[citation needed]—which has few resources to handle such a situation.

If severe climate changes occur, Bangladesh will lose land along the coast line.^[10] This will be highly damaging to Bangalies especially because nearly two-thirds of Bangladeshis are employed in the agriculture sector, with rice as the single-most-important product. The economy has grown 5-6% over the past few years despite inefficient state-owned enterprises, delays in exploiting natural gas resources insufficient power supplies, and slow implementation of economic reforms. However, Bangladesh remains a poor, overpopulated, and inefficiently-governed nation.^[11] If no further steps are taken to improve the current conditions global warming will affect the economy severely worsening the present issues further.^[citation needed]

Social

Climate Change in India will have a disproportionate impact on the more than 400 million that make up India's poor (See Poverty in India). This is because so many depend on natural resources for their food, shelter and income. More than 56% of people in India work in agriculture, while many others earn their living in coastal areas.^[12]

Indian journalist, Praful Bidwai, argues that the Indian Government's climate policy does not address the interests of the majority of these peoples for whom climate change will mean hunger, food insecurity, and destruction of livelihoods but is instead focused on maximising Indian elite's freedom to consume by maintaining high emissions-intensive GDP growth.^[13]

Past climate change



Thick haze and smoke along the Ganges River in northern India.

However, such shifts are not new: for example, earlier in the current Holocene epoch (4,800–6,300 years ago), parts of what is now the Thar Desert were wet enough to support perennial lakes; researchers have proposed that this was due to much higher winter precipitation, which coincided with stronger monsoons.^[14] Similarly, Kashmir, which once had a warm subtropical climate, shifted to a substantially colder temperate climate 2.6–3.7 mya; it was then repeatedly subjected to extended cold spells starting 1 years ago.^[15]

Pollution

Thick haze and smoke, originating from burning biomass in northwestern India^[16] and air pollution from large industrial cities in northern India^[17], often concentrate inside the Ganges Basin. Prevailing westerlies carry aerosols along the southern margins of the steep-faced Tibetan Plateau to eastern India and the Bay of Bengal. Dust and black carbon, which are blown towards higher altitudes by winds at the southern faces of the Himalayas, can absorb shortwave radiation and heat the air over the Tibetan Plateau. The net atmospheric heating due to aerosol absorption causes the air to warm and convect upwards, increasing the concentration of moisture in the mid-troposphere and providing positive feedback that stimulates further heating of aerosols.^[17]

Awareness

Tribal people in India's remote northeast plan to ^[18] honour former U.S. Vice President Al Gore with an award for promoting awareness on climate change that they say will have a devastating impact on their homeland.

Meghalaya -- meaning 'Abode of the Clouds' in Hindi -- is home to the towns of Cherrapunji and Mawsynram, which are credited with being the wettest places in the world due to their high rainfall.

But scientists state that global climate change is causing these areas to experience an increasingly sparse and erratic rainfall pattern and a lengthened dry season,^[19] affecting the livelihoods of thousands of villagers who cultivate paddy and maize. Some areas are also facing water shortages.

Practicing Information Technology Auditing for Fraud

Fraud is often difficult to detect and even harder to prove in a court of law. This paper provides insight into common practices applicable to practicing professionals who are auditing for fraud in an information technology (IT) environment.

The term "occupational fraud" is defined as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."¹ The study used as the basis for this definition was compiled from data associated with 1,134 occupational fraud investigation cases that occurred between January 2004 and January 2006. Selected key findings of this report concluded that in 2006:

US organizations suffered an estimated 5 percent loss of annual revenues to fraud (estimated at approximately US \$652 billion)

The median financial loss due to occupational fraud was US \$159,000

Less than 8 percent of the perpetrators had convictions prior to committing their frauds

The extent of fraud losses was strongly related to the position of the perpetrator

Figure 1—COBIT's Control Objectives on IT Processes

Plan and Organize		Deliver and Support	
PO1	Define a strategic IT plan.	DS1	Define and manage service levels.
PO2	Define the information architecture.	DS2	Manage third-party services.
PO3	Determine technological direction.	DS3	Manage performance and capacity.
PO4	Define the IT processes, organization and relationships.	DS4	Ensure continuous service.
PO5	Manage IT investment.	DS5	Ensure systems security.
PO6	Communicate management aims and direction.	DS6	Identify and allocate costs.
PO7	Manage IT human resources.	DS7	Educate and train users.
PO8	Manage quality.	DS8	Manage service desk and incidents.
PO9	Assess and manage IT risks.	DS9	Manage the configuration.
PO10	Manage projects.	DS10	Manage problems.
Acquire and Implement		DS11	Manage data.
AI1	Identify automated solutions.	DS12	Manage the physical environment.
AI2	Acquire and maintain application software.	DS13	Manage operations.
AI3	Acquire and maintain technology infrastructure.	Monitor and Evaluate	
AI4	Enable operation and use.	ME1	Monitor and evaluate IT performance.
AI5	Procure IT resources.	ME2	Monitor and evaluate internal control.
AI6	Manage changes.	ME3	Ensure compliance with external requirements.
AI7	Install and accredit solutions and changes.	ME4	Provide IT governance.

Roles of IT Auditor in Fraud Control

Whether or not an auditor is auditing for fraud, all auditors are expected to assume responsibility for detecting fraud and assessing antifraud programs. The Statement on Auditing Standards (SAS) 99 of the American Institute of Certified Public Accountants (AICPA)² emphasizes auditors exercising their professional skepticism to identify risks that may result in a material misstatement due to fraud. The US Public Company Accounting Oversight Board (PCAOB)³ also requires auditors to evaluate fraud-related activities as a component of an internal audit function.

With rapid advancements in information communications and technologies (ICT) and an increasingly mobile accessible environment (i.e., wireless networking), it is no surprise that companies are increasingly reliant on IT equipment and applications for the delivery of company operations. IT audit provides a vital role in the prevention, detection and investigation of fraud.

To make a valuable contribution toward fraud control, requirements need to be elaborated on and understood by the IT auditor with respect to the various IT processes and types of fraud, each of which contributes to the development of fraud risk assessment.

IT Processes

Control Objectives for Information and related Technology (COBIT)⁴ provides excellent coverage of IT processes. An IT process, according to COBIT, can be classified into one of four specific domains:

- 📁 Plan and Organize (PO)
- 📁 Acquire and Implement (AI)
- 📁 Deliver and Support (DS)
- 📁 Monitor and Evaluate (ME)

A total of 34 IT processes are listed within these four domains, as shown in **figure 1**.

Whether or not a fraud is likely to occur in each of the identified IT processes is debatable. To better understand if a fraud is likely to occur, the fraud triangle hypothesis, developed by criminologist Dr. Donald R. Cressey, should be considered by all auditors.⁵ According to Cressey, three factors, each of which is briefly described in **figure 2**, are associated with any person who commits fraud.

Since there is a human association in any IT process, regardless of the IT system's degree of automation, the possibility of a fraud should always be considered.

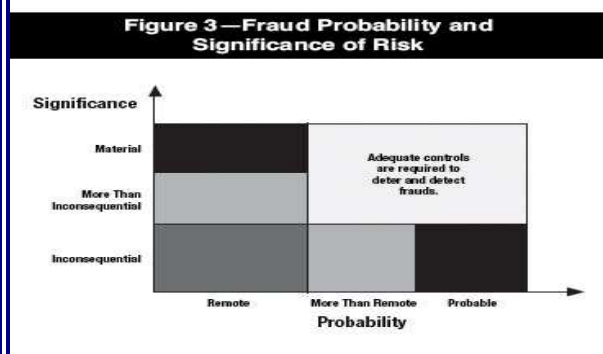


Figure 2—Cressey's Fraud Triangle

Factor	Description
Perceived unsharable financial need	This is the original motive. The fraudster has some financial problem that he/she is unable to solve through legitimate means. The financial problem can be personal or professional. Examples of problems that commonly lead to fraud include a: <ul style="list-style-type: none"> • Need to meet productivity targets at work • Need to meet earnings to sustain investor confidence • Drug or gambling addiction
Perceived opportunity	This defines the method by which the fraud can be committed. The fraudster believes he/she can abuse his/her position of trust to solve the financial problem with a low perceived risk of getting caught. For example, an employee has the authority to make an IT investment and has a strong influence in selecting a vendor.
Rationalization	The vast majority of fraudsters are first-time offenders, and they do not view themselves as criminals. The fraudster must justify the crime to himself in a way that makes it an acceptable or justifiable act. Common rationalizations include: <ul style="list-style-type: none"> • "I am only borrowing the money" • "I am underpaid" • "My employer/supervisor is dishonest to others and deserves to be fleeced"

Types of Fraud

Typically, occupational frauds fall into one of three major categories:⁶

1. **Asset misappropriation**—Any scheme that involves the theft or misuse of an organization's assets, e.g., use of software and software licenses purchased by the company for personal use or financial gain
2. **Corruption**—Any scheme in which a person uses his/her influence in a business transaction to obtain an unauthorized benefit contrary to that person's duty to his/her employer, e.g., awarding outsourcing IT equipment maintenance services to the vendor that provides cash and/or gifts
3. **Fraudulent statement**—The falsification of an organization's financial statement to make it appear more or less profitable, e.g., spending to adjust the average revenue per user (ARPU) figure of the telecommunications operator

Each of these categories can be further broken down into different fraud schemes. The knowledge of different types of fraud and awareness of common fraud schemes across industries can greatly facilitate the appropriateness and accuracy of fraud risk assessments.

Fraud Risk Assessment

The fraud risk assessment begins with ranking the likelihood and significance of fraud activities associated with IT processes. PCAOB Auditing Standard (AS) No. 2 provides an example of the probability of a risk and its corresponding significance. This PCAOB standard specifies three risk levels:

- Remote
- More than remote
- Probable

The PCAOB standard also defines significance of a risk into three categories:

- Inconsequential
- More than inconsequential
- Material

Figure 3 illustrates the relationship between the significance and the probability of risk. Upon the completion of ranking fraud activities associated with IT processes, the fraud risk assessment process can map the IT processes with types of fraud and controls in place (if any), as shown in **figure 4**.

Figure 4—IT Process vs. Fraud Control Matrix			
IT Process	Types of Fraud	Fraud Scenario	Internal Controls
Manage IT human resources.	Corruption	The IT project manager (budget approver) overstates the development efforts and requests additional contractors to receive kickbacks from the human resources agency.	<p>Procedures exist to control additional IT human resources.</p> <p>Selection criteria for human resources agency are established and the quality of IT contractors provided is subject to regular monitoring (e.g., background check).</p> <p>There is regular review of IT human resources and IT workloads/deliverables.</p>
Procure IT resources.	Asset misappropriation	<p>IT hardware/software is purchased without actual deployment for a prolonged period of time. The related assets are either missing or not being used.</p> <p>Fraudulent invoicing occurs on a number of software licenses acquired.</p>	<p>Procurement procedures are established.</p> <p>Reconciliation of hardware/software procurement evidence is maintained, and the inventory record is conducted on a regular basis.</p> <p>An inspection mechanism is available to verify the actual deployment of software features.</p>

Fraud risk assessments allow organizations to easily visualize the areas for occurrence of fraud and prioritize their resources against these potential fraud areas. Since both the business and IT environments are changing rapidly, the fraud risk assessment should be carried out on a regular basis or whenever there is a major change in an IT process. Furthermore, in identifying an IT process for fraud risk assessment, an auditor may use history patterns of fraud within the company as a benchmark reference.

Fraud Prevention

The term prevention is self-explanatory—to stop something from happening. Common sense tells us that it is more costly to make a change after the completion of product, project or IT application, than to have the right design in the beginning. Fraud prevention applies to activities auditors are already undertaking today. Auditors have an increasing influence on the early stages of development of a business product, process or IT application. Wherever controls are found to be inadequate to protect against fraud risks, or the risk level is rated as being "more than remote" or higher and simultaneously at a "more than inconsequential" level (or greater) in terms of financial value, appropriate measures should be designed, selected and integrated to prevent, detect and/or minimize the fraud in a timely manner (refer to **figure 3**). These measures can be built-in controls (BICs), integrated as part of particular processes to deter potential frauds, or early warning signals (EWSs) on occurrence of frauds. **Figure 5** provides samples of BICs and EWSs for consideration.

Figure 5—Fraud Prevention Analysis		
IT Process	Internal Controls	
	BICs	EWSs
<p><i>Manage projects/Acquire and maintain application software</i></p> <p>An IT application is designed to streamline the mortgage loan application process. The approval logic depends on the amount of the loan and hence requires approvals from different personnel with appropriate approval limits.</p>	<ul style="list-style-type: none"> • Approval functions or features to enforce the business requirement • Control to approve feature or function and the related system parameter • Audit trail on above 	
<p><i>Manage data</i></p> <p>While it is not practical to impose too many controls on accessing sensitive information (e.g., customer information) as part of daily operations, observations on various EWSs can be indicators of potential fraud in abusing company assets.</p>		<ul style="list-style-type: none"> • Accessing the sensitive data outside office hours, from unusual login location, excessive login attempts by system/security administrator • Removal of complete audit trail or part of an audit trail

Fraud Detection

The *2006 Report to the Nation on Occupational Fraud and Abuse* indicates that around 34 percent of fraud cases were uncovered by advice being received (e.g., through the use of whistle-blower facilities), and a total of 51.4 percent were detected by the combination of internal audits, internal controls and external audits. There is little doubt that discovery of fraud by auditors relies heavily on evaluating and testing the operating effectiveness of adopted controls. But what percentage of fraud cases do IT auditors actually uncover? Currently, most of the IT audit programs appear to focus on compliance with established procedures and standards on operations of IT systems and applications, but with few internal control questionnaires (ICQs) aimed to detect potential fraud activities and to

ascertain the effectiveness of antifraud control measurements in practice. Some possible explanations as to why this deficiency exists are that IT auditors:

- Tend to be too technically oriented

- Expect that uncovering fraud is the responsibility of financial auditors only

- Do not anticipate discovering any fraud activities when performing IT audits

Upon the completion of a fraud risk assessment with linkages to IT processes and associated detective controls, the IT auditor can build ICQs to evaluate and test adopted controls, including the antifraud programs. While financial auditors can evaluate the controls over a business's financial records and the appropriateness of its business operations, IT auditors should be focusing in areas around ICT systems and ICT-related processes. The quality of ICQs in detecting potential fraud may be strongly influenced by an IT auditor's competency in a technical sense, expert knowledge in specific areas (e.g., software programming, database administration, network design, network implementation, IT security), and insight to both IT and business operations. The development of these ICQs may reference established procedures within an organization, industry best practices and/or regulatory requirements.

For example, the complexity of technical and business arrangements in international long distance (IDD) call operations allows the fraudster to concede related activities from the company's financial record. Due to the "fixed" communication cost of the IDD provider, the fraudster could configure the IDD system to serve other IDD service providers without being detected by a financial auditor. In such a scenario, the fraud could be revealed by ICQs on system change controls, validation of system and/or application logs, or the logical security controls of the IDD system.

Fraud Investigation

The extensive use of ICT in today's business implies that evidence is extremely likely to be available for verification and confirmation as to an occurrence of a fraud. Evidence collected on ICT systems could well be used to sustain the occurrence of a fraud case. IT auditors tend to be better equipped with specialized knowledge on the behaviors of IT systems, and it is only a matter of whether an IT auditor is able to detect the fraud. To this extent, IT audits may either initiate or assist a fraud investigation through one or more of the following activities:

- Generation and/or reconciliation of report

- Identification/retrieval of evidence and missing records on computer system

- Conducting of computer forensics analysis

While an IT auditor may not be competent in conducting computer forensics analysis, the auditor should be aware of its methodology and capability.

Conclusion

IT auditors are expected to be involved in auditing for fraud both directly and indirectly. This article provides a fraud risk assessment approach covering various areas of fraud control through IT auditing, including:

- Integrating controls in the early stages of IT project development

- Raising necessary BICs and identifying EWSs as references for fraud prevention

- Developing ICQs around the process (both IT and business) instead of being technically focused

- Initiating and assisting in fraud investigations through the identification and recovery of direct and circumstantial evidence

The ability to identify and investigate a fraud by an IT auditor is strongly influenced by the extent of the IT auditor's knowledge of the business operations, IT process and technical know-how. Through this report, it is expected that IT auditors will have obtained a better understanding of the common practices that allow an enhanced level of fraud detection in an IT environment.