Information Risk and Risk Assurance in Auditing

Accounting is the art of recording, classifying and summarising of economic events in a logical manner for the purpose of providing financial information for decision making by the users of the accounting information. To provide relevant information, accountants must have a thorough understanding of the principles and rules that provide the basis for the preparation of the accounting information. While conducting the auditing of accounting data, auditors' attention is on determining whether recorded accounting information properly reflects the economic events that occurred during the accounting period. This is because international accounting standards provide the criteria for evaluating as to whether the accounting information is properly recorded and reflected through financial statements and for this purpose the auditors must also understand those accounting standards. As society becomes more complex, decision makers are more likely to receive unreliable information. There are several reasons for this unreliable information and this unreliability of information invites risk. Auditing has no effect on either the risk-free interest rate or business risk, but it can have a significant effect on information risk. This article analyses the concept of Information Risk and Risk Assurance in auditing.

Dr. (CA.) Sanjib Kumar Basu

(The author is a member of the Institute and Faculty Member, Department of Commerce, St. Xavier's College, Kolkata. He can be reached at eboard@icai.org)

Need for Accurate Financial Information

In order to get the idea about the need of accurate information, the process of decision making by a bank manager in granting a loan to a business (customer) can be considered. This decision of the bank manager for granting loan to the customers will be based on a number of factors such as previous financial relationships with the customer and the present financial condition of the business as reflected by its financial statements. If the bank makes the loan, it will charge a rate of interest determined primarily by three factors. These are:

1. **Risk-free interest rate:** This is approximately the rate the bank could earn by investing in Government Bonds for the same length of time as the business loan.
2. **Business risk for the customer:** This risk reflects the possibility that the business will not be able to repay its loan because of unfavourable economic

or business conditions, such as recession, poor management decisions or unexpected competition in the industry in which this business belongs.

3. **Information risk:** Information risk reflects the possibility that the information upon which the business risk decision was made is inaccurate. A likely cause of the information risk is the possibility of inaccurate financial statements.

Auditing has no effect on either the risk-free interest rate or business risk, but it can have a significant effect on information risk. If the bank officer is satisfied that there is minimal information risk because the borrower's financial statements are audited, then the bank's risk is substantially reduced and the overall interest rate to the borrower can be reduced. The reduction of information risk can have a significant effect on the borrower's ability to obtain capital at a reasonable cost.

Causes of Information Risk

As society becomes more complex, decision makers are more likely to receive unreliable information. There are several reasons for this unreliable information and this unreliability of information invites risk.

The reasons for the unreliable information are:

i. **Remoteness of information**
In a global economy, it is nearly impossible for a decision maker to have much firsthand knowledge about the organisation with which they do business. Information provided by others must be relied upon. It is the fact that when information is obtained from others, the likelihood of its being intentionally or unintentionally misstated, increases.

ii. **Biases and motives of the provider**
If information is provided by someone whose goals and objectives are inconsistent with those of the decision maker, the information provided may be biased in favour of the provider. The reason can be honest optimism about future events or an intentional emphasis designed to influence users. In either case, the result is a misstatement of information. For example, when a borrower provides financial statements to a lender, there is considerable likelihood that the borrower will bias the statements to increase the probability of obtaining a loan. The misstatement could be incorrect rupee amounts or inadequate or incomplete disclosures of information.

iii. **Voluminous data**
As organisations become larger, so does the volume of their economic events and transactions. This increases the likelihood that improperly recorded information is included in the records- perhaps buried in a large amount of other information. For example, if a large business organi-sation overpays a vendor's invoice by ₹20,000, it is unlikely to be uncovered unless the concern has instituted reasonably complex procedures to find this type of misstatement. If many minor misstatements remain undiscovered, the combined total can be significant.

iv. **Complex exchange transactions**
In the past few decades, economic events and trans actions between organisations have become increasingly complex and therefore more difficult to record properly. For example, the correct accounting treatment of the business combination of one entity with another poses relatively difficult accounting problems. Other examples include properly combining and disclosing the results of operations of subsidiaries with the parent organisation in different industries and properly disclosing derivative financial instruments as prescribed in the applicable accounting standards.

"After comparing costs and benefits and required analysis, business managers and financial statement users may conclude that the best way to deal with information risk is simply to have it remain unreasonably high. A small company may find it less expensive to pay higher interest costs than to increase the cost of reducing information risk. For larger businesses, it is usually practical to incur costs to reduce information risk."

Reducing Information Risk

After comparing costs and benefits and required analysis, business managers and financial statement users may conclude that the best way to deal with information risk is simply to have it remain unreasonably high. A small company may find it less expensive to pay higher interest costs than to increase the cost of reducing information risk.

For larger businesses, it is usually practical to incur costs to reduce information risk. There are three ways to do so. These are:

i. **User verifies information**
The user may go to the business premises to examine records and obtain information about

the reliability of the financial statements. Normally, this is impractical because of cost. In addition, it is economically inefficient for all users to verify the information individually. Nevertheless, some users perform their own verification. For example, tax department does considerable verification of business and individual tax returns to determine whether the tax returns filed reflect the actual tax due to the government. Similarly, if a business intends to purchase another business, it is common for the purchaser to use a special investigation team to independently verify and evaluate key information of the prospective business.

ii. **User shares information risk with management**
There is considerable legal precedent indicating that management is responsible for providing reliable information to the users. If users rely on inaccurate financial statements and as a result incur a financial loss, they may have a basis for lawsuit against management. A difficulty with sharing information risk with management is that users may not be able to collect on losses. If a company is unable to repay a loan because of bankruptcy, it is unlikely that management will have sufficient fund to repay users.

iii. **Audited financial statements are provided**
The most common way for users to obtain reliable information is to have an independent financial audit. Decision makers can then use the audited information on the assumption that it is reasonably complete, accurate and unbiased.

Typically, management of a private company or the audit committee for a public company engages the auditor to provide assurances to the users that the financial statements are reliable. If the financial statements are ultimately determined to be incorrect, the auditor can be sued by both the users and the management. Auditors obviously have considerable legal responsibility for their work, because they are providing required assurance about the reliability of accounting information to the users of the information including the management and the shareholders.

Information Assurance Services

An assurance service is an independent professional service that improves the quality of information for decision makers. Such services are valued because the assurance provider is independent and perceived as being unbiased with respect to the information examined. Who are responsible for making business decisions seek assurance services to help improve the reliability and relevance of the information used as the basis for their decisions.

"Information assurance" covers all activities that deal with the issues raised by the following key information security concepts. This includes:

- Ensuring the integrity, authenticity and reliability of information;
- Providing unambiguous identification and availability of this information;
- Establishing which individuals are authorised to view, edit and transmit the information;
- Protecting sensitive information from illegitimate recipients or interference, and unsuspecting recipients from false information;

Assuring information security is central to the success of any business activity. This is particularly pertinent in the age of modern technology, when information can leak and spread like a viral infection, and politically sensitive issues such as ID theft can bring down powerful individuals, businesses and government parties. There are nine key concepts of information security, encompassing technology, law, best practice and ethics.

- Regulating what legitimate users do with the information to which they have access.

Key concepts of information security

Assuring information security is central to the success of any business activity. This is particularly pertinent in the age of modern technology, when information can leak and spread like a viral infection, and politically sensitive issues such as ID theft can bring down powerful individuals, businesses and government parties.

Nine key concepts of information security, encompassing technology, law, best practice and ethics are:

1. Confidentiality

As an information security concept, confidentiality relies on the premise that there is some information which should be accessed only by certain people. If this principle is accepted, then we might create in addition information categories that reflect the degree of confidentiality required.

For example, we might argue that medical records should be completely private (available

only to the individual and the appropriate medical practitioners), internal (shared with all medical practitioners, and perhaps also with members of the individual's family) or public.

Maintaining confidentiality is a three-step method:

- authentication (establish the identity of the proposed recipient)
- authorisation (confirm whether the proposed recipient is authorised to receive the information)
- access control (regulate the level of access available to the proposed recipient, e.g. through the use of 'read-only' texts).

2. Integrity

Within the context of information security and risk management, 'integrity' means ensuring that data remains unchanged while in storage or transmission. This affects policies regarding both official records and also communication systems.

When sending an e-mail, we rely on the security of the IT system to ensure that the e-mail reaches the intended recipient intact. When we enter or retrieve data from a spreadsheet, we do not expect the information to change, either by technological fault or through illegitimate interference.

One means of establishing the integrity of data storage or communication systems are computational techniques for verifying data, including comparisons, checksums, message authentication and message digests.

3. Accountability

'Accountability' holds an unusual position within the world of information security and risk management. Essentially, it is a means of protecting information. However, unlike the digital signatures, passwords and encryption familiar to the technology savvy, accountability deals with the interface between information security, law and ethics.

According to Andreas Schedler (in his article *Conceptualising Accountability*) the basic illustration of accountability can be states as follows: "A is accountable to B when A is obliged to inform B about A's (past or future) actions and decisions, to justify them, and to suffer punishment in the case of eventual misconduct." In real terms, this means understanding and fulfilling one's own responsibilities regarding information security. At its simplest, these might include not sharing the contact details of customers with commercial organisations. At higher levels of management, individuals might be responsible for communication or even establishing suitable information security policies.

Within the sphere of corporate governance, accountability also encompasses issues such as: to which individual or organisation a business leader should be accountable; how organisational policies can be regulated; and how much control the government should exercise over the information security policies of individual public sector departments.

4. Non-repudiation

As a general concept, 'repudiation' means that a party denies the validity of a statement or a contract (for example, by claiming that a signature has been forged). Within the context of information security, 'non-repudiation' means that a statement or contact cannot be repudiated. This might be provided by a service that guarantees authentication or proof of the integrity and origin of the data. Familiar technological means of providing non-repudiation are digital signatures and certificates.

5. Authenticity

If a toy car says *Made in Japan*, we usually take this on trust. If a wine-seller claims that the bottle we have bought is from Singapore, then we would expect this information to be accurate. If we receive a new pin code from the bank, then it is vital that we can rely on the authenticity of the information – that is, assurance that the information exchanged is from the source that it claims to be from.

This assurance can be provided through something that the user knows (e.g. a password or a pin code), something that the user has (e.g. an ID card or a digital certificate) or even something that the user is (e.g. checking fingerprints and iris-scanning).

6. Identification

So much of information security is concerned with protecting sensitive information from illegitimate users that there is a danger of forgetting the importance of protecting unsuspecting users from false or inaccurate information. Within the context of information security,

"Information assurance is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of Information Assurance encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security which in turn grew out of practices and procedures of computer security."

Some practitioners make the mistake of thinking of the integrity attribute as being only data integrity. While data integrity is a major part of this attribute, it is not everything. This attribute also addresses whether the physical and electronic systems have been maintained without breach or unauthorised change. It even refers to the people involved in handling the information; are they acting with proper motivation and integrity.

'identification' means the capability to retrieve, edit and report specific data without ambiguity. This capability is usually delivered through the use of unique reference codes, such as ID numbers.

7. Reliability

Information reliability is primarily concerned with the information that needs to be retained about the author or source of information to assure its authenticity. This raises issues regarding version control (logging information about the changes made to versions of a document or product), archiving and document reviews.

In terms of information security, 'reliability' also means ensuring that information or an information system is protected against tampering and fraud.

Information Assurance Process

The Information Assurance process typically begins with the enumeration and classification of the information assets to be protected. Next, the Information Assurance practitioner will perform a risk assessment. This assessment considers both the probability and impact of the undesired events. The probability component may be subdivided into threats and vulnerabilities. The impact component is usually measured in terms of cost. The product of these values is the total risk.

Information assurance is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of Information Assurance encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security which in turn grew out of practices and procedures of computer security.

In the 1960s, Information Assurance was not as complex as it is today. Information Assurance was as simple as controlling access to the computer room by locking the door and placing guards to protect it. Since the 1970s, information security has held confidentiality, integrity and availability (known as the CIA triad) as the core principles. One newer model of Information Assurance adds Authentication and Non-repudiation to create the five Pillars of Information Assurance. In contrast, Donn B. Parker developed a model that added three attributes of authenticity, utility, and possession to the core C-I-A.

Therefore, there are three basic models used in the practice of Information Assurance to define assurance requirements and assist in covering all necessary aspects or attributes.

- The first is the classic information security model, also called the CIA Triad, which addresses three attributes of information and information systems, confidentiality, integrity, and availability. This C-I-A model is extremely useful for teaching introductory and basic concepts of information security and assurance; the initials are an easy mnemonic to remember, and when properly understood, can prompt systems designers and users to address the most pressing aspects of assurance.
- The next most widely known model is the Five Pillars of Information Assurance model, promulgated by the U.S. Department of Defense in a variety of publications, beginning with the National Information Assurance Glossary, Committee on National Security Systems. The Five Pillars model is sometimes criticised because authentication and non-repudiation are not attributes of information or systems; rather, they are procedures or methods useful to assure the integrity and authenticity of information, and to protect the confidentiality of the same.
- A third, less widely known Information Assurance model is the Parkerian Hexad, first introduced by Donn B. Parker in 1998. Like the Five Pillars, Parker's Hexad begins with the C-I-A model, but builds it out by adding authenticity, utility, and possession (or control). It is significant to point out that the concept or attribute of authenticity, as described by Parker, is not identical to the pillar of authentication as described by the US Department of Defense.

Information assurance is closely related to information security and the terms are sometimes used interchangeably. However, Information Assurance's broader connotation also includes reliability and emphasises strategic risk management over tools and

tactics. In addition to defending against malicious hackers and code (e.g., viruses), Information Assurance includes other corporate governance issues such as privacy, compliance, audits, business continuity, and disaster recovery. Further, while information security draws primarily from computer science, Information Assurance is interdisciplinary and draws from multiple fields, including accounting, fraud examination, forensic science, management science, systems engineering, security engineering, and criminology, in addition to computer science. Therefore, Information Assurance is best thought of as a superset of information security.

The core principles as described in different models are discussed below:

I. Core Principles as per CIA Triad

a. Confidentiality

Confidentiality is the assurance that information is not disclosed to unauthorised individuals, processes, or devices. Confidential information must only be accessed, used, copied, or disclosed by users who have been authorised, and only when there is a genuine need. A confidentiality breach occurs when information or information systems have been, or may have been, accessed, used, copied or disclosed or by someone who was not authorised to have access to the information.

For example, permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it would be a breach of confidentiality if they were not authorised to have the information. If a laptop, which contains employment and benefit information about 100,000 employees, is stolen from a car could result in a breach of confidentiality because the information is now in the hands of someone who is not authorised to have it. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorised to have the information.

b. Integrity

Some practitioners make the mistake of thinking of the integrity attribute as being only data integrity. While data integrity is a major part of this attribute, it is not everything. This attribute also addresses whether the physical and electronic systems have been maintained without breach or unauthorised change. It even refers to the people involved in handling the information; are they acting with proper motivation and integrity.

Integrity means data cannot be created, changed or deleted without proper authorisation. It also means that data stored in one part of a database system is in agreement with other related data stored in another part of the database system (or another system).

For example, a loss of integrity occurs when an employee accidentally or with malicious intent, deletes important data files. A loss of integrity can occur if a computer virus is released onto the computer. A loss of integrity can occur when an on-line shopper is able to change the price of the product they are purchasing.

c. Availability

Availability is timely, reliable access to data and information services for authorised users. Availability means that the information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is needed. The opposite of availability is the lack thereof, one example of this is a common attack known as a denial of service attack.

"Authenticity is necessary to ensure that the users or objects (like documents) are genuine (they have not been forged or fabricated). As files are shared across multiple organisations, there can be circumstances when duplicate copies of that file may exist. In such cases, it is important to establish not only which is the master copy, but also to establish a way for those who use the data to know where file, and all of the tagged data sets in the file, came from. A Tagged Data Authority Engine is one way to do this."

II. Additional Pillars as Given in Newer Model

a. Authentication

Security measure designed to establish the validity of a transmission, message or originator or a means of verifying an individual's authorisation to receive specific categories of information is considered as authorisation in this context. Authentication breach can occur when a user's login id and password is used by unauthorised users to send unauthorised information.

b. Non-repudiation

Non-repudiation indicates the

Based on the risk assessment, the Information Assurance practitioner will develop a risk management plan. This plan proposes countermeasures that involve mitigating, eliminating, accepting or transferring the risks and considers prevention, detection, and response. Countermeasures may include tools such as firewalls and anti-virus software, policies and procedures such as regular backups and configuration hardening, training such as security awareness education or restructuring such as forming a computer security incident response team or computer emergency response team.

assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. Non-repudiation implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. For example, electronic commerce uses technology such as digital signatures to establish authenticity and non-repudiation.

III. Donn B. Parkers' Additional Issues

a. Authenticity

Authenticity is necessary to ensure that the users or objects (like documents) are genuine (they have not been forged or fabricated). As files are shared across multiple organisations, there can be circumstances when duplicate copies of that file may exist. In such cases, it is important to establish not only which is the master copy, but also to establish a way for those who use the data to know where file, and all of the tagged data sets in the file, came from. A Tagged Data Authority Engine is one way to do this.

b. Utility

Utility means usefulness and usability. For example, suppose someone encrypted data on disk to prevent unauthorised access or undetected modifications – and then lost the decryption key that would be a breach of utility. The data would be confidential, controlled, integral, authentic, and available – they just wouldn't be useful in that form. Similarly, conversion of salary data from one currency into an inappropriate currency would be a breach of utility, as would the storage of data in a format inappropriate for specific computer architecture. A tabular representation of data substituted for a graph could be described as a breach of utility if the substitution made it more difficult to interpret the data. Utility is often confused with availability because breaches such as those described in these examples may also require time to work around the change in data format or presentation. However, the concept of usefulness is distinct from that of availability.

c. Possession

Possession means custody or control over the information, i.e., under whose control the information is kept. If everyone would have the access to the information generated, that can be considered as a good sign for the organisation. However, if the unauthorised possession of the information is with the persons at the input end, that creates problems to the information users and also it throws a great challenge to the information security profile of the organisation.

Conclusion

Based on the risk assessment, the Information Assurance practitioner will develop a risk management plan. This plan proposes countermeasures that involve mitigating, eliminating, accepting or transferring the risks and considers prevention, detection, and response. Countermeasures may include tools such as firewalls and anti-virus software, policies and procedures such as regular backups and configuration hardening, training such as security awareness education or restructuring such as forming a computer security incident response team or computer emergency response team. The cost and benefit of each countermeasure is carefully considered. Thus, the Information Assurance practitioner does not seek to eliminate all risks, were that possible, but to manage them in the most cost-effective way.

After the risk management plan is implemented, it is tested and evaluated, perhaps by means of formal audits. The Information Assurance process is cyclical; the risk assessment and risk management plan are continuously revised and improved based on data gleaned from evaluation.

References

1. *Auditing and Assurance Services- Arens, Elder and Beasley: ACL Publisher (13th Edition).*
2. *Principles of Auditing- An Introduction to International Standards on Auditing- Rick Hayes, Roger Dassen, Arnold Schilder and Philip Wallage: Pearson Education Schweiz.*
3. *Auditing Cases- Beasley, Buckleas, Glover and Prawitt: Prentice Hall (4th Edition).*
4. *Parker, Donn B. (1998). Fighting Computer Crime. New York.*
5. *Parker, Donn B: Towards a New Framework of Information Security- The Computer Security Handbook (4th Edition) - John Wiley, New York.* ■