To Our Readers

The Institute of Chartered Accountants of India has, of recent, placed considerable emphasis on Information Technology related areas. This is not merely because it is something that India and Indians are supposed to be good at. It is also because corporates, banks and almost everybody else is waiting up to the fact that Information Technology related investments are now an imperative. As businesses grow and spread geographically, and as the number of transactions become astronomical, and more, as the amount of information demanded by customers, shareholders and stakeholders in general multiply, there is no other way but to invest in Information Technology.

But this investment carries with it its own risks. As data bases become larger, and as number of users of these data bases increase geometrically, so does the risk of invasion of the whole system. And since all departments and functional areas of a company are linked to each other, the possibility of that invasion penetrating into company secrets is very real.

It is for that reason, that Information Systems Audit including audit of information security is now emerging as an essential part of Business Risk Management. However, Boards and managements across the globe do not necessarily see things this way. Perhaps it is because it is easier to understand the need for putting in physical security to protect companies' assets. The realisation that information is also an equally important asset, and the need to spend money in order to protect, is sadly lacking.

One of the reasons could be that Boards are accustomed to see things in quantifiable terms. One of the challenges of managing risks is convincing a company's decision makers to spend a lot of resources to protect their information assets. Where there is poor IT security and inadequate auditing of it, someone can bring an entire industry to its knees.

To obtain the necessary funding for Information Risk Management, internal auditors must report their concerns to Boards in a framework that the Board can understand – Cost Benefit Analysis or concrete comparisons of IT security risks with physical risks. Boards need to understand that Information Technology is a strategic initiative. The price includes controls and a commitment to continual employee training to keep the controls adequate and regular information security audit. Internal auditors need to draw the attention of Audit Committees to examine the significance of these issues and assign money values.

While it is difficult to assign money values to unknown risks, nevertheless both internal auditors and Information System auditors need to work on clear statements for minimising the risk of maximum loss, be it through the leakage of trade secrets and formulas, or marketing and pricing strategies. The internal auditors' role is to help the organisation to design a cost effective solution for ensuring the security and privacy of information assets. This can be done by using the chartered accountants skills in internal control and auditing, supported additionally by acquired skills in information systems and security auditing.

The Institute of Chartered Accountants of India is putting greater stress on its already popular ISA Course and the Council of the Institute has recommended to the Government for approval of a course on Information Security Audit. This trend may result in India also having the largest pool of chartered accountants who are also information system audit qualified and this in turn, will vastly increase the professional opportunities available to the members of the Institute.

November, 2002

Editor
The Institute of Chartered Accountants of India