Audit of Automated Systems & Compliance– The Way Forward

The Companies Act, 2013 has two very important Sections, 134 & 143, which are on similar lines to Section 302 & 404 of the Sarbanes Oxley Act. The Governance, Risk & Compliance (GRC) space has generated worldwide interest after the enactment of specific corporate laws by the regulators. Many organisations focus mainly on the "C" part, to ensure that they comply with the laws and regulations of the land. However, when laws specifically prescribe that a governance system must exist, risks identified and controls are tested for its adequacy and effectiveness, the consequences can be far reaching. In order for the Directors or Auditors to pass an opinion on the adequacy and effectiveness of controls it is imperative that controls are monitored on a continuous basis. To achieve this, risks and key risk indicators must be identified and the relevant controls that are required to mitigate the risks must be built into the business processes. Any unwanted or suspicious event must be automatically captured and highlighted to the senior management for taking corrective or preventive action. Read on…

Current Scenario

Section 134 of the Companies Act, 2013 on "Financial statement, Board's report, *etc.*" states *inter alia*:

(5) *The Directors' Responsibility Statement referred to in clause (c) of sub-Section (3) shall state that:*

(c) the directors had taken proper and sufficient care for the maintenance of adequate accounting records in accordance with the provisions of this Act for safeguarding the assets of the company and for preventing and detecting fraud and other irregularities;

(e) the directors, in the case of a listed company, had laid down internal financial controls to be followed by the company and that such internal financial controls are adequate and were operating effectively.

Explanation: For the purposes of this clause, the term "internal financial controls" means the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and

CA. Babu Jayendran

(The author is a member of the Institute. He can be reached at babujay@gmail.com)

detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information

(f) the directors had devised proper systems to ensure compliance with the provisions of all applicable laws and that such systems were adequate and operating effectively.

Section 143 of the Companies Act, 2013 on "Powers and duties of auditors and auditing standards" states *inter alia*:

(3) The auditor's report shall also state:

(i) whether the company has adequate internal financial controls system in place and the operating effectiveness of such controls.

When we talk in terms of "adequacy and effectiveness of controls" it refers to the adequacy of the control design and whether the control has been working effectively during the relevant financial year. The impact of this statement is that it involves continuous control monitoring during the year and not a review "as at" a particular date.

Challenges

In automated systems, this requires a good understating of the software application supporting the business and the company's information technology environment, in order to pass an opinion on the adequacy and effectiveness of controls.

It is a well-known fact that the IT world thrives on jargon. This has led to many non-IT personnel, getting confused, and avoiding the issue of IT threats and vulnerabilities and addressing the associated exposures and risks. Organisations spend substantial amounts to capture data. Raw data is useless unless it is converted into some meaningful information for decision-making. If this information is not correct or accurate it adds to our problems. The irony of this scenario is that the risks associated with such data processing activities have not been given the importance it deserves.

If we address the following questions to the environment we work in, the answers could be revealing:

- Are the financial statements correct?
- Are the systems that generate these statements secured?
- Data, a company's most valuable asset, is it protected?
- Is the information being obtained in the most effective and efficient manner?
- Is the information reliable and available when needed?
- Are laws and regulations being complied with?
- Is the information accurate?
- Is the company management aware of the potential exposures and risks?

As the saying goes "ignorance is bliss," but in Information Technology driven organisations such ignorance can be costly.

In the olden days of manual accounting, any changes made to the books of accounts was visible. Computer data is not visible and reports generated always look neat and correct. In very simple terms, data is processed by computers using programmes written by human beings - who do make mistakes! This can have grave consequences, since computers have the uncanny ability to keep doing the same mistake again and again until detected and corrective action taken. CAs who normally play a very important role in any organisation should identify the risks of all business processes, define the security policies and procedures and ensure adequate controls are in place to mitigate the risks. There is a school of thought that feels that controls can be unproductive and there is no real value added to the business. This is not true. Controls ensure that unwanted events are prevented, detected and corrected.

Opportunities

Major corporations worldwide have used Information Technology (IT) to stay ahead in business. The competitive edge in terms of fast information flow, to support the business, can be an important factor between success and failure.

The efficiency of an enterprise depends on the quick flow of information across the complete supply chain, *i.e.*, from the customer to manufacturers to the suppliers. With the globalisation of the market place coupled with competition and increasing customer expectations organisations have to address certain fundamental areas like lowering costs in the supply chain, reducing throughput times, optimising stock levels, improving product quality, improving service to the customer, efficiently handling cross border data flow *etc.* Today's IT systems achieve all this.

The core to any organisation's success is to have an efficient and effective financial information system to support decision-making and monitoring. As CAs we have to be involved, in order to ensure that the organisation's information architecture has been

designed properly to meet the business objectives. The risks, controls and security of such systems should be clearly understood if we have to pass an objective opinion about the adequacy of control in an IT environment.

The gruelling training of the CA course has created CAs with an excellent understanding of business processes and its impact on the financial statements. From the time of articleship, tracing source documents to financial statements is a daily phenomenon. Understanding data flow within or across an organisation is part of the DNA of any CA. This is a very powerful skill set. The world today is looking for Business Process Experts who can use their domain knowledge to make business processes efficient, effective and risk free. The most logical professionals to fill this gap are Chartered Accountants.

Organisations would prefer to talk to consultants that see the 'big picture.' Today, many organisations work in two 'silos': domain, and technology! Communicating across silos is not easy since CAs may talk "debits & credits" while technologists in terms of "Java, .Net, JBoss, Linux, ABAP," *etc.*! There has to be a cross over for things to happen efficiently andeffectively. If CAs go that extra mile in understanding technology the returns to the organisation and the individual can increase manifold!

Audit of Automated Systems–The Way Forward

CA's should leverage on the fact that all information in today's corporate world is digitised. This makes it easier for auditors to use machines to do the "number crunching" and analytics and use the results generated to pass an opinion.

Organisations today capture hoards of raw data. Data must be converted to meaningful information for the management to make the right decisions. Interpretation of data and its usefulness can only be effectively done by persons with domain knowledge. CAs can contribute extensively in this area.

A number of organisations today have disparate systems co-existing and a number of tools have evolved to make these systems talk to each other. So in reality, we have an abundance of base software to do business, analytics and integration.

Organisations have spent millions to implement high-end ERP systems and Business Intelligence tools. However, the irony is that as the information moves higher up the organisation structure it starts moving into Excel spreadsheets for consolidation and decision-making. Does this make sense? I call this the 'Excel Syndrome!' Data is taken from these high-end systems and entered in an excel sheet for MIS reporting. Why? With all the tools that we have today why isn't information consolidation happening the way it should? How is data integrity maintained? It is absolutely important that the decision-makers get the information from the same systems where the data is captured and all users should access the same data source. These are fundamental questions that CAs should ask.

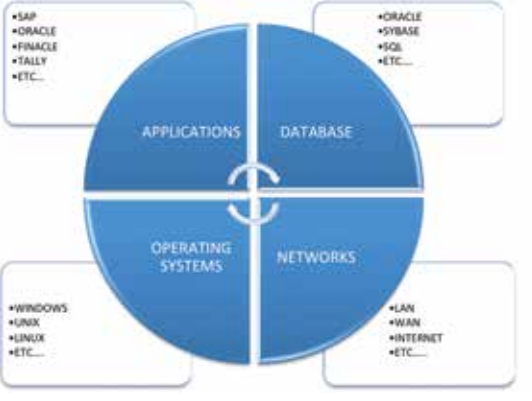
Is it because:

- the base systems are not aggregating the information in the manner in which the decision-makers want to see it?
- the consultants have not understood the requirements?
- the comfort level of using Excel is much more than using high-end systems?
- the terminology and jargon that keeps evolving in the tech world is confusing senior management?
- the functional and technology gap is widening?
- systems and solutions are growing at such a fast pace that it becomes difficult for persons at the top to comprehend the real benefits?
- of different technologies, protocols, formats, communication channels, *etc.*?
- entities are scattered across different geographies across the globe and this makes consolidation very difficult?

These questions could go on and on, but what is the answer? CAs can definitely contribute substantially in addressing these problems and finding solutions.

I would like to highlight below some important areas that need to be covered in the audit of automated systems:

Layers of Audit



At the very outset it is important to know the scope of audit, in the context of automated systems. In order to pass an opinion on the adequacy and effectiveness of controls, an auditor should cover the above layers. As you will appreciate, it is not possible for me to cover all the layers in an article. I will restrict myself to some important areas in Application Control.

Application Control

The "application" represents the software that supports the business. This can be SAP (© Copyright SAP AG) or any other software.

Application controls are required by the business and forms an integral part of each business process. This is generally implemented through normal business process mapping and system customisation processes. The major business processes must be audited and a review of the controls must cover three parts, namely Configuration, Transaction, and Master Data. In high-end applications these controls can be continuously monitored by defining data sources and business rules. Based on the number of deficiencies found, the system will automatically give a score on the adequacy and effectiveness of the controls. Control self-assessment is also provided so that the business process owner can answer a questionnaire on the control design, which basically refers to the adequacy of the control. The advantage of the automated monitoring is that if the business process owner indicates that the control design is adequate but the continuous control monitoring shows that a number of deficiencies have been identified, then the auditor can come to the conclusion that the control is not effective.

The table below indicates some sample automated controls:

BUSINESS PROCESSES					
Order Management	Set up policies & procedures	Enter sales orders			
Inventory & Shipping			Ship goods & perform services		
Accounts Receivable				Manage billing & receipts	
General Ledger					Recognise revenue
SAMPLE AUTOMATED CONTROL TO BE MONITORED					
Configuration		Monitor tolerances for customer order volume	Monitor tolerances for returns	Analyse receipts posting & document change rules	Monitor posting tolerances for revenue journals
Transaction		Analyse order amounts over company specific thresholds	Evaluate shipments without proper sales documents	Detect excessive returns & credits	Monitor adjusting journals for bad debts over company specific threshold
Master Data		Monitor customer creation and changes	Monitor goods receipts of unauthorized returns	Monitor pricing & exchange rate adjustments	Analyse changes to revenue accounts

CAs who normally play a very important role in any organisation should identify the risks of all business processes, define the security policies and procedures and ensure adequate controls are in place to mitigate the risks. There is a school of thought that feels that controls can be unproductive and there is no real value added to the business. This is not true. Controls ensure that unwanted events are prevented, detected and corrected.

The advantage of Continuous Control Monitoring & Event Monitoring is that, for all scenarios configured, the monitoring is done for the complete population and is not based on a sample. Further, if an Auditor's Role is created in a company with only "Read" rights, the auditor will be able to pass an opinion on the adequacy and effectiveness of controls, by reviewing exception reports, dashboards and heatmaps.

Access Controls

This represents the technical controls within an application that allow functions (business and technical) to be restricted to appropriate personnel, on a "need to know" basis. This includes access controls to various operating system and database technologies. This can be quite a complex review if the auditor is unaware of the company's system landscape. If users of systems have unauthorised access the potential of fraud can be high.

I would like to highlight my point of view by taking an example on Segregation of Duties (SOD) from the SAP (© Copyright SAP AG) environment.

Let us first try and understand the scenario in which most organisations work in. The responsibility for Security and Authorisations has evolved over a period of time and the staff that normally handles this function have been 'upgraded' from a technical background. Most of them are hard-core techies and excel in the tech space. Business transaction codes for them is nothing but a jumble of alphanumeric characters! It can be MM01, FB01 or VK01; it does not matter since they are normally not aware of the business process and the impact of the related risk, if there is an SOD violation. The reality is that they do not have business exposure and we do not expect them to know. Some techies have picked up this business knowledge over the years and I give them full credit for going that extra mile!

The fundamental principle of SOD is to ensure that in any business process the tasks of "Initiating", "Authorising," "Recording," "Processing," and "Reporting" are segregated so that no employee has access to any two tasks. The underlying assumption being that if they do, the potential of doing any fraudulent activity increases.

Let me give you an example to drive my point. Create Material Master Record 'MM01' conflicts with Create Purchase Order 'ME21', as per the globally accepted SOD rules. The risk is that the employee who has this access can create a Material in the Material Master and create a Purchase Order, to favor a specific vendor. The Mitigation Control could be that a Release Strategy has been configured for the Purchase Order to be released, which is given to another employee. It is extremely important that the individual who is reviewing this and granting the authorisations is aware of the risk and whether the mitigation control actually mitigates the risk. If the individual granting authorisation is not aware, the possibility of the organisation living with this risk cannot be ignored.

I am only trying to highlight the importance of individuals responsible for "Authorisations" being fully aware of business processes and its related risks. If this does not happen the organisation could be exposed to potential risks and as auditors will definitely have to highlight this as an audit finding.

The convergence of a CA's domain knowledge with the knowledge of the technology supporting access control can be an excellent combination for passing an opinion on the control design and effectiveness, as required by Section 143 of the Companies Act, 2013.

Pattern Recognition

Section 134, of the Companies Act 2013, talks about *"....preventing and detecting fraud and other irregularities...."*.

I do believe that, as much as auditors check the effectiveness of controls, fraudsters check the

The gruelling training of the CA course has created CAs with an excellent understanding of business processes and its impact on the financial statements. From the time of articleship, tracing source documents to financial statements is a daily phenomenon. Understanding data flow within or across an organisation is part of the DNA of any CA. This is a very powerful skill set.

ineffectiveness of controls! The reality is that fraudsters commit their fraudulent activities over a period of time, till they are detected. This temporal nature of their behavior makes it essential that auditors should look for suspicious patterns occurring over a period of time. Today, with the use of technology like Neural Networks and Artificial Intelligence, pattern recognition software is available which can identify suspicious activities and highlight such transactions in exception reports. This is particularly relevant when auditors have to handle 'big data'.

A changing environment requires an adaptive solution. It is necessary to pin point non-obvious relationships among transactions, accounts, customers and other entities. Machine learning algorithms coupled with data mining techniques are essential to discover the hidden truth behind each and every transaction for building the holistic intent across all channels and legal entities.

Given below are some technologies available for digital forensics:

- Business Intelligence
- Data Analytics
- Data Mining
- Statistical Analysis
- Rules
- Rule Builder
- Geo Spatial Analysis
- Artificial Intelligence
- Neural Networks
- Burst Detectors
- Pattern Analysis
- Clue Detectors
- Fraud Scenario Library
- Memoriser
- Link Analysis
- Profile Behavior
- Risk Profiling

These technologies can filter out suspicious transactions from large volumes of data, which the auditors can verify, with supporting evidence, to establish the genuineness of the transaction.

The world today is looking for Business Process Experts who can use their domain knowledge to make business processes efficient, effective and risk free. The most logical professionals to fill this gap are Chartered Accountants.

Conclusion

The Companies Act, 2013 has the vision of bringing in the best practices in the areas of Governance, Risk Management & Compliance, in the corporate sector. In my opinion, this will immensely benefit companies, the stake holders and of course the whole nation. In this environment, it is absolutely essential that organisations utilise the power of automated solutions to effectively monitor the GRC health of an organisation.

In order for the Directors or Auditors to pass an opinion on the adequacy and effectiveness of controls it is imperative that controls are monitored on a continuous basis. To achieve this, risks and key risk indicators must be identified and the relevant controls that are required to mitigate the risks must be built into the business processes. Any unwanted or suspicious event must be automatically captured and highlighted to the senior management for taking corrective or preventive action. I do believe that in the near future senior management will continuously get information, through dashboards or heatmaps, on their iPads, tablets or smart phones, on the GRC health of their organisation. May be, we could call this "MOM" – Monitoring on the Move!

Automated GRC solutions provide the functionalities to meet the requirements of the regulations and seamlessly integrates across modules. An enterprise GRC platform approach will allow companies to have complete management of all risks and controls from a single repository, which should give comfort to Directors, Auditors and other stakeholders. ■