G Padmanabhan: Issues in IT governance

Address by Mr G Padmanabhan, Executive Director of the Reserve Bank of India, at the College of Agricultural Banking, Pune, 16 July 2012.

*   *   *

Assistance provided by S/Shri P K Chopla, A Madhavan and D Nandi gratefully acknowledged.

Smt. Meena Hemchandra, Principal CAB, members of CAB faculty and participants; wish you all a very good morning. I thank the Principal for the privilege given to me to address this gathering of CTOs and CIOs of banks, who are responsible for managing information, the most valuable resource for banks today. It is indeed appreciable and thoughtful of the CAB to organize a programme with a theme which has great contemporary relevance.

Emergence of corporate governance

Let me start by briefly discussing about the general concept of Corporate Governance. As is commonly known, Corporate Governance is a process by which an institution is governed to achieve the set goals, resolving conflict of interest between different stakeholders, both internal and external. So, governance is primarily a Board level function, managing the affairs of the company, driven top-down, based on the principle of fiduciary duty, centered on oversight of management functioning, to ensure ethical, legal and regulatory compliance. However, the philosophy of corporate governance has been a bit nuanced in the geographical sphere. If the American model predominantly centered around shareholders interest and compulsory disclosures, the European-Japanese model encapsulated interest of the employees, managers, suppliers, community etc. In India, Securities and Exchange Board of India (SEBI) defined corporate governance as the "acceptance by management of the inalienable rights of shareholders as the true owners of the corporation and of their own role as trustees on behalf of the shareholders. It is about commitment to values, about ethical business conduct and about making a distinction between personal & corporate funds in the management of a company."[1] This scope has however undergone changes over time to include ethical conduct by the organization and its functionaries, rather than just ensuring strict compliance with laws and precise regulation. The changed interpretation about Governance and role of the Board has gained greater currency in the wake of some big ticket events like collapse of Enron, WorldCom, HIH and in the aftermath of recent crisis, where a large part of the blame was attributed, inter alia, to unethical conduct of various entities and market participants. As we all know, we are yet to hear the last word about the recent controversies ranging from the activities of a well known management "Guru" to the issue of "fixing" of LIBOR and the role of banking community.

IT governance

From the foregoing, what clearly emerges is that, Governance is being re-emphasized as an oversight function through which organizations ensure compliance with laws and regulations, not only in letter but in spirit as well, with adequate, effective safeguards for interests of all stakeholders and society. When we look at things in this context, the first thing to be safeguarded in an organization would be its assets and the resources that secure them. If the level of attention required to secure each asset is in proportion to its value and criticality,

[1] "Report of the SEBI Committee on Corporate Governance, February 2003". SEBI Committee on Corporate Governance. http://www.sebi.gov.in/commreport/corpgov.pdf.

then certainly, IT management would qualify to receive top most and special attention as part of the overall corporate governance process.

Information Technology, as we all know, has perhaps, impacted the banking and financial service industry more than any other sector. Almost all the business activities of this industry have undergone a kind of metamorphosis over recent times due to various factors, with Information Technology being amongst the most significant. The industry products, services, processes, channels, delivery modes and deliverables themselves have moved from physical to electronic, whether it is deposits, loans, assets, liabilities or specific business /product domains like G-sec, Forex etc. So, we have come to a stage in banking, where IT is the enabler, the most important driver and a crucial component of the business process itself. Further, the regulators and the stakeholders who are outside the organization as also the customers are highly concerned on the usage of IT and the risks associated with it So, it is imperative that all the related aspects are discussed and debated.

Mandating governance

The first major state intervention on the corporate governance practices was the enactment in the United States of the Sarbanes-Oxley Act of 2002 (SOX). Correspondingly, UK adopted the Combined Code, and OECD the Governance Principles. In all these enactments, compliance is mandatory, rather than “comply or explain”. After the promulgation of the SOX, the US standards setting bodies, such as, Security Exchange Commission (SEC), the, American Institute of Certified Public Accountants (AICPA), the US and Public Company Accounting Oversight Board (PCAOB) etc made significant efforts to enforce the SOX Act. Among the regulations and guidelines, Auditing Standard No. 2 has the most significant impact on IT governance. The IT governance requires testing of (i) IT general controls,(ii) checking IT process element at the time of each period-end financial reporting (iii) examining the IT process flow control of actual transactions and (iv) measuring the effectiveness of IT general controls over financial reporting. Thus, SOX had effectively mandated IT governance over financial reporting and operational control. The Basel accords, Basel II and Basel III, factored operational risk controls in aligning capital adequacy requirement and hence, IT governance in banks was a direct fall out of these accords. In the Indian context, we have elaborate clauses relating to corporate governance under the Indian Companies Act with the Companies Bill 2004, various regulatory guidelines from the regulators. Recently, the Reserve Bank appointed the Gopalakrishna Committee to look into various aspects of IT in the financial sector. The recommendations of the Committee – The Report of the Working Group on Electronic Banking – had exhaustively covered the issue of IT governance in banks

What do we mean by IT governance?

All the governance principles and practices are generally top down and the IT governance is no exception to this hierarchical initiative and responsibility. IT governance, as a subset of corporate governance, also requires to be driven from the board level. The core of the IT governance is to create IT strategy that forms part of the effective corporate strategic planning process and thus ensuring alignment of IT design and its controls with the business goals. The basic objectives of the IT governance can be summarized as follows:

- Aligning IT strategy with Business Strategy
- IT as strategic resource to deliver value
- IT risk management
- IT resource and financial management
- IT performance management

- IT Policies and Procedures

Before we begin to discuss some specific issues of the IT governance, let me caution that sometimes IT governance is confused with IT controls and operations. It needs to be appreciated that while IT governance is a strategy initiative, IT implementation, operations and control mechanisms are the means to ends.

Alignment of IT strategy with business strategy

It is imperative that the business strategy and IT strategy should go hand in hand, else the means would not lead to logical and planned ends. It is the business strategy which should necessitate and seek appropriate IT requirements and therefore, should clearly define how the IT should support the enterprise business strategy.

Further, the governance oversight also should ensure putting in place processes by which proper coordination is established at organisational level between CIO/CTO and CEO with members across the business units so that the IT deployment strategy synchronises with the business strategy in order to harness the full capability of the IT systems. Notwithstanding the timelines – be it short term or long term – it is the turnaround time of the IT strategy and its implementation that would be critical to the success of any business strategy. Therefore, at the board level it would be imperative to ensure that the business and IT units are not driven in silos.

Some of the important questions that arise in this context are: Who decides IT resource/asset requirement? Is it by IT team or by Business team? Or is it Board driven? Investment in IT is a strategic decision which will have large long term impact on the bank.

It is proven fact that the IT strategy of the firm and its declaration of IT investment plan impact the value of the firm.[2] IT strategy can be deployed differently in different circumstances and include:

- ***Automate*** – i.e. substituting manual intervention with automated business processes
- ***Provide information, at the asking, for decision making*** – i.e. provide correct information about business activities to senior management on time for taking right decision and also provide information about business activities to employees across the firm
- ***Transform*** – fundamentally redefine business and industry processes and relationships
- ***Combination of the above*** – While under normal circumstances automation could evolve over a period of time, in an incremental manner, typically in Kaizen mode, the sudden challenge of the quickly changing business environment may need sweeping transformation, in the Kaikaku mode.

It is important for any bank to be certain about what strategy they are following. When banks took upon the Core Banking implementation challenge, what was actually targeted? Was it 100% branches coverage or effective managerial control over the banking assets and liabilities or MIS or merely regulatory compliance and in the process harnessing residual benefits? Was it "Automate" strategy or simple "mechanisation"? Or was it the "Transform" strategy? Even after many years of CBS implementation banks are struggling to provide information required for decision making or not able to automate the regulatory report

[2] "The Value Relevance of Announcement of Transformational Information Technology Investment" – Bruce Dehning, Veron J. Richardson and Robert W Amud

requirements out of CBS. This raises the question whether the required alignment between business and IT strategies as also the involvement of business team in the automation process was there. To my mind it appears that in the initial stages banks were too keen to first automate the branch banking into core banking, relegating other important benefits that the full-scale automation could have provided. Perhaps on this score, the late entrants to the banking business started fresh on the IT front and reaped better benefits.

IT as strategic resource to add value

Do we validate or assess whether IT is delivering value addition to the business by means of customer service and satisfaction, improvement of internal processes, better controls to avoid fraud and better MIS for Decision Support System (DSS)? If the answer is yes, how many banks are using DSS and Business Intelligence (BI)? If technology is geographically neutral, then why do we charge for account services from branches other than the "home" branch? In the name of the risk management, do we drive even our physically challenged and differently abled persons to travel thousands of miles to the so called "home" branch to just collect the renewed ATM card and in the process collect their ire? I think we could have implemented CBS in our banks with better strategic thinking, of making IT as strategic resource to "Transform". Let us at least now put in place a proper IT Governance structure so that the mistakes are not repeated and we ensure that IT adds value to business. How do we do that? The answer, to a large extent, is ***Business Process Re-engineering (BPR)*** which is a very popular term but hardly practiced concept. Have we performed BPR while implementing CBS? Mostly the answer is No. Let me dwell a bit on the subject of BPR.

BPR is the mechanism through which the business processes are analysed by the subject matter experts with the knowledge of business and IT. Each and every existing business processes are analysed and re-designed to meet the current or future objectives by ushering in processes that are more efficient, secure, simple and customer friendly. The key success factor of BPR is to take care of three important aspects as follows:

- Evaluate the new business/IT requirement or review existing IT infrastructure to handle new business environment and ensure to put in place robust IT environment, preserving the existing investment to the possible extent. While network is the key element to be taken care of as applications are generally centralized, ensure that the DR systems and BCP related activities are in place.
- Involve subject matter experts and operations people to ensure the shared ownership of the system. If the business process change is owned by the operating staff, then the change management and implementation would be smooth.
- External experts can be associated to bring in rich experience. Brain storming by combination of business and IT teams with internal and external experts would add significant value while designing new systems.

IT risk management

It may be pertinent to mention that 70% of the operation risk in banking sector arises from IT risk. As per Basel guidelines banks are required to maintain additional capital for operational risk and there are incentives to those who manage it by implementing Advanced Measurement Approach (AMA). How many banks have moved towards AMA approach model for operational risk? Very few, if at all. Does this not point to inadequacy of IT risk management frame work in banks? Good IT process control would substantially reduce operational risk (if put in practice) and therefore, the risk management of IT resources themselves are the key for low operational risks. IT risk management is the integral part of IT governance.

The critical elements of IT risk relate to, Safety and Security, Availability, Performance and Compliance. What are the issues that need to be taken note of by the banks? The IT systems of the banks are often web enabled. This leads to better customer service and new delivery channel and the same time exposes the banks to greater risks. Various studies reveal that the incidence of malicious attacks are increasing and the nature of attacks are very dynamic and getting sophisticated. Are all the employees educated about IT security threats? Whether all employees are aware of Information Security policy of the bank? Do we periodically check the IT security incidence reporting and review the IS policy? If so how frequently? The types and numbers of security threats range from IP spoofing to Denial of Service attacks (DOS, Trojan horses, spams to malwares, etc and are mind boggling. Social hacking adds another dimension to this threat. The awareness of various attacks and putting in place proper IT infrastructure to protect the IT resources are very critical for ensuring business continuity. So, implementation of data center and DR systems are to be integrated with the overall BCP of the bank to ensure the availability of the business in extreme situations.

IT resource management

Let me flag some concerns. Do we put in place policies to review at Board level to monitor utilisation of infrastructure procured at a huge cost? Do we put in control measures that track the entire life cycle of the IT resource from procurement to end-of-life? Another important element to IT resource management is human capital management. Do we have a separate policy for grooming HR resource towards IT? Do we have a proper outsourcing policy? Are we using the right type of technology? For instance, should we go in for Virtualisation, cloud computing? Are we making adequate efforts to implement green computing? Some of these are difficult questions for many banks but critical for the officials attending this seminar to get answers to perform their roles effectively.

IT performance management

IT performance assessment and management is equally vital to ensure efficient IT services. Do we periodically stress test our systems? How much maximum volume can it handle in a single day? If for instance, all the NREGA payments are made as Electronic Benefit Transfers, do we have an idea about the possible daily volume? It could well be in millions. If all Government payments are made in electronic format, can the current IT systems of the agency banks handle them? In other words, how scalable is the IT system?

IT policies and procedures

IT implementation being key to sustenance of successful business require critical policies to be driven from the board level. These include:

- IT Administration policy and Procedures
- IT Asset management policy and Procedures
- IT Security Policy and Disaster Recovery Procedures
- IT Training and Support
- IT Project Management guidelines and procedures

Having discussed about the importance of IT in the world of business and banking, let us look at a related issue- the project management scenario. While IT has added great value to businesses there are innumerable examples of large IT project failures, time and budget over runs. Let me cite a few to emphasise the need for greater attention to be paid to this area. A project, named "Shield", aimed at providing live camera links from police cars and other fixed locations to a central command location in the US failed to achieve the desired results. Equipment failures, poor planning and poor training meant that as an integrated system, it was worthless. Staff was unfamiliar with how to use the system, the data collected through the system was of questionable value and failure to understand operating environment in which the system would function resulted in equipment that failed under the extreme temperatures that were not uncommon in those areas. Contributing factors as reported in the press were: lack of oversight, faulty equipment, poor training, underestimation of complexity and ineffective procurement practices.

Rollout of the Care Records Service component of the UK's National Program for IT ground to a halt after pilot sites reported significant problems. Already four years behind schedule, the initial pilot released in London was branded as shambles, as failure to address the culture change issues, coupled with "technical faults" to produce weeks of chaos at hospitals. After several months of working on the problems, the rollout was placed on hold and in Sep 2010, Department of Health announced that efforts to centralize health records were abandoned. Over the years many studies have shown high failure rates in the IT sector. As per a 2008 study by US Government Accounting Office (GAO), of 840 federally funded projects 49% of were poorly planned, poorly performing or both . A 2008 study by the Information Systems Audit and Control Association that found that 43% of 400 respondents admitted that their organization had a recent project failure. (Source – The Story Behind the High Failure Rates in the IT Sector).

A 2002 Gartner survey found that 20 percent of all expenditures on IT is wasted – a finding that represents, on a global basis, an annual destruction of value totaling about US $600 billion. A 2004 IBM survey of Fortune 1000 CIOs found that, on average, CIOs believe that 40 percent of all IT spending brought no return to their organizations. A 2006 study conducted by The Standish Group found that only 35 percent of all IT projects succeeded while the remainder (65 percent) were either challenged or failed. Many surveys have consistently revealed that 20 to 70 percent of large‐scale investments in IT‐enabled change are wasted.

Indian context

Before coming to some conclusions from the above incidents and survey reports let us come to the Indian context, where banking has traversed a long journey from the days of mechanization, followed by word processing on standalone PCs onto IT based applications. As things stand today the customer related functions in banks are all run on IT enabled systems. It is the reach and capacity of Information Technology that has enabled banks to overcome the constraints of geographical reach, enormously increasing transaction volumes and, to an extent, availability of human resources. Banks are gearing up to cater to fast increasing customer needs through IT based payment systems, internet based access and technology enabled service delivery modes. While banks keep churning out new projects, an important key to the success of any project/software is exception handling. While routine transactions generally go well executed, it is the exception handling that makes or breaks the software. While testing the software, adequate efforts should be made to prepare exhaustive test scenarios of exception and how the system handles them. That brings us to the most important software success factor – rigorous user acceptance testing. Assessing whether the current staff could professionally handle exception testing or they need the association of experts in testing is an important decision to be made every time a new project is taken up. The more rigorous the testing and exception handling, the higher would be the probability of success of the project.

Another area of significant importance to the managements, regulators and shareholders is the quality and efficiency of reporting. Indian banking, even today, has housekeeping, MIS and reporting processes which are largely interspersed with manual intervention. This has implications for the quality, consistency and timeliness of data; subjective interpretation, even manipulation and delays. In cases where the information collection and submission process are largely IT based, process design itself has to be aligned to reporting requirements. The risk remains that the management, board, regulators or the shareholders and customers may not get correct or timely information and disclosures due to inadvertent or deliberate action on the part of those compiling or submitting information. There have been instances of process design facilitating manipulation of data for monitoring and regulatory compliance, with serious implications. Automated data flow initiative by RBI is a step in the direction of effectively addressing these issues. Benefits for banks in such implementation are many. First of all this will result in cutting down the number of procedures and sub-processes in the MIS and regulatory reporting processes with lesser human resource deployment, having positive impact on cost and time parameters. Further, internal monitoring, review and decision making shall also be facilitated to become more efficient and effective, as the scope for misreporting is curtailed.

Have you ever debated in a group on further investments and support from IT in compliance with the tighter regulatory regime of the future? Banking regulation across the globe is undergoing tremendous change in the wake of recent financial crisis. Basel III requirements have enhanced the need for continuous monitoring of data on several parameters to ensure continuing rather than point of time compliance. There are new regulatory provisioning requirements which can be complied only by proper data collection, compilation, analysis and reporting. It is mandated that business decision making and regulatory reporting processes use the same data and information. Any lacuna in the integrity of data is increasingly being viewed adversely by the markets, customers, shareholders and regulators. It would be highly inefficient for banks to collect, compile and report on the basis of voluminous data on diverse parameters through processes having manual interventions. The time criticality is further heightened by the need to act and react fast in a highly competitive market environment where growth and survival require quick information dissemination and decision making. Risks and opportunities have to be spotted quickly, followed by swift action. So, it is in the interest of all stakeholders that a single view of information and data in the banks with automated/ straight through processing is ensured for internal and external reporting.

Our banks have come a long way by using the prowess of IT, but, IT deployment is still evolving and a lot more is yet to be done. So, what does it mean for the CTOs and CIOs? Well, an obviously increasing importance of role and enhancement in budgets; which come along with much higher responsibilities for design, execution, management of more, bigger IT projects and enhanced requirements for efficient, effective service delivery. Leanings from all the incidents and surveys can come in handy in decision making. There are a number of IT project failures, but reasons may be diverse and unique in each case. As rightly stated, "Decision-centric complexity is the essence of an IT project. While it's easy to get lured into a false sense of security because a Gantt chart can make an IT project look relatively simply, the underlying web of interrelated decisions is the dimension that makes managing IT projects so hard to do. By recognizing that dimension and understanding the many and varied factors that affect the way individuals, teams and organizations make decisions, organizations can start on the long road towards developing the levels of expertise needed to be able to improve their chances of success".(R. Goatham)

Having discussed about IT governance, where do the CTOs and CIOs come in? Well, everywhere, as far as the IT management and Governance space is concerned. I recently came across a blog on Archeology Institute site , where one opinion read, everyone knows that an IT manager's job is "to do the thing right and do the right thing". But as we know the original quote by Peter Drucker was "Efficiency is doing things right; effectiveness is doing the right things". For IT managers, – "do the things right" means deliver to the business quality systems, on time and on budget – " do the right thing" means to partner with the business in view to innovate."

In conclusion, I would say that expectation from CTOs and CIOs is to advocate IT Governance evolution, support it on continuing basis and utilize the structures to perform better in IT project implementation and enhance service delivery for value addition to their respective organization.

Thank you for your patience. Wish you all two very enriching days of fruitful deliberations.