IT Governance @board.level

Sanjay Sharma
MD-CEO
IDBI Intech Ltd

IDBI intech
Looking beyond the obvious!

IT Governance

Effective IT Governance is the responsibility of the Board of Directors and Executive Management.

The basic principles of value delivery, IT Risk Management, IT resource management (including IT project management) and performance management must form the basis of governance framework.

Roles and Responsibilities of Board of Directors/ IT Strategy Committee

- ❑ Approving IT strategy and policy documents.
- ❑ Ensuring that the management has put an effective strategic planning process in place
- ❑ Ratifying that the business strategy is indeed aligned with IT strategy.
- ❑ Ensuring that the IT organizational structure complements the business model and its direction.
- ❑ Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business.
- ❑ Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable.
- ❑Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources.

Roles and Responsibilities of Board of Directors/ IT Strategy Committee Contd..

- Ensuring proper balance of IT investments for sustaining bank's growth.
- Becoming aware about exposure towards IT risks and controls and evaluating effectiveness of management's monitoring of IT risks.
- Assessing Senior Management's performance in implementing IT strategies.
- Issuing high-level policy guidance (e.g. related to risk, funding, or sourcing tasks).
- Confirming whether IT or business architecture is to be designed, so as to derive the maximum business value from IT.
- Overseeing the aggregate funding of IT at a bank-level, and ascertaining if the management has resources to ensure the proper management of IT risks.
- Reviewing IT performance measurement and contribution of IT to businesses (i.e., delivering the promised value).

Information security governance consists of the leadership, organizational structures and processes that protect information and mitigation of growing information security threats.

Roles and Responsibilities of Board of Directors/Senior Management

- The Board of Directors is ultimately responsible for information security.

- Senior Management is responsible for understanding risks to the bank to ensure that they are adequately addressed from a governance perspective. To do so effectively, requires managing risks, including information security risks, by integrating information security governance in the overall enterprise governance framework of the organization.

IT SERVICES OUTSOURCING

The Board is Responsible for

- Instituting an appropriate governance mechanism for outsourced processes, comprising of risk based policies and procedures, to effectively identify, measure, monitor and control risks associated with outsourcing in an end to end manner
- Defining approval authorities for outsourcing depending on nature of risks in and materiality of outsourcing.
- Assessing management competencies to develop sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements
- Undertaking a periodic review of outsourcing strategies and all existing material outsourcing arrangements

IS Audit

Audit Committee of the Board

- A designated member of an Audit Committee needs to possess the knowledge of Information Systems, related controls and audit issues.
- Designated member should also have competencies to understand the ultimate impact of efficiencies identified in IT internal control framework by the IS Audit.

Cyber Fraud

The Board for Financial Supervision (BFS) of RBI has observed that in terms of higher governance standards, the fraud risk management and fraud investigation must be 'owned' by the bank's CEO, Audit Committee of the Board and the Special Committee of the Board.

Special Committee of the Board for monitoring large value frauds

•Banks are required to constitute a special committee for monitoring and follow up of cases of frauds involving amounts of 1 crore and above exclusively, while the Audit Committee of the Board (ACB) may continue to monitor all the cases of frauds in general.

•it is imperative that the Special Committee of the Board be briefed separately on frauds of values less than Rs.1 crore, which have the potential to reach large proportions, to keep them aware of the proportions of the fraud, modus operandi and the steps taken by the bank to mitigate them.

•The Special Committee should specifically monitor and review the progress of the mitigating steps taken by the bank in case of electronic frauds and the efficacy of the same in containing fraud numbers and values at least on a quarterly basis.

Business Continuity Planning

BCP forms a part of an organisation's overall Business Continuity Management (BCM) plan, which is the "preparedness of an organisation", which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes, at an agreed level and limit the impact of the disaster on people, processes and infrastructure (includes IT); or to minimise the operational, financial, legal, reputational and other material consequences arising from such a disaster.

- A bank's Board has the ultimate responsibility and oversight over BCP activity of a bank.
- The Board approves the Business Continuity Policy of a bank.

Legal Aspects

- Basel Committee on Banking Supervision, in its "Consultative Document on Operational Risk", defines "operational risk" as the risk of direct, or indirect, loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk.

- The Information Technology Act, 2000 (IT Act, 2000) was enacted to handle certain issues relating to Information Technology. The IT Amendment Act, 2008 has made further modifications to address more issues such as cyber crimes. It is critical that impact of cyber laws is taken into consideration by banks to obviate any risk arising there from.

- The Risk Management Committee at the Board-level needs to put in place, the processes to ensure that legal risks arising from cyber laws are identified and addressed. It also needs to ensure that the concerned functions are adequately staffed and that the human resources are trained to carry out the relevant tasks in this regard **Operational Risk Group:** This group needs to incorporate legal risks as part of operational risk framework and take steps to mitigate the risks involved in consultation with its legal functions within the bank.

THANK YOU

IDBI intech
Looking beyond the obvious!