# Chapter 1: IT GOVERNANCE

## Introduction:

Corporate Governance constitutes the accountability framework of a bank. IT Governance is an integral part of it. It involves leadership support, organizational structure and processes to ensure that a bank's IT sustains and extends business strategies and objectives. Effective IT Governance is the responsibility of the Board of Directors and Executive Management.

The role of IT Governance cannot be over emphasized. According to Richard Nolan and F. Warren McFarlane of Harvard Business School, "Lack of Board oversight for IT activities is dangerous; it puts the firm at risk in the same way that failing to audit its books would". Access to reliable information has become an indispensable component of conducting business, indeed, in a growing number of banks, information is business.

With IT increasingly being intrinsic and pervasive, attention must be paid to IT Governance, with an increased focus on how strongly a bank relies on IT and just how critical IT is for the execution of the business strategy, since:

– IT is critical in supporting and enabling bank's business goals

– IT is strategic to business growth and innovation

– Due diligence is increasingly important due to IT implications of mergers and acquisitions

– Risks of failure have wider reputational impact

In a 2009 survey, the Information Technology Governance Institute (ITGI) found a positive statistical correlation between advancement of IT Governance practices and IT outcomes. The survey indicated that better IT Governance practices led to improved IT outcomes. For example, the frequency with which IT was included on the Board's agenda, or an increased alignment between business and IT, resulted in IT-enabled investments to create value within the enterprise and or increase the degree to which IT performed against expectations.

IT has enabled banks to plan, deliver, manage and integrate products, in line with customers' needs through a range of products and services that are available to both retail and corporate customers. These include emergence of technologies such as sweep-in or sweep-out facilities, channel financing, straight through processing, multi-channel banking, mobile banking, Real Time Gross Settlement (RTGS), National Electronic Fund Transfer system (NEFT) and cheque truncation solutions, etc.

Today, almost every commercial bank branch is at some stage of technology adoption: total branch automation or core banking solution (CBS), or alternate delivery channels such as internet banking, mobile banking, phone banking and ATMs. In view of the large branch network, CBS is being implemented across banks in a phased manner. According to RBI's report on "Trend and Progress of Banking in India 2009-10", there was a significant rise in the percentage of branches of public sector banks implementing CBS from 79.4 percent in end-March 2009, to 90 percent by end-March 2010. Further, 97.8 percent of the PSB branches were computerized by end-March 2010. The growth in ATMs for all scheduled commercial banks was observed to be 37.8 percent in 2009-10. The number of ATMs for all Scheduled Commercial Banks, at the end of March 2010, stood at 60,153.

## Challenges

Though increased use of IT has enhanced a bank's business opportunities, it has resulted in newer challenges. One of them being the need to integrate independent applications developed on varied technology platforms for services and enabling IT trust among stakeholders.

Challenges faced while aligning bank's IT practices with regulatory directives across jurisdictions and industry frameworks, and meeting growing business needs, are:

a) Retaining IT human resources, training and IT service costs provided by vendors is one. Then, inflexibility of applications requiring changes, insufficient business process re-engineering, organisational structure of IT not in line with business needs, act as impediments in implementing effective IT Governance
b) Inadequate Senior Management and Board awareness on IT use and governance
c) Lack of ownership of IT Governance policies and procedures due to inadequate support or direction from stakeholders
d) Use of IT for committing frauds such as Phishing, SQL Injection, database and server hacking, network attacks, Denial of Service attack, web page defacing, Cross Site scripting, card cloning, etc. that result in financial and reputational loss
e) Risks arising from money laundering through electronic channels and its countering are a challenging task for banking system. This risk is compounded, as customers use alternate delivery channels.
f) Legal and reputational loss due to compromise of customers' and credit-card holders' accounts
g) With shorter life-cycle of technology products, banks are required to consider cost of replacing investments made in hardware and software vis-à-vis their expected benefits
h) Risks arising out of outsourcing requiring suitable mitigating actions

## A. GUIDANCE FOR BANKS

### a) *Roles and Responsibilities and Organizational Framework:*

Well-defined roles and responsibilities of Board and Senior Management are critical, while implementing IT Governance. Clearly-defined roles enable effective project control. People, when they are aware of others' expectations from them, are able to complete work on time, within budget and to the expected level of quality.

IT Governance Stakeholders include:

- Board of Directors
- IT Strategy Committees
- CEOs
- Business Executives
- CIOs
- IT Steering Committees (operating at an executive level and focusing on priority setting, resource allocation and project tracking)
- Chief Risk Officer

- Risk Committees

### *b) Organisation Structure:*

i). Expertise *at the Board Level:* IT Strategy Committees should have some form of participation at the Board level. This is to ensure that as part of the Corporate Governance initiatives, IT Governance is also addressed, so as to advice on strategic direction on IT and to review IT investments on Board's behalf.

ii). *Qualified and Independent IT Strategy Committee:* A qualified and an independent IT Strategy Committee should be set up with a minimum of two directors as members, one of whom should be an independent director. IT Strategy Committee members should be technically competent. At least one member should have substantial IT expertise in managing technology.

(Explanation1: Technically herein will mean the ability to understand and evaluate technology systems.

Explanation 2: A member will be considered to have “substantial IT expertise” if he has a minimum of seven years of experience in managing IT systems and/or leading/guiding technology initiatives/projects. Such a member should also have an understanding of banking processes at a broader level and of the impact of IT on such processes. If not, then the member should be trained on these aspects.)

iii). *Chairman of an IT Strategy Committee shall be an independent director.* Also, the CIO should be a part of this committee, who should be present at Board meetings to help IT strategy align with business goals. The IT Strategy Committee should meet at appropriate frequency as and when needed (at least four times in a year) and not more than four months should elapse between two meetings.

iv). *Powers of IT Strategy Committee:* It is recommended that the committee should have following powers:

- Perform oversight functions over the IT Steering Committee (at a senior management level)
- Investigate activities within this scope
- Seek information from any employee
- Obtain outside legal or professional advice
- Secure attendance of outsiders with relevant expertise, if it considers necessary
- Work in partnership with other Board committees and Senior Management to provide input, review and amend the aligned corporate and IT strategies

### *c) Recommended Roles and Responsibilities:*

Board of Directors/ IT Strategy Committee:

Some of the roles and responsibilities include:

- 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
- 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)

Risk Management Committee*:*

- Promoting an enterprise risk management competence throughout the bank, including facilitating development of IT-related enterprise risk management expertise
- Establishing a common risk management language that includes measures around likelihood and impact and risk categories

Executive Management Level (CEO, CIO, Business Executive):

*i) IT strategy:*

- Aligning and integrating IT strategy with business goals. Aligning IT operations with business operations
- Cascading strategy and goals to all levels of a bank
- Driving IT strategy development and execution and ensuring timely delivery of a measurable value within budget both on current and future projects
- Setting up organizational structures and responsibilities that facilitate IT strategy implementation

*ii) Value Delivery:*

- Ensure a realistic IT budget and investment plan and integrate it into an overall financial plan
- Establish business priorities and ensure that resources are allocated to enable effective IT performance
- Drive optimization of costs

*iii) IT Risk Management:*

- Adopt and monitor a risk control and governance framework and embed responsibilities for IT risk management
- Assess risks. Mitigate them efficiently and enable transparency to stakeholders
- Obtain assurance on IT performance, risks and controls and an independent comfort about major IT decisions
- Understand a bank's IT organisation, infrastructure and capabilities
- Provide inputs on business impact assessments to bank risk management process
- Implement relevant IT standards, policies and procedures
- Ensure calendar of review is submitted to the Board and Senior Management, containing a review of technology architecture (e.g. summary of transaction volumes, scalability, developments in technology)

*iv) IT Resource Management:*

- Educate executives on dependence on IT capabilities, costs and technology issues
- Provide insights and clarify and demonstrate IT value
- Proactively seek ways to increase contribution of IT value
- Establish strong IT project management
- Drive definition of business requirements and own them
- Sponsor IT projects
- Approve, control and monitor service levels
- Assess and publish operational benefits of owned IT investments
- Allocate business resources required to ensure effective IT Governance over projects and operations
- Provide IT infrastructure that facilitate creation and sharing of business information at optimal cost
- Ensure availability of suitable IT resources, skills and infrastructure to meet strategic objectives
- Ensure that critical roles for deriving maximum IT value are appropriately defined and staffed
- Standardize architectures and technology

*v) Performance Management*

- Work with CIO on designing and implementing suitable IT performance measurement methodologies such as "IT balanced scorecard" to ensure appropriate linkage to business goals
- Prioritize IT performance problems and corrective actions
- Ensure efficient day-to-day management of IT processes and controls

<u>Chief Risk Officer (CRO):</u>

- Integrate IT risks as a part of the enterprise-risk management framework

<u>Business Unit Level:</u>

<u>IT Steering Committee</u>*:*

An IT Steering Committee needs to be created with representatives from the IT, HR, legal and business sectors. Its role is to assist the Executive Management in implementing IT strategy that has been approved by the Board. It includes prioritization of IT-enabled investment, reviewing the status of projects (including, resource conflict), monitoring service levels and improvements, IT service delivery and projects. The committee should focus on implementation. Its functions *inter-alia* include:

- Defining project priorities and assessing strategic fit for IT proposals
- Performing portfolio reviews for continuing strategic relevance
- Reviewing, approving and funding initiatives, after assessing value-addition to business process
- Balancing between investment for support and growth
- Ensuring that all critical projects have a component for "project risk management"
- Sponsoring or assisting in governance, risk and control framework, and also directing and monitoring key IT Governance processes
- Defining project success measures and following up progress on IT projects
- Consult and advice on the selection of technology within standards
- Advice on infrastructure products
- Provide direction relating to technology standards and practices
- Ensure that vulnerability assessments of new technology is performed
- Verify compliance with technology standards and guidelines
- Consult and advice on the application of architecture guidelines
- Ensure compliance to regulatory and statutory requirements
- Provide direction to IT architecture design and ensure that the IT architecture reflects the need for legislative and regulatory compliance, the ethical use of information and business continuity

IT Line Management*:*

IT line managers, reporting to senior IT management, supervise resources and activities of a specific IT function, department, or subsidiary. They usually co-ordinate services between data processing areas and user departments. Some IT functions that often rely on line managers, include data centre operations, network services, application development, systems administration, telecommunications and customer support. Front-line managers co-ordinate daily activities, monitor current status, ensure adherence to established schedules and enforce corporate policies and controls.

Business Unit Management:

This unit consists of bank managers in business lines, who also have IT responsibilities:

- Establishing processes for on-going communication of business needs and strategy
- Determining MIS needs and product development plans and communicating them to the IT support or line management
- Establishing processes to test compliance with IT-related control policies within a business unit
- Ensuring that the IT development efforts are prioritized, funded and aligned with business continuity planning within units
- Ensuring that required backup IT resources are available
- Ensuring that participation in testing processes is ongoing

Specific roles of IT Line Management and Business Unit Management, with respect to technology, may vary depending upon the bank's approach to risk management and policy enforcement – either a centralized or a decentralized strategy.

- **In a centralized IT environment:** IT Line Management typically acquires, installs and maintains technology for the organisation. They have a greater ability to control and monitor the organization's technology investment. A centralized approach promotes greater operational efficiencies. Business Line Managers retain the responsibility for enforcing internal controls within their area.
- **In a decentralized IT environment:** IT Line Management only has an advisory role in some departments' acquisition, installation and technology maintenance. This approach is prevalent in banks with a complex structure, where it expedites the availability of IT services by transferring decision-making authority to strategically significant departments. Business Line Management has a much greater responsibility in ensuring that technology investments are consistent with organisation-wide strategic plans. In such situations, banks need to ensure system compatibility and the enforcement of bank-wide policies in a decentralized environment, which would require inputs from IT Line Management.

### *d) IT Organizational Structure:*

The IT organizational structure should be commensurate with the size, scale and nature of business activities carried out by the bank and the underlying support provided by information systems for the business functions. The broad areas or functions that can be considered for IT organizational structure will include technology and development, IT operations, IT assurance and supplier and resource management, each of which may be headed by suitably experienced and trained senior officials (preferably not less than the rank of AGM).

Illustrative functions of the various divisions may include:

- **Technology:** All IT architecture (systems, software, networks and telecommunications), strategic technology decisions, technology life-cycle management, thought leadership and technology research and prototype development
- **Development:** All IT development initiatives or projects, related budgets, project management, quality of outcomes, managing outsourced IT development, testing all solutions (developed in-house or outsourced)
- **IT Operations:** All IT operations (servers, operating systems, databases, applications and help desks), such as managing IT Infrastructure (facilities, data centres, networks and telecommunication), high availability and reliability of systems, managing outsourced IT operations and services
- **IT Assurance Function:** All quality, risk and compliance management initiatives within the IT vertical such as performance or conformance metrics, reports, dashboards, internal user feedback and analysis, monitoring IT projects, interaction with audit, risk and compliance functions within a bank

### **Critical Components of IT Governance Framework*:***

IT Governance has two aspects: value add to business through use of technology and mitigating IT risks. The first is driven by strategic alignment of IT with Business. The second is driven by embedding accountability in the bank. Both focus areas require support through adequate resources and measurement to ensure that results are delivered.

One of the well-known international frameworks in achieving effective control over IT and related risks is the "Control Objectives for Information Technology" (COBIT) that is issued by ITGI. The framework provides five focus areas for IT Governance. Value delivery and IT risk management are outcomes, while the remaining three are drivers: strategic alignment, IT resource management and performance measurement. IT Governance is a continuous life-cycle. It's a process in which IT strategy drives the processes, using resources necessary to execute responsibilities.

Focus Areas for IT Governance:

IT Governance entails number of activities for the Board and Senior Management, such as becoming aware of role and impact of IT on a bank: assigning responsibilities, defining constraints within which to operate, measuring performance, managing risk and obtaining assurance.

Recommendations, Actions on IT Governance practices:

Before adopting these, banks are required to evaluate their nature and scope of activities and the current level of leverage of IT and related controls.

1. **Policies and Procedures:**
   (a) The bank needs to have IT-related strategy and policies that covers areas such as:
   - Existing and proposed hardware and networking architecture for a bank and its rationale
   - Broad strategy for procurement of hardware and software solutions, vendor development and management
   - Standards for hardware or software prescribed by the proposed architecture
   - Strategy for outsourcing, in-sourcing, procuring off-the-shelf software, and in-house development
   - IT Department's Organizational Structure
   - Desired number and level of IT expertise or competencies in bank's human resources, plan to bridge the gap (if any) and requirements relating to training and development
   - Strategy for keeping abreast with technology developments and update systems as and when required
   - Strategies converted into clear IT Initiatives with a broad time frame

   (b) IT strategy and policy needs to be approved by the Board
   (c) Detailed operational procedures may be formulated in relevant areas including for data centre operations
   (d) A bank needs to follow a structured approach for the long-range planning process considering factors such as organizational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third-parties or market, planning horizon, business process re-engineering, staffing, in- or outsourcing, etc.
   (e) There needs to be an annual review of IT strategy and policies taking into account the changes to the organization's business plans and IT environment
   (f) Long-range IT strategy needs to be converted to short-range plans regularly,

for achievability

(g) The short-range plan,inter-alia, may cover the following: plan for initiatives specified in the long-range plan or initiatives that support the long-range plans, System wise transition strategy, Responsibility and plan for achievement

(h) Banks need to establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT strategy. The model should facilitate optimal creation, use and sharing of information by a business, in a way that it maintains integrity, and is flexible, functional, cost-effective, timely, secure and resilient to failure

(i) There is also a need to maintain an "enterprise data dictionary" that incorporates the organization's data syntax rules. This should enable the sharing of data among applications and systems, promote a common understanding of data among IT and business users and preventing incompatible data elements from being created

(j) Banks need to establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g. public, confidential, or top secret) of enterprise data. This scheme should include details of data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements (criticality and sensitivity). It should be used as a basis for applying controls such as access controls, archiving or encryption. Banks also need to define and implement procedures to ensure integrity and consistency of data stored in electronic form (read: databases, warehouses and archives). More details are indicated in the "Chapter: Information security".

(k) There is a need for a CIO in banks. He has to be the key business player and a part of the executive decision-making function. His key role would be to be the owner of IT functions: enabling business and technology alignment. The CIO is required to be at a level equivalent to that of the Chief General Manager (CGM) or General Manager (GM), having credible operational experience or proven leadership and awareness and knowledge of IT or having related IT experience

## 2. IT Strategic Alignment

This addresses the key question–whether a bank's technology investment is aligned to its strategic business objectives, enabling the formation of capabilities necessary to deliver business value. IT strategy provides banks the opportunity to:

- Add value to products and services
- Assist in competitive positioning
- Reduce costs and improve administrative efficiency
- Increase managerial effectiveness

When formulating an IT strategy, a bank must consider:

- Business objectives and competitive environment
- Current and future technologies: costs, risks and benefits
- Capability of the IT organisation and technology to deliver current and future levels of service and its implication on the bank (extent of change and investment)
- Operating cost of current IT: whether this provides sufficient value to the business
- Regulatory and compliance requirements

As IT gets more critical for a bank's survival in addition to enabling growth, IT Strategy Committees need to broaden their scope beyond offering advice on strategy, to other areas like IT risks, value and performance.

Challenges in IT Strategy*:*

- Identifying barriers to strategic alignment
- Evaluating effectiveness of alignment of IT and strategic business initiatives
- Ensuring business and IT goals cascade throughout the bank into roles, responsibilities and actions
- Identifying inter-dependencies of strategic initiatives and impact on value delivery and risk
- Ensuring an effective communication and engagement between business and IT management
- Monitoring and assessing current and future technology improvements

With Respect to IT Strategic Alignment, Banks Need to, inter-alia, ensure the following:

a) Banks should have an up-to-date business strategy that sets out a clear direction for IT that is in accordance with the business objectives
b) Major IT development projects need to be aligned with business strategy, having a business case
c) IT investments need to be suitably balanced between maintaining the infrastructure that support the bank's "as is" operations, and the infrastructure that transforms the operations and enables the business to grow and compete in new areas
d) IT budget reflects priorities established by the portfolio of IT-related investment programmes and includes ongoing costs of maintaining the infrastructure
e) Board's IT Strategy Committee reviews and advises the management about IT-related investments
f) IT Steering Committee (or equivalent) composed of executives from business and IT management have responsibility to: determining prioritization of IT-related investment; track status of projects; resolve resource conflict; monitor service levels and service improvements
g) IT Steering Committee should assess if the IT Governance structure fosters accountability, is effective and transparent, has well-defined objectives, actions and unambiguous responsibilities for each level in the organisation structure
h) Performance of IT management is monitored
i) Comprehensive and ongoing due diligence and oversight process is established for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking (Also see "IT Outsourcing" in report)

### 3. Value Delivery

The basic principles of IT value delivery are on time and within budget delivery of IT projects, with appropriate quality, which achieves benefits that were promised. Often, Senior Management and Boards fear to start major IT investments because of the size of investment and the uncertainty of outcome. For effective IT value delivery to be achieved, both actual costs and Return on Investment (ROI) need to be managed.

The value that IT adds to a business is a function of the degree to which the IT organisation is aligned with the business objectives and how far it meets expectations. The business should set expectations relative to IT deliverables:

- Fit for purpose and meeting business requirements
- Flexibility to adopt future requirements
- Throughput and response times
- Ease of use, resiliency and security
- Integrity, accuracy and confidentiality of information

To manage expectations of the management, IT and business should use a common language for value, which translates business and IT terminology and is factual. Therefore, technology should be aligned to provide value, so that it supports bank by delivering on time, with appropriate functionality and intended benefits. Alignment of technology to business also provides value by delivering infrastructure that enable the bank to grow by improving customer satisfaction, assuring customer retention, breaking into new markets, increasing overall revenue and driving competitive strategies.

a) <u>Capacity to deliver is dependent on</u>:
   - Timely, usable and reliable information about customers, processes and markets, etc.
   - Productive and effective practices (performance measurement and knowledge management, etc.)
   - Ability to integrate technology
   - Realizing that different strategic contexts require different indicators of value

b) <u>The Board of Directors and bank's Senior Management should consider following aspects before adopting recommendations given in this section:</u>
   - Whether current reports provided to Board and Senior Management illustrate the value that IT delivers to business: from the perspective of customer service, cost, speed of delivery, quality, ROI and value-add to business, etc
   - Current system of reporting and tracking major IT projects
   - Current rate of failure of IT projects
   - Costs involved in managing incidents (network outages and system downtime)
   - Level of end-user and customer satisfaction with the quality of IT services

c) <u>With respect to "value delivery", banks needs to *inter-alia* ensure that</u>:

i) IT-enabled investment programmes and other IT assets and services are managed to ascertain that they deliver the greatest possible value in supporting the bank's strategy and objectives:
   - Infrastructure to facilitate creation and sharing of business information
   - Flexibility and ensuring programmes are amenable to maintenance and integration
   - They are functional, timely, secure and resilient to failure

- Logically extends, maintains and manages disparate legacy systems and new applications
- Ensures standard, reusable and modular applications and components

ii) Effective IT controls are in place to minimize IT related vulnerabilities, increase efficiency, use resources optimally and increase the effectiveness of IT processes

iii) IT function supports robust and comprehensive Management Information System in respect of various business functions as per the needs of the business that facilitate decision making by management

iv) Project management and quality assurance steps should be implemented to ensure systems are delivered on time, to cost and with the necessary level of functionality

v) IT internal control failures and weaknesses and their actual and potential impact need to be evaluated and management takes suitable actions in respect of such control failures or weaknesses

vi) Project-level steering committees needs to be created for taking responsibility for execution of the project plan, achievement of outcomes and project completion. The various responsibilities include reviewing progress against the project plan, reviewing and approving changes to project resource allocation, time lines, objectives, costs, keeping the project scope under control and approving changes to the business case, acting on escalated project issues and resolving conflicts between stakeholder groups and assisting in evaluation of project risks, and project risk management approaches

vii) Independent assurance on the achievement of IT objectives and the containment of IT risks is conducted regularly

viii)IT Steering Committee or any of its sub committees involving the CIO and senior business managers prioritize IT initiatives and assign ownership for IT-enabled business opportunities

ix) Periodical review of all non-performing or irrelevant IT projects in the bank, if any, and taking suitable actions

## 4. IT Risk Management

a) Effective risk management begins with a clear understanding of the bank's risk appetite and identifying high-level risk exposures.

b) Having defined risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Dependent on the type of risk, project and its significance to the business, Board and Senior Management may choose to take up any of the **three** actions:

- **Mitigate**—Implement controls (e.g. acquire and deploy security technology to protect the IT infrastructure)
- **Transfe**r—Share risk with partners or transfer to insurance coverage
- **Accept—**Formally acknowledge that the risk exists and monitor it

c) At a basic level, risk should at least be analysed, even if there is no immediate action to be taken, the awareness of risk will influence strategic decisions. An IT control framework defines stakeholders and relevant controls for effective Enterprise Risk Management. The "risk register", usually in form of a table, is a tool that assists in risk management. It is also called a "risk log". It usually is used when planning for the future that includes project, organizational, or financial plans. Risk management uses risk registers to identify, analyse and manage risks in a clear and concise manner. Risk register contains information on each identified risk and planned responses are recorded in the event the risk materializes, as well as a summary of what actions should be taken before hand to reduce the impact. Risks are ranked in order of likelihood, or of their impact and record the analysis and evaluation of risks that have been identified. The register or the log may be created for a new project or investment.

d) Banks should consider following aspects before adopting recommendations given in this section:
- Consider the current position of a bank relative to risks: risk avoiding or risk taking? In short, risk appetite and tolerance levels
- Maintain a list of IT risks included in the register and ratings
- Implement and document risk framework to assess, mitigate approach and analyse cost against benefits
- Document measures adopted to contain IT risks
- Consider reporting systems used to provide information relating to IT risks: including operational and compliance aspects
- Whether there are actual or potential conflicts between operational functions and IT functions

e) In respect to IT risk management, banks should *inter-alia* consider the following:

i. IT management needs to assess IT risks and suitably mitigate them

ii. Bank-wide risk management policy, in which operational risk policy includes IT-related risks, is in place. The Risk Management Committee periodically reviews and updates the same (at least annually)

iii. Bank's risk management processes for its e-banking activities are integrated into its overall risk management approach. A process should be in place to have effective management oversight over the risks associated with e-banking activities, including specific accountability, policies and controls to manage these

iv. All risks related to suppliers are considered. Risk mitigation measures such as proactive relationship management, escrow and second sourcing

v. Appropriate incident response plans which include communication strategies ensuring business continuity, control reputation risk and limit liability associated with disruptions in their IT-enabled services, including those originating from outsourced systems and operations. (Details indicated in chapters relating to "Information Security" and "IT Operations".)

vi. Operational risk inherent in all material products, activities, processes and systems, are assessed and relevant controls are implemented and monitored

vii. Appropriate measures are implemented to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services, including foreign jurisdictions where the bank operates

viii. Appropriate procedures are implemented to comply with legislative, regulatory and contractual requirements on the use of systems and software where IPR, copyrights and on the use of proprietary software products are applicable

ix. Information security policy is in place and requirements indicated in the chapter on information security are considered

x. Comprehensive and centralized change control system is implemented at levels (project or application), so that changes are appropriately reviewed and approved

xi. Appropriate programme and project management framework is implemented for the management of all IT projects that ensures the correct prioritisation and co-ordination

xii. For managing project risks, a consistent and formally-defined programme and project management approach needs to be applied to IT projects that enable stakeholder participation and monitoring of project risks and progress. Additionally, for major projects, formal project risk assessment needs to be carried out and managed on an ongoing basis

xiii. Components of well-known IT control frameworks such as COBIT and ITIL as applicable to each bank's technology environment may be implemented providing a standardised set of terms and definitions that are commonly interpreted by stakeholders, allowing them to bridge the gap with respect to control requirements, technical issues and business risks, and communicate a level of control

xiv. Inter-dependencies between risk elements are considered in the risk assessment process, as threats and vulnerabilities have the potential to compromise interconnected and interdependent systems and processes

xv. An appropriate Business Continuity Management Framework is implemented and tested as per requirements in the chapter on BCM framework.

xvi. A process is implemented to evaluate vendors, who provide outsourced services, including comprehensive due diligence procedures, monitoring vendor performance and managing service-level agreements. (Details provided in “IT Outsourcing” chapter.)

## 5. IT Resource Management

A key to successful IT performance is optimal investment, use and allocation of IT resources: people, applications, technology, facilities and data, in servicing the bank's needs. Additionally, the biggest challenge in recent years has been to know where and how to outsource, and then to know how to manage the outsourced services in a way that delivers the values promised at an acceptable price.

IT assets are complex to manage and continually change due to the nature of technology and changing business requirements. Effective management of hardware life-cycles, software licences, service contracts and permanent and contracted human resources is a critical success factor. It is critical not only for optimising the IT cost base, but also for managing changes, minimising service incidents and assuring a reliable service quality.

Out of the IT assets, human resources represent the biggest part of the cost base. It is most likely to increase on a unit basis. It is essential to identify skill sets requirements through delineation of job roles and responsibilities and an assessment of required core competencies in the workforce. An effective recruitment, retention and training programme is necessary, to ensure that a bank has the skills to utilise IT effectively, so as to achieve the stated objectives.

Ability to balance the cost of infrastructure assets with the quality of service (including those provided by outsourced external service providers) is critical to successful value delivery.

### Project Management

a) Programme and project management framework (for IT and non-IT related projects which are critical to a bank), is an important component of resource management. Its framework ensures a project's correct prioritisation and co-ordination. It includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, a formal test plan, testing and post-implementation review (after installation) to ensure project risk management and value delivery to the business.

b) Project Management is achieved by:
- Defining and enforcing programme and project framework and approach
- Issuing project management guidelines

- Performing planning for each project in the portfolio

c) Project Management can be measured by:

- Percentage of projects meeting stakeholders' expectations (on time, on budget and meeting requirement weighted by importance)
- Percentage of projects receiving post-implementation reviews
- Percentage of projects following project management standards and practices

For resource management, banks need to have operational plans and budgets that specifically identify IT components and implement processes for capacity planning. Banks need to consider the following aspects before adopting the recommendations.

- Current practices followed for managing IT assets
- Trend of asset utilisation that reflects efficiency: are assets under-utilised or over-utilised?
- Current short-term and long-term IT strategy: in view of the expected business growth
- Nature and extent of activities outsourced and the outsourcing strategy
- Skills and competencies available in the current IT employees' pool and expected skills requirement

For IT resource management, banks should, *inter-alia,* consider the following:

i) That the Board is appropriately aware of IT resources and infrastructure to meet strategic business objectives: banks are aware that a process is in place to record resources available and potentially available

ii) Policies and procedures for information systems monitoring facilitate, consistent and effective reporting and review of logging, monitoring and reporting of system events

iii) Responsibilities and authorities of individuals, accountable for creating and managing records, are identified throughout for records management

iv) Requirement for trained resources, with the requisite skill sets for the IT function, is understood and assessed. A periodic assessment of the training requirements for human resources is made to ensure that sufficient, competent and capable human resources are available

v) Information on IT investments is available to the Board and Senior Management

vi) Procedures to assess the integration and interoperability of complex IT processes (such as problem, change and configuration management) exists before committing additional investments

vii) Responsibilities, relationships, authorities and performance criteria of project team members and stakeholders are stated

viii) Bank's procurement practices is used to plan and manage the procurement of products and services required for project

## 6. Performance Measurement

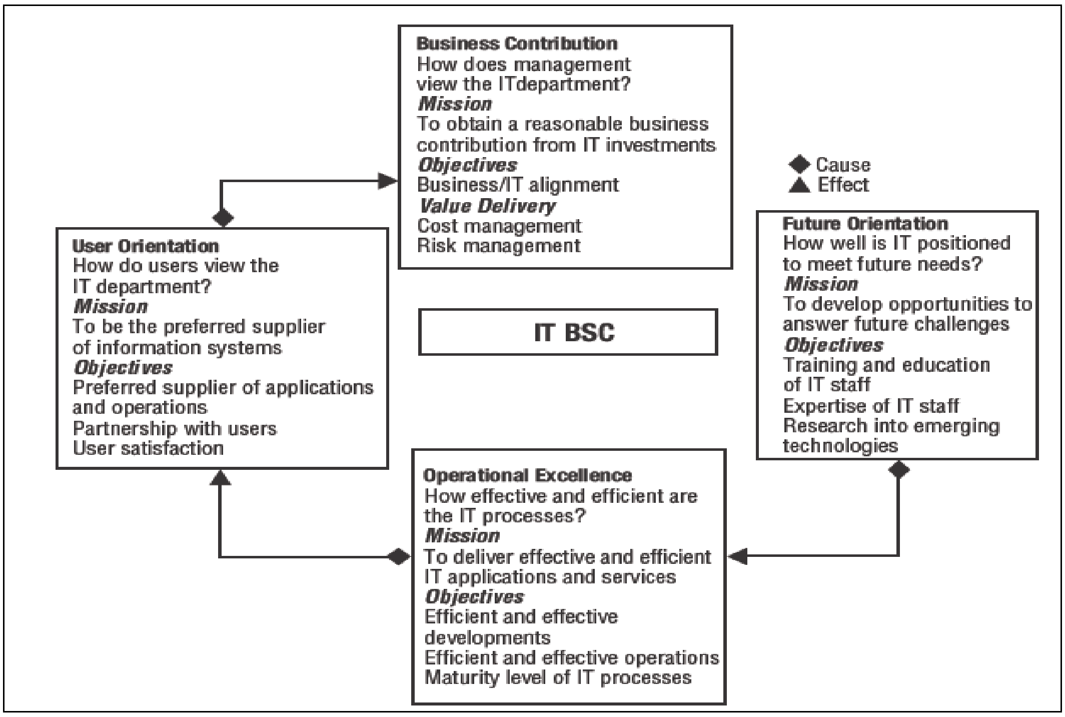
a) IT performance management aims at:

- Identifying and quantifying IT costs and benefits
- Overcoming limitations of traditional quantifiable performance measures (financial terms) such as ROI, Net Present Value (NPV), Internal Rate of Return (IRR) and payback method

- Overcoming limitations of measuring “unquantifiable” values

b) Balanced scorecards translate strategy into action, to achieve goals within a performance measurement system that goes beyond conventional accounting, measuring relationships and knowledge-based assets necessary to compete in the information age such as: customer focus, process efficiency and an ability to learn and grow. The scorecard consists of financial, customer, internal and learning perspectives. An example of a balanced scorecard is one that uses metrics such as customer satisfaction feedback, IT performance parameters (server and network downtime) or capacity utilisation. By using the scorecard, beyond the short-term financial measures as indicators of the company’s performance management, it also takes into account intangible items such as level of customer satisfaction, streamlining of internal functions and the creation of operational efficiencies and development of staff skills. This unique and more holistic view of business operations contributes to linking long-term strategic objectives with short-term actions.

c) Use of an **IT balanced scorecard (IT BSC)** is one of the means that can be considered by banks to aid the Board and Senior Management to achieve alignment of IT and business strategies. The objectives are to establish a vehicle for management reporting to the Board, to foster consensus among key stakeholders about IT’s strategic aims, to demonstrate the effectiveness and add value by use of technology, and to communicate IT’s performance, risks and capabilities. The schema of IT Balanced Scorecard is shown below.


Business Contribution
How does management view the ITdepartment?
Mission
To obtain a reasonable business contribution from IT investments
Objectives
Business/IT alignment
Value Delivery
Cost management
Risk management
◆ Cause
▲ Effect
User Orientation
How do users view the IT department?
Mission
To be the preferred supplier of information systems
Objectives
Preferred supplier of applications and operations
Partnership with users
User satisfaction
IT BSC
Future Orientation
How well is IT positioned to meet future needs?
Mission
To develop opportunities to answer future challenges
Objectives
Training and education of IT staff
Expertise of IT staff
Research into emerging technologies
Operational Excellence
How effective and efficient are the IT processes?
Mission
To deliver effective and efficient IT applications and services
Objectives
Efficient and effective developments
Efficient and effective operations
Maturity level of IT processes

d) IT **Governance maturity model** is another tool to ascertain the level of maturity of a bank's IT Governance. Levels include:

✓ 0–**Nonexistent:** This is when IT-related risks are not managed properly. An oversight exists, as far as IT-related activities of a bank are considered, among the Senior

Management. Also, IT goals that add value to the business is absent.

- ✓ 1–**Initial or Ad Hoc:** No formal IT Governance is present. The oversight is again based mostly on the Senior Management's lack of consideration of IT-related issues on a case-to-case basis. IT Governance is dependent on initiatives and experiences of IT management team, with limited input from the rest of the bank's functions.
- ✓ 2–**Repeatable but Intuitive:** A realization of requirement of a more formalized oversight of IT, that needs to be a shared management responsibility requiring the support of Senior Management, is favoured. Regular governance practices take place, but rely mostly on the initiative of the IT management team, with voluntary or co-opted participation by key stakeholders, depending on current IT projects and priorities.
- ✓ 3–**Defined Process:** This is when organizational and process framework is defined for oversight. IT management is introduced in the bank as a basis for IT Governance. The Board issues guidance, developed into management procedures covering key governance activities (regular target-setting, performance review and capability assessments against planned needs, project planning and funding) and for IT improvements. Previous informal, but successful practices, are institutionalized. Techniques followed are simple.
- ✓ 4–**Managed and Measurable:** Sophisticated target-setting is developed with relationships between business terms outcomes and IT process improvement measures. It is considered measured when a balanced scorecard is used to communicate real results to management. The bank management works together for a common goal which is maximizing IT value delivery and managing IT-related risks. Relationships among the IT function, users in the business community and external service providers, are based on service definitions and service agreements.
- ✓ 5–**Optimized:** This is when IT Governance practices are developed into a sophisticated approach, using effective techniques. There is a transparency in IT activities. The Board is in control of the IT strategy. Balanced scorecard approach evolves into one that is focused on the important measures relevant to the bank’s overall business strategy. The effort spent on risk management is streamlined through adoption of standardized and, wherever possible, automated processes. Overall, the IT cost is monitored effectively. The Bank is able to achieve optimal IT spending through internal improvements.

e) A bank may consider the following aspects before adopting recommendations:

- Assess current performance measurement metrics used to ensure that it meets expectations
- Assess current management information systems to report on performance of IT function
- processes to evaluate performance of contractors and outsourced service providers. Then take remedial action in cases of deviation from expected levels
- Assess practices for managing service-level expectations of business functions: are there formal service-level agreements for IT functions?
- Assess ROI trends generated by IT function: is the ROI as projected while committing investments?
- Assess practices followed by industry competitors and the bank's performance status in comparison

f) In respect to the IT performance management, the considerations for a bank are the following:

- That information on IT projects that have an impact on the bank’s risk profile and strategy are reported to appropriate levels of management and undergo appropriate strategic and cost and reward analysis on a periodic basis

- Processes for making return versus risk balance may be considered and supported with standard templates or tools
- Tools such as IT balanced scorecard is considered for implementation, with approval from key stakeholders, to measure performance along dimensions: financial, customer satisfaction, process effectiveness, future capability and assess IT management performance based on metrics such as scheduled uptime, service levels, transaction throughput and response times and application availability
- The bank may also consider assessing the maturity level, set a target as per the IT Governance maturity model, design an action plan and subsequently implement it to reach the target maturity level
- Periodic assessment of IT budget deviations
- Periodic review and update of IS Policies and guidelines

## B. INDUSTRY LEVEL RECOMMENDATIONS

(a) **A forum in India**– akin to the “Financial Services Technology Consortium” (FSTC) in the US, under the aegis of IDRBT, can work collaboratively to solve shared problems and challenges, as well as pioneer new technologies that benefits banks. Through the FSTC, more than 100 of the top North American financial services and technology firms, academic institutions and government agencies come together to discuss and research technology issues. FSTC Standing Committees sponsor collaborative research projects, technology development pilots, proof-of-concept tests and more. Some of the benefits may include updation regarding current developments and trends, promoting standards, networking on shared technical challenges, discussing the legal and regulatory dimension of complex technical issues facing the banking industry, conducting studies affecting industry as a whole and voicing and resolving any problems or issues faced by banks, while dealing with vendors, in a collective manner.

(b) **An exclusive forum for CIO and senior bank IT officials**, under the aegis of IDRBT or IBA, can be encouraged to enable sharing of experiences, best practices and discussion of issues of contemporary relevance for the benefit of the industry as a whole. The regulator can also be part of the meeting as observer.

## KEY RECOMMENDATIONS

1. Banks needs to formulate Board-approved IT plan document, which is long-term in nature and provides the IT road map. Additionally, IT policy needs to be framed for regular management of IT function. Detailed documentation in terms of procedures, guidelines and authorizations need to exist and be implemented. There needs to be an annual review of IT strategy or plans and policies taking into account changes to the organization’s business plans and IT environment.
2. There is a need for creation of exclusive Board-level IT Strategy Committee, which shall have a minimum of two directors as members. Out of these two members, one should be an independent director. Members of IT Strategy Committee shall be technically competent. At least one member shall have substantial IT expertise in managing technology.
3. Risk Management Committee of a Board needs to promote development of IT-related enterprise risk management expertise and help managers align risk responses with an entity’s risk tolerances and develop appropriate controls.
4. There is a need for the position of a CIO in banks. The CIOs need to be key business players. They need to be a part of the executive decision-making process. Their key

role would be as a owner of the IT function and enable business and technology alignment. The CIO is required to be at a level equivalent to Chief General Manager (CGM) or the General Manager (GM), having credible operational experience and proven leadership with awareness or knowledge and/or experience relating to IT.

5. IT Steering Committee needs to be created with representations from IT, HR, legal and business sectors (as appropriate). The committee's role will be to assist the executive management implement IT strategy that has been approved by the Board. Tasks will include prioritization of IT-enabled investment, reviewing status of projects (resolving resource conflict), monitoring service levels and improvements.
6. Organizational structure for IT should be commensurate with size, scale and nature of business, and underlying support provided by information systems for business functions.
7. Key focus areas of IT Governance includes strategic alignment, value delivery, risk management, resource management and performance management.
8. Requirements for trained resources with requisite skill sets for IT function need to be understood and assessed. A periodic assessment of human resources is made to ensure that sufficient, competent and capable human resources are available.
9. Bank’s risk management processes for its e-banking activities need to be integrated into the bank's overall risk management approach. A process should be in place to have an effective management oversight of the risks associated with e-banking, including specific accountability, policies and controls.
10. Banks need to establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT strategy. The model should facilitate optimal creation, use and sharing of information by a business, in a way that it maintains integrity, and is flexible, functional, timely, secure and resilient to failure
11. There is also a need to maintain an “enterprise data dictionary” that incorporates the organization’s data syntax rules. This should enable the sharing of data among applications and systems, promote a common understanding of data among IT and business users and preventing incompatible data elements from being created
12. Board needs to be adequately aware of IT resources and infrastructure available to meet required strategic business objectives and that a process is in place to record the resources available and potentially available.
13. IT Steering Committee should assess if the IT Governance structure fosters accountability, is effective and transparent, has well-defined objectives, actions and unambiguous responsibilities for each level.
14. Performance of IT management needs to be monitored, to ensure delivery on time and within budget, with appropriate functionality and intended benefits.
15. Information on IT investments needs to be made available (periodically) to the Board and Senior Management for evaluation
16. Procedures to assess the integration and interoperability of complex IT processes such as problem, change and configuration management need to exist, depending upon the extent of technology leverage in a bank.
17. Appropriate programme and project management framework needs to be implemented for the management of IT projects, which ensures the correct prioritization and co-ordination.
18. For managing project risks, a consistent and formally-defined programme and project management approach should be applied to IT projects that enable stakeholder participation and monitoring of project risks and progress. Additionally, for major projects, formal project risk assessment needs to be carried out and managed on an ongoing basis.
19. IT functions need to support comprehensive Management Information System in respect to business functions as per business needs that provide inputs for effective decision-making on the part of the management.
20. Bank-wide risk management policy, in which operational risk policy includes the IT-

related risks, needs to be in place. The Risk Management Committee periodically has to review and update the same (annually).

21. Components of well-known IT control frameworks like COBIT, as applicable to the technology environment of each bank, may be considered for implementation in phased manner, for providing a standardized set of terms and definitions, interpreted by stakeholders.
22. Effective IT control practices avoid breakdowns in internal control and oversight. They increase efficiency by using resources optimally thereby increasing the effectiveness of IT processes.
23. Information on major IT projects, which have a significant impact on the bank's risk profile and strategy, are reported to appropriate levels of management. It has to be made sure that such information undergoes appropriate strategic and cost-and-reward analysis on a periodic basis.
24. Project-level steering committees need to be created to take responsibility for the execution of project plan, outcome achievement and project completion.
25. IT balanced scorecard may be considered for implementation, with approval from key stakeholders, to measure IT performance along financial dimension and others such as customer satisfaction, process effectiveness and future capability. And there is the need to assess IT management performance based on metrics such as scheduled uptime, service levels, transaction throughput, response times and application availability.
26. Banks may consider assessing its IT maturity level by setting a target as per the IT Governance Maturity Model, designing the action plan and implementing it to reach the target level.
27. There is a need for a forum in India (either independent or under the aegis of IDRBT), similar to the US-based Financial Services Technology Consortium, to work collaboratively to solve shared challenges, as well as pioneer new technologies that benefits all banks.
28. An exclusive forum for CIO and senior IT officials, under the aegis of IDRBT or IBA, can be encouraged to enable sharing of experiences and issues of contemporary relevance for the benefit of the industry. The regulator can also be part of the meeting as observer.