Executive Summary

Background:

Technology has become a part of all walks of life and across all business sectors, and even more so in banking. There has been massive use of technology across many areas of banking business in India, both from the asset and the liability side of a bank's balance sheet. Delivery channels have immensely increased the choices offered to the customer to conduct transactions with ease and convenience. Various wholesale and retail payment and settlement systems have enabled faster means of moving the money to settle funds among banks and customers, facilitating improved turnover of commercial and financial transactions. Banks have been taking up new projects like data warehousing, customer relationship management and financial inclusion initiatives to further innovate and strategise for the future and to widen the reach of banking.

The dependence on technology is such that the banking business cannot be thought of in isolation without technology, such has been the spread of technology footprints across the Indian commercial banking landscape. Developments in IT have also brought along a whole set of challenges to deal with. The dependence on technology has led to various challenges and issues like frequent changes or obsolescence, multiplicity and complexity of systems, different types of controls for different types of technologies/systems, proper alignment with business objectives and legal/regulatory requirements, dependence on vendors due to outsourcing of IT services, vendor related concentration risk, segregation of duties, external threats leading to cyber frauds/crime, higher impact due to intentional or unintentional acts of internal employees, new social engineering techniques employed to acquire confidential credentials, need for governance processes to adequately manage technology and information security, need for appreciation of cyber laws and their impact and to ensure continuity of business processes in the event of major exigencies.

Technology risks not only have a direct impact on a bank as operational risks but can also exacerbate other risks like credit risks and market risks. Given the increasing reliance of customers on electronic delivery channels to conduct transactions, any security related issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks. Inadequate technology implementation can also induce strategic risk in terms of strategic decision making based on inaccurate data/information. Compliance risk is also an outcome in the event of non-adherence to any regulatory or legal requirements arising out of the use of IT. These issues ultimately have the potential to impact the safety and soundness of a bank and in extreme cases may lead to systemic crisis.

Keeping in view the changing threat milieu and the latest international standards, it was felt that there was a need to enhance RBI guidelines relating to the governance of IT, information security measures to tackle cyber fraud apart from enhancing independent assurance about the effectiveness of IT controls. To consider these and related issues, RBI announced the creation of a Working Group on Information Security, Electronic Banking, Technology Risk Management and Tackling Cyber Fraud in April, 2010. The Group was set up under the Chairmanship of the Executive Director Shri.G.Gopalakrishna.

The Group delved into various issues arising out of the use of Information Technology in banks and made its recommendations in nine broad areas. These areas are IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programmes and Legal issues.

Major Recommendations of the Working Group

The Group felt that the recommendations are not “one-size-fits-all” and the implementation of these recommendations need to be based on the nature and scope of activities engaged by banks and the technology environment prevalent in the bank and the support rendered by technology to the business processes.

On IT Governance:

- Banks need to formulate a Board approved IT strategy/plan document. An IT policy needs to be framed for regular management of IT functions and ensure that detailed documentation in terms of procedures and guidelines exists and are implemented. The strategic plan and policy need to be reviewed annually.
- A need was felt to create an exclusive Board level IT Strategy Committee with a minimum of two directors as members, one of whom should be an independent director. All members of the IT Strategy Committee would need to be technically competent while at least one member would need to have substantial expertise in managing/guiding technology initiatives.

- A need was felt for the position of CIO in banks, to be the key business player and play a part in the executive decision-making function. The key role of the CIO would be to act as an owner of the IT function and enable the alignment of business and technology.
- IT Steering Committee needs to be created with representations from various IT functions, HR, Legal and business functions as appropriate. The role of the IT Steering Committee would be to assist the Executive Management in the implementation of the IT strategy approved by the Board.
- The IT Steering Committee should assess whether the IT Governance structure fosters accountability, is effective and transparent, has well defined objectives and actions and unambiguous responsibilities for each level in the organization.
- The organizational structure for IT 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 business functions.
- Key focus areas of IT Governance that need to be considered include strategic alignment, value delivery, risk management, resource management and performance management.
- Requirements for trained resources with requisite skill sets for the IT function need to be understood and assessed appropriately. A periodic assessment of the training requirements for human resources should be made to ensure that sufficient, competent and capable human resources are available.
- The Board needs to be adequately aware of IT resources and infrastructure available to meet required strategic business objectives and ensure that a process is in place to record the resources available/ potentially available to the bank.
- Performance of IT function should be monitored to ensure delivery on time and within budget, with appropriate functionality and with intended benefits.
- 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
- 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

- 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.
- An appropriate programme and project management framework needs to be implemented for the management of all IT projects, which ensures correct prioritization and co-ordination
- For managing project risks, a consistent and formally defined programme and project management approach should be applied to IT projects that enable appropriate stakeholder participation and monitoring of project risks and progress
- For major projects, formal project risk assessment needs to be carried out and managed on an ongoing basis
- The bank-wide risk management policy or operational risk policy needs to include IT related risks and the Risk Management Committee should periodically review and update the same (at least annually).
- IT function needs to support a robust and comprehensive Management Information System with respect to various business functions as per business needs and in coordination with business personnel so as to provide inputs for effective decision making by management
- Components of well-known IT control frameworks such as COBIT as applicable to each bank's technology environment may be considered for implementation in a phased manner providing a standardized set of terms and definitions that are commonly interpreted by all stakeholders.
- Effective IT control practices and their monitoring are required to avoid breakdowns in internal control and oversight, increase efficiency, use resources optimally and increase the effectiveness of IT processes.
- Information on major IT projects that have a significant impact on the bank's risk profile and strategy needs to be reported to appropriate levels of management and undergo appropriate strategic and cost/ reward analysis on a periodic basis.
- Project level steering committees needs to be created to take responsibility for execution of the project plan, achievement of outcomes and project completion.
- An IT balanced scorecard may be considered for implementation, with approval from key stakeholders, to measure IT performance along different dimensions such as financial aspects, customer satisfaction, process effectiveness, future capability, and for assessing IT management performance.

- Banks may also consider assessing their IT maturity level, based on well known international standards, design an action plan and implement the plan to reach the target maturity level.
- A forum in India, under the aegis of IDRBT, akin to the Financial Services Technology Consortium in the US, can work collaboratively to solve shared problems and challenges, as well as pioneer new technologies that benefits all banks.
- An exclusive forum for CIO and senior IT officials of banks, under the aegis of IDRBT, can be encouraged to enable sharing of experiences and discuss issues of contemporary relevance for the benefit of the industry as a whole.

On Information Security:

- The major role of the Board/ Top Management should involve approving information security policies, establishing necessary organizational processes/ functions for information security and providing necessary resources.
- Each bank needs to create a separate information security function to focus exclusively on information security management. The organization of the information security function should be commensurate with the nature and size of activities of a bank and extent of IT leverage and e-delivery channels. The function should be adequately resourced in terms of the number of staff, their range and level of skills, and tools or techniques.
- A sufficiently senior level official of the rank of GM/DGM/AGM needs to be designated as the Chief Information Security Officer (CISO) responsible for articulating and enforcing the policies that a bank uses to protect its information assets apart from coordinating the information security related issues / implementation within the organization as well as relevant external agencies. The CISO needs to report directly to the Head of the Risk Management function and should not have a direct reporting relationship with the CIO.
- A Board approved Information security policy needs to be in place and reviewed at least annually. The policy framework should take into consideration, inter-alia, aspects like :alignment with business objectives; the objectives, scope, ownership and responsibility for the policy; information security organizational structure; information security roles and responsibilities; exceptions; knowledge and skill sets required; periodic training and continuous professional education; compliance review and penal measures for non-compliance of policies.
- Risk assessment is the core competence of information security management for a bank. The risk assessment must, for each asset within its scope, identify the threat/

vulnerability combinations that have a likelihood of impacting the confidentiality, availability or integrity of that asset - from a business, compliance and/or contractual perspective.

- Job descriptions, including roles and responsibilities, employment agreements and policy awareness acknowledgements from staff increase accountability for security. Management can communicate general and specific security roles and responsibilities for all employees based on their job descriptions. Management should expect all employees, officers, and contractors to comply with information security and/or acceptable-use policies and protect the institution's assets, including information.
- Digital evidence needs to be considered as similar to any other form of legal proof. It needs to withstand challenges to its integrity, its handling must be carefully tracked and documented, and it must be suitably authenticated by the concerned personnel. A policy needs to be in place in this regard.
- Maintaining detailed inventory of information assets and classification of information/data are among the key components of information security management.
- Banks need to grant authorisation for access to information assets only where a valid business need exists and only for a definite time period for which the access is required.
- Personnel with elevated system access privileges should be closely supervised.
- Information security needs to be considered at all stages of an information asset's (like hardware, software) life-cycle which typically includes: planning and design; acquisition and implementation; maintenance and support; and disposal so as to minimise exposure to vulnerabilities.
- Banks should have a process in place to verify job application information on all new employees. The sensitivity of a particular job or access level may warrant additional background and credit checks.
- Banks should implement suitable physical and environment controls taking into consideration threats, and based on the entity's unique geographical location, building configuration, neighboring entities, etc.
- There is a vital need for initial, and ongoing, training/awareness programmes on information security for employees and vendor personnel. There should also be a mechanism to track the effectiveness of the training programmes periodically through an assessment process designed for testing the understanding of relevant policies.
- A robust incident management process needs to be in place to maintain the capability to manage incidents within an enterprise, to enable containment of exposures and to achieve recovery within a specified time period. Incidents could include aspects relating

to misuse of computing assets, information disclosure or events that threaten the continuance of business processes.

- A bank needs to have clear accountability mechanisms and communication plans (for escalation and reporting to the Board and senior management and customer communication where appropriate) to limit the impact of information security incidents. Institutions would also need to pro-actively notify CERT-In/IDRBT/RBI regarding major cyber security incidents.
- There should be documented standards/procedures for administering an application system, which are approved by the application owner and kept up-to-date. Access to the application should be based on the principle of least privilege and "need to know" commensurate with the job responsibilities. Adequate segregation of duties needs to be enforced.
- Every application affecting critical/sensitive information, for eg. impacting financial, customer, control, risk management, regulatory and statutory aspects, must provide for detailed audit trails/ logging capability with details like transaction id, date, time, originator id , authorizer id, actions undertaken by a given user id, etc. Other details like logging IP address of client machine, terminal identity or location also need to be available. Alerts regarding use of the same machine for both maker and checker transactions need to be considered. The logs/alerts/exception reports with regard to systems should be analyzed and any issues need to be remedied at the earliest.
- The audit trails should satisfy a bank's business requirements apart from regulatory and legal requirements. It should also be facilitating the conduct of audit, serving as forensic evidence when required and assisting in dispute resolution including for non-repudiation purposes. Audit trails should be secured to ensure the integrity of the information captured and preservation of evidence.
- Banks may obtain application integrity statements in writing from the application system vendors providing for reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs, and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done).
- Data security measures need to be in place. Banks need to define and implement procedures to ensure the integrity and consistency of all critical data stored in electronic form, such as databases, data warehouses and data archives.
- Direct back-end updates to database should not be allowed except during exigencies, in the event of a genuine business need and after due authorization as per relevant policy

- Any changes to an application system/data need to be justified by genuine business need and approvals supported by documentation and subjected to a robust change management process.
- For all critical applications, either source code must be received from the vendor or a software escrow agreement needs to be in place with a third party to ensure source code availability in case the vendor goes out of business. It needs to be ensured that product updates and programme fixes are also included in the escrow agreement.
- Data transfer from one process to another or from one application to another, particularly in respect of critical or financial applications, should not have any manual intervention in order to prevent any unauthorized modification. The process needs to be automated and properly integrated through "Straight Through Processing" methodology with an appropriate authentication mechanism and audit trails.
- In the event of data pertaining to Indian operations being stored and/or processed abroad, for example, by foreign banks, there needs to be suitable controls like segregation of data and strict access controls based on 'need to know' and robust change controls. The bank should be in a position to adequately prove the same to the regulator. Regulator's access to such data/records and other relevant information should not be impeded in any manner and RBI would have the right to cause an inspection to be made of the processing centre/data centre and its books and accounts by one or more of its officers or employees or other persons.
- Robust system security testing needs to be carried out.
- Multi-tier application architecture needs to be implemented for critical e-banking systems like internet banking which differentiate session control, presentation logic, server side input validation, business logic and database access.
- A bank needs to have a documented migration policy specifying a systematic process for data migration and for ensuring data integrity, completeness and consistency. Explicit sign offs from users/application owners need to be obtained after each stage of migration and also after the migration process has been completed. Audit trails need to be available to document the conversion, including data mappings and transformations.
- Banks need to carry out due diligence with regard to new technologies/systems since they can potentially introduce additional risk exposures
- Any new business products introduced, along with the underlying information systems, need to be assessed as part of a formal product approval process which incorporates, inter-alia, security related aspects and fulfilment of relevant legal and regulatory prescriptions.

- Cryptographic techniques need to be used to control access to critical and sensitive data/information in transit and storage. Banks should only select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, reputable security vendors or government agencies.
- Normally, a minimum of 128-bit SSL encryption is expected. Constant advances in computer hardware, cryptanalysis and distributed brute force techniques may induce use of larger key lengths periodically. It is expected that banks will properly evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution that is commensurate with the degree of confidentiality and integrity required.
- Banks need to scan frequently for vulnerabilities and address discovered flaws proactively to avoid the likelihood of having their computer systems compromised. Automated vulnerability scanning tools need to be used against all systems in their networks on a periodic basis.
- Banks need to have monitoring processes in place to identify suspicious events and unusual behavioural patterns that could impact the security of IT assets. The strength of the monitoring controls should be based on the criticality of an IT asset. A bank would need to establish a clear allocation of responsibility for regular monitoring mechanism, and the tools and processes in this regard need to be commensurate with the level of monitoring required.
- Critical functions , for example relating to financial, regulatory and legal, MIS and risk management, need to be done through proper application systems and not manually or in a semi-automated manner through spreadsheets which pose risks relating to data integrity and reliability. Use of spreadsheets in this regard should be restricted and should be replaced by appropriate IT applications in a phased manner within a definite timeframe.
- A robust process needs to be in place for “effective malware control”. Typical controls to protect against malicious code use layered combinations of technology, policies and procedures and training. The controls are of the preventive and detective/corrective in nature.
- Establishing a robust network protection strategy and layered security based on the principle of defence-in-depth is an absolute necessity for banks.
- There should be arrangements for monitoring and reporting of the information security condition of the organization, which are documented, agreed with top management and

performed regularly. Security related metrics can be used to measure security policy implementation.

- Given the multiplicity of devices and systems, banks should deploy suitable automated tools for log aggregation and consolidation from multiple machines/systems and for log correlation and analysis.
- Security and Audit Processes of Critical service providers/vendors need to be assessed regularly since ineffective third-party controls can weaken the ability of a bank to achieve its control objectives.
- Commercial banks should implement ISO 27001 based Information Security Management System (ISMS) best practices for their critical functions. Additionally, other reputed security/IT control frameworks may also be considered by banks.
- Strong controls need to be initiated against any remote access facility. The management should establish policies restricting remote access and be aware of all remote-access devices attached to the bank’s systems. These devices should be strictly controlled.
- Events that trigger the implementation of a business continuity plan may have security implications. Risk assessments should consider the changing risks that appear in business continuity scenarios and different security postures that may need to be established.
- Information security assurance needs to be obtained through periodic penetration testing exercises, audits and vulnerability assessments. The assurance work needs to be performed by appropriately trained and independent information security experts/auditors. The strengths and weaknesses of critical internet-based applications, other critical systems and networks needs to be carried out before each initial implementation, and at least annually thereafter. Any findings needs to be reported and monitored using a systematic audit remediation or compliance tracking methodology.
- Provision of various electronic banking channels like ATM/debit cards/internet banking/phone banking should be issued only at the option of the customers based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions from the customer. A customer should not be forced to opt for services in this regard. Banks should provide clear information to their customers about the risks and benefits of using e-banking delivery services to enable customers to decide on choosing such services.
- In view of the proliferation of cyber attacks and their potential consequences, banks should implement two-factor authentication for critical activities like fund transfers and changing customer related details through internet banking facility.

- The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the institution’s internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or corporate/commercial); customer transactional capabilities (e.g., bill payment, fund transfer), the sensitivity of customer information being communicated to the bank and the volume of transactions involved.
- While not using the asymmetric cryptosystem and hash function is a source of legal risk, the banks, at the least, need to implement dynamic two-factor authentication through user id/password combination and second factor like (a) OTP/dynamic access code through various modes like SMS over mobile phones or hardware token or (b) a digital signature, through a card/token containing a digital certificate and associated private key (preferably for corporate customers).
- To enhance online processing security, confirmatory second channel procedures(like telephony, SMS, email etc.) should be applied with regard to transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits. In devising these security features, the bank should take into account their efficacy and differing customer preferences for additional online protection.
- Based on mutual authentication protocols, customers could also authenticate the bank’s web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes and/or the secure sockets layer (SSL) server certificate verification. In recent times, Extended Validation Secure Sockets Layer (EV-SSL) Certificates are increasingly being used. It should, however, be noted that SSL does not provide end-to-end encryption security at the application layer but is only designed to encrypt data in transit at the network transport layer.
- A risk based transaction monitoring or surveillance process needs to be put in place. The banks may consider dynamic scoring models and related processes to trigger or alert transactions which are not normal to improve preventive/detective capability. Study of customer transaction behavioral patterns and stopping irregular transactions or obtaining prior confirmation from customers for outlier transactions may be incorporated as part of the process.
- Chip based cards house data on microchips instead of magnetic stripes, making data more difficult to steal and cards more difficult to reproduce. It is recommended that RBI may consider moving over to chip based cards along with requiring upgradation of necessary infrastructure like ATMs/POS terminals in this regard in a phased manner.

- For debit / credit card transactions at the POS terminals, PIN based authorization system needs to be put in place (without any looping) in place of the existing signature based system and the non-PIN based POS terminals need to be withdrawn in a phased manner.
- Given that control, security and legal issues on cloud computing are still evolving, a bank needs to be cautious and carry out due diligence to assess the risks comprehensively before considering cloud computing.
- There needs to be forum of CISOs who can periodically interact and share experiences regarding any information security threats. It is reported that a CISO forum is already functional under IDRBT. The forum may, among other functions, endeavour to share good practices, identify any specific information security issues and flag them to appropriate stakeholders like the regulator, IBA etc.
- There is a need for a system of information sharing akin to the functions performed by FS-ISAC (Financial Services Information Sharing Agency) in the US. IDRBT as a sub-CERT to the banking system can function as a nodal point for information sharing.
- Accreditation and empanelment of security audit qualifications/certifications and security audit vendors can be considered at a wider level by the Government of India/CERT-In or by IDRBT for the banking sector.
- In order to reduce the time, cost, and complexity of software assurance and to ensure its security, sustainability and resilience and increase the effectiveness of the methods used by the banking industry for software assurance, an initiative similar to FSTC Software Assurance Initiative (SAI) in the US can be considered in India, possibly under the aegis of IDRBT along with various stakeholders.
- There is a need for IBA, IDRBT and reputed institutions like DSCI to collaborate and develop security frameworks and detailed implementation methodologies and procedures for the benefit of the banking sector, based on the information security related aspects covered in this report.
- There is an increasing need for specific detailed research in security of banking technology and bringing out innovative and secure banking products in collaboration with reputed academic bodies like the IITs. IDRBT can expand its activities/initiatives in this regard.
- Given the nature of the problem of cyber security, there needs to be engagement at a wider level nationally and internationally, with the government, law enforcement agencies, various industrial associations and academic institutions.
- RBI can consider having a multi-disciplinary Standing Committee on Information Security with representation from various stakeholders to consider new security related

developments and also legal developments, and based on the same, provide recommendations for suitable updation of guidelines on periodic basis.

- Collaborative efforts may also be made by reputed bodies like IDRBT, IIBF and DSCI coordinated by IBA to create customized indigenous certification courses to certify specific knowledge and skillsets in IT/information security areas for various categories of bank personnel at operational and managerial levels so as to create a large and diverse pool of requisite talent within the banking system.

On IT operations:

- The Board of Directors and Senior Management should oversee the implementation of a safe and sound IT operations environment. The policies and procedures defined as part of IT operations should support a bank's goals and objectives as well as follow statutory and regulatory requirements.
- IT operations include business services which are available to the internal or external customers of the organization using IT as a service delivery component. Instances include Mobile Banking and Internet Banking. IT Operations also include IT components which are used to support IT Operations, which can be service desk application, ticketing tools, event management tools etc. Banks may consider including test environment, quality assurance environment and any other such environment besides production environment within the scope of IT Operations.
- Banks should analyze their IT operation environment, including technology, human resources and implemented processes to identify threats and vulnerabilities and conduct a periodic risk assessment. As part of risk identification and assessment, banks should identify events or activities that could disrupt operations or negatively affect reputation or earnings and assess compliance to regulatory requirements. Banks should define various attributes for each risk component like probability of occurrence, financial impact etc. These attributes along with the business process involved should be used to prioritize risk mitigation actions and control framework.
- IT Strategy as framework should provide feedback to IT operations on the services to be supported, their underlying business processes, prioritization of these services etc. A well-defined IT strategy framework will assist IT operations in supporting IT services as required by the business and defined in SLAs.
- Service Valuation is the mechanism that can be considered by banks to quantify the services which are available to its customers (internal / external) and supported by IT operations in financial terms. Service Valuation will assist the IT Operation Function to showcase the involvement of the function in supporting the core business of the banks.

- Demand Management process provides guidelines which may be used by banks to understand the business processes IT operations support to identify, analyze and codify Patterns of Business Activities (PBA) to provide sufficient basis for capacity requirement.
- The components which should be considered when designing a new IT service or making a change to the existing IT service include business processes, service level agreements, IT infrastructure, IT environment etc.
- Over the years, the IT infrastructure in banks has grown and developed, and there may not be a clear picture of all the IT services currently being provided, and the consumers for each service. In order to establish an accurate IT landscape it is recommended that an IT Service Catalogue is defined, produced and maintained. The Service Catalogue can be considered a repository that provides information on all the IT services supported by the IT Operations framework.
- Banks need to institute a Service Level Management process for planning, coordinating, and drafting, agreeing, monitoring and reporting of service attributes used to measure the quality of service. The framework needs to include guidelines for ongoing reviews of service achievements to ensure that the required and cost-justifiable service quality is maintained and gradually improved. The Service Level Management framework defined by the banks should also have guidelines defined for logging and management including escalation of complaints and compliments.
- A Capacity Management process is required to ensure that cost-justifiable IT capacity for IT services exists and matches the current and future business requirements as identified in the Service Level Agreement. Banks adopting the capacity management process should ensure that the framework encompasses all areas pertaining to technology i.e. hardware, software, human resources, facilities etc.
- The availability and reliability of IT services can directly influence customer satisfaction and the reputation of banks. Availability Management is essential in ensuring IT delivers the right level of service required by the business to satisfy its business objectives. When defining Availability targets for a business service, banks should consider identifying Vital Business Function (VBF).
- Attributes that can be used by banks to report availability of IT services include availability (in percentage), Mean Time between service incidents, Mean Time between Failures and Mean Time to Repair.
- Implementation of Service Asset and Configuration Management framework has cost and resource implications and therefore there need to be strategic discussions about the priorities to be addressed.

- Banks need to implement a ‘change management’ process for handling any changes in technology and processes to ensure that the changes are recorded, assessed, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner and environment.
- Operations phase as part of the Service Management lifecycle is responsible for executing and performing processes that optimize the cost of the quality of services. As part of the organization, it is responsible for enabling the business to meets its objectives. As part of technology, it is responsible for the effective functioning of components that support business services. The various aspects that banks need to consider include event management, incident management, problem management and access management.

<u>On IT outsourcing:</u>

- The Board and senior management are ultimately responsible for outsourced operations and for managing risks inherent in such outsourcing relationships. Responsibilities for due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions continue to rest with the bank, Board and senior management.
- Banks need to assess the degree of ‘materiality’ inherent in the outsourced functions. Whether an outsourcing arrangement is ‘material’ to the business context or not is a qualitative judgment and may be determined on the basis of criticality of service, process or technology to the overall business objectives. Where a Bank relies on third party employees to perform key banking functions such as applications processing, etc. on a continuous basis, such outsourcing may also be construed as ‘material’, whether or not the personnel are located within the premises of the Bank.
- Outsourcing of non-financial processes, such as technology operations, is ‘material’ and if disrupted, has the potential to significantly impact business operations, reputation and stability of a Bank.
- Risk evaluation should be performed prior to entering into an outsourcing agreement and reviewed periodically in light of known and expected changes, as part of the strategic planning or review process.
- Banks should evaluate vendor managed processes or specific vendor relationships as they relate to information systems and technology. All outsourced information systems and operations may be subject to risk management and security and privacy policies that meet a bank’s own standards and any external requirements.
- While negotiating/ renewing an outsourcing arrangement, appropriate diligence should be performed to assess the capability of the technology service provider to comply with

obligations in the outsourcing agreement. Due diligence should involve an evaluation of all information about the service provider including qualitative, quantitative, financial, operational and reputational factors.

- Banks must be required to report to the regulator where the scale and nature of functions outsourced are significant, or extensive data sharing is involved across geographic locations as part of technology / process outsourcing
- The terms and conditions governing the contract between the bank and the service provider should be carefully defined in written agreements and vetted by the bank's legal counsel on their legal effect and enforceability.
- Banks should ensure that the contract brings out the nature of the legal relationship between the parties (agent, principal or otherwise), and addresses risks and mitigation strategies identified at the risk evaluation and due diligence stages. Contracts should clearly define the roles and responsibilities of the parties to the contract and include suitable indemnification clauses. Any ‘limitation of liability’ consideration incorporated by the service provider should be assessed in consultation with the legal department.
- In the event of multiple service provider relationships where two or more service providers collaborate to deliver an end to end solution for the financial institution, the bank remains responsible for understanding and monitoring the control environment of all service providers that have access to the bank’s systems, records or resources.
- Banks should establish a structure for management and control of outsourcing, based on the nature, scope, complexity and inherent risk of the outsourced activity.
- Management should include SLAs in the outsourcing contracts to agree and establish accountability for performance expectations. SLAs must clearly formalize performance criteria to measure the quality and quantity of service levels. For outsourced technology operations, specific metrics may be defined around service availability, business continuity and transaction security, in order to measure services rendered by the external vendor organization.
- Banks should evaluate the adequacy of the internal controls environment offered by the service provider. Due consideration should be given to implementation by the service provider of various aspects like information security policies and employee awareness of the same, logical access controls, physical and environmental security and controls, controls for handling data etc.
- Outsourcing should not impede or interfere with the ability of the bank or the regulator in performing its supervisory functions and objectives. As a practice, institutions should conduct pre- and post- outsourcing implementation reviews. An institution should also review its outsourcing arrangements periodically (atleast annually) to ensure that its

outsourcing risk management policies and procedures, and these guidelines, are effectively complied with.

- An institution should, at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet outsourcing obligations.
- Banks should also periodically commission independent audit and expert assessments on the security and control environment of the service provider.
- Banks should ensure that their business continuity preparedness is not compromised on account of outsourcing.
- Banks need to take effective steps to ensure that risks with respect to confidentiality and security of data are adequately mitigated.
- In the event of outsourcing of technology operations, the banks should subject the same to enhanced and rigorous change management and monitoring controls since ultimate responsibility and accountability rests with the bank.
- Banks, while framing the viable contingency plan, need to consider the availability of alternative service providers or the possibility of bringing the outsourced activity back-in-house in an emergency (for example, where number of vendors for a particular service is extremely limited) and the costs, time and resources that would be involved and be prepared to take quick action, if warranted.
- The engagement of service providers across multiple geographies exposes the organization to country risk – economic, social and political reasons in the country that may adversely affect the bank's business and operations. Banks should proactively evaluate such risk as part of the due diligence process and develop appropriate mitigating controls and as required, an effective exit strategy.
- Emerging technologies such as data center hosting, applications as a service and cloud computing have given rise to unique legal jurisdictions for data and cross border regulations. Banks should clarify the jurisdiction for their data and applicable regulations at the outset of an outsourcing arrangement. This information should be reviewed periodically and in case of significant changes performed by the service provider.
- Banks should ensure that quality and availability of banking services to customers are not adversely affected due to the outsourcing arrangements entered into by the bank. Banks need to institute a robust grievance redressal mechanism, which should not be compromised in any way due to outsourcing.
- IBA may facilitate requisite data sharing between banks to maintain scoring information for existing / new service providers which may include any fraud or major operational lapses committed by the service providers.

- Detailed service provider assessment and monitoring frameworks and best practices from a banking context can be explored by IBA in collaboration with institutions like DSCI and IDRBT.

On IS Audit:

- To meet the responsibility to provide an independent audit function with sufficient resources to ensure adequate IT coverage, the board of directors or its audit committee should provide an internal audit function which is capable of evaluating IT controls adequately.
- Banks should enable an adequately skilled composition of the Audit Committee to manage the complexity of the IS Audit oversight. A designated member of the Audit Committee needs to possess the relevant knowledge of Information Systems, IS Controls and audit issues. The designated member should also have relevant competencies to understand the ultimate impact of deficiencies identified in IT Internal Control framework by the IS Audit function. The Board or its Audit Committee members should seek training to fill any gaps in the knowledge related to IT risks and controls.
- The Audit Committee should devote appropriate and sufficient time to IS audit findings identified during IS Audits and members of the Audit Committee would need to review critical issues highlighted and provide appropriate guidance to the bank's management.
- Banks should have a separate IS Audit function within the Internal Audit department led by an IS Audit Head, assuming responsibility and accountability of the IS audit function, reporting to the Chief Audit Executive (CAE) or Head of Internal Audit. Where the bank uses external resources for conducting IS audit in areas where skills are lacking within the bank, the responsibility and accountability for such external IS audits still remain with the IS Audit Head and CAE.
- IS Auditors should act independently of the bank's management. In all matters related to the audit, the IS Audit should be independent of the auditee in both attitude and appearance. IS Auditors should be professionally competent, having the skills, knowledge, training and relevant experience to conduct an audit. IS Auditors should exercise due professional care, which includes following professional auditing standards in conducting the audit.
- Banks may decide to outsource the execution of segments of the audit plan to external professional service providers, as per the overall audit strategy decided in co-ordination with the CAE and the Audit Committee. The work outsourced shall be restricted to execution of audits identified in the audit plan. Banks need to ensure that the overall

ownership and responsibility of the IS Audit including the audit planning process, risk assessment and follow up of compliance remains within the Bank. External assistance may be obtained initially to put in place necessary processes in this regard, if required.

- An Audit Charter / Audit Policy is a document which guides and directs the activities of the Internal Audit function. IS Audit, being an integral part of the Internal Audit function, should also be governed by the same Audit Charter / Audit Policy. The audit policy should be documented to contain a clear description of its mandate, purpose, authority and accountability (of relevant members/officials in respect of the IS Audit i.e. IS Auditors, audit management and the audit committee) and the relevant operating principles. The document should be approved by the Board of Directors.
- IS Audit policy/charter should be subjected to an annual review to ensure its continued relevance and effectiveness.
- The IS auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys etc.) to understand the auditee's needs and expectations relevant to the IS audit function. These needs should be evaluated against the policy with a view to improving the service or changing the service delivery or audit charter, as necessary.
- Banks need to carry out IS Audit planning using the Risk Based Audit Approach. The approach involves aspects like IT risk assessment methodology, defining the IS Audit Universe, scoping and planning the audit, execution and follow up activities.
- The IS Audit Universe can be built around the four types of IT resources and various IT processes like application systems, information or data, infrastructure(technology and facilities like hardware, operating systems, database management systems, networking, multimedia, etc., and the environment that houses and supports them that enable the processing of the applications) and people (internal or outsourced personnel required to plan, organize, acquire, implement, support, monitor and evaluate the information systems and services).
- The IS Auditor must define, adopt and follow a suitable risk assessment methodology. A successful risk-based IS audit program can be based on an effective scoring system arrived at by considering all relevant risk factors. Banks should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the Audit Committee or the Board of directors. Risk assessment related guidelines will vary for individual banks depending on their size, complexity, scope of activities, geographic diversity, and various technologies/systems used.
- The IS Audit Plan (either separately or as part of the overall internal audit plan) should be a formal document, duly approved by the Audit Committee initially and during any

subsequent major changes. The Audit plan should be prepared so that it is in compliance with appropriate external regulatory/legal requirements, in addition to well-known IS Auditing Standards.

- The IS Audit Head is responsible for the annual IS Audit Plan which is prepared based on the scoping document and risk assessment. The Audit plan typically covers the overall audit strategy, scoped audit areas, details of control objectives identified in the scoping stage, sample sizes, frequency of audit based on risk assessment, nature and extent of audit and IT audit resources identification. A report on the status of planned versus actual IS audits, and any changes to the annual IS audit plan, needs to be presented periodically to the Audit Committee and Senior management.
- IT governance, information security governance related aspects, critical IT general controls like data centre controls and processes and critical business applications/systems having financial/compliance implications including MIS and regulatory reporting systems and customer access points (like delivery channels) need to be subjected to IS Audit(or integrated audit) atleast once a year (or more frequently, if warranted by risk assessment).
- IS Audits should also cover branches, with focus on large and medium branches, in critical areas like password controls, control of user ids, operating system security, anti-malware controls, maker-checker controls, segregation of duties, rotation of personnel, physical security, review of exception reports/audit trails, BCP policy and testing etc.
- Detailed pre-implementation application control audits and data migration audits with regard to critical systems need to be subjected to an independent external audit.
- Banks also need to conduct a post-implementation detailed application control audit. Furthermore, banks should also include application control audits in a risk based manner as part of the regular Internal Audit/IS Audit plans with focus on data integrity (among other factors). General internal auditors with requisite functional knowledge need to be involved along with the IS Auditors in the exercise to provide the requisite domain expertise.
- IS Auditors should periodically review the results of internal control processes and analyze financial or operational data for any impact on risk assessment or scoring. Accordingly, various auditee units should be required to keep auditors up to date on all major changes in departments or functions, such as the introduction of a new product, implementation of a new system, application conversions, significant changes in organization or staff , new regulatory and legal requirements, security incidents etc.
- IS Auditors should be reasonably conversant with various fraud risk factors and should assess the risk of occurrence of irregularities connected with the area under audit. The

IS Auditor should also consider Fraud Vulnerability assessments undertaken by the Fraud Risk Management group, while identifying fraud risk factors as part of IT risk assessment and audit process.

- Banks should consider using testing accelerators — tools and techniques that help support the procedures IS Auditors will be performing — to increase the efficiency and effectiveness of the audit.
- Auditors need to enhance utilization of CAATs, which may be used effectively in areas such as detection of revenue leakage, assessing impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume and value of transactions are reported. Suitable "read-only" access rights should be provided to auditors for enabling use of CAATs.
- Banks may consider, wherever possible, a continuous auditing approach for critical systems, which involves performing control and risk assessments on a more frequent basis by using technology suitably.
- The Board (or the Audit Committee) should be informed of Senior Management's decision on all significant observations and recommendations. When IS Auditors believe that the bank has accepted a level of residual risk that is inappropriate for it, they should discuss the matter with Internal Audit function and Senior Management. If the IS Auditors are not in agreement with the decision regarding residual risk accepted by the bank, IS Auditors and Senior Management should report the matter to the Board (or the Audit Committee) for resolution.
- Services provided by a third party are relevant to the scope of IS Audit of a bank when those services, and the controls within them, form part of the bank's information systems. These need to be adequately assessed as part of the IS Audit process.
- In order to provide assurance to management and regulators, banks are required to conduct a quality assurance, at least once every three years, on the Banks Internal Audit including IS Audit function to validate the approach and practices adopted by them in the discharge of their responsibilities as laid out in the Audit Policy.
- Accreditation and empanelment of IS audit qualifications/certifications and IS audit vendors/firms can be considered by the Government of India.

On Cyber Fraud:

- Most retail cyber frauds and electronic banking frauds would be of values less than Rs.1 crore and hence may not attract the necessary attention of the Special Committee of the Board. Since these frauds are large in number and have the potential to reach large proportions, it is recommended that the Special Committee of the Board be briefed separately on this to keep them aware of the proportions of the fraud and the steps taken by the bank to mitigate them. The Special Committee should specifically monitor 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.

- The activities of fraud prevention, monitoring, investigation, reporting and awareness creation should be owned and carried out by an independent fraud risk management group in the bank. The group should be adequately staffed and headed by a senior official of the bank, not below the rank of General Manager/DGM.
- Fraud review councils should be set up by the fraud risk management group with various business groups in the bank. The council should consist of the head of the business, head of the fraud risk management department, the head of operations supporting that particular business function and the head of information technology supporting that business function. The councils should meet at least every quarter to review fraud trends and preventive steps taken that are specific to that business function/group.
- Various fraud prevention practices need to be followed by banks. These include fraud vulnerability assessments(for business functions and also delivery channels), review of new products and processes, putting in place fraud loss limits, root cause analysis for actual fraud cases above Rs.10 lakhs, reviewing cases where a unique modus operandi is involved, ensuring adequate data/information security measures, following KYC and Know your employee/vendor procedures, ensuring adequate physical security, sharing of best practices of fraud prevention and creation of fraud awareness among staff and customers.
- No new product or process should be introduced or modified in a bank without the approval of control groups like compliance, audit and fraud risk management groups. The product or process needs to be analyzed for fraud vulnerabilities and fraud loss limits to be mandated wherever vulnerabilities are noticed.
- Banks have started sharing negative/fraudulent list of accounts through CIBIL Detect. Banks should also start sharing the details of employees who have defrauded them so that they do not get hired by other banks/financial institutions.
- Quick fraud detection capability would enable a bank to reduce losses and also serve as a deterrent to fraudsters. Various important requirements recommended in this regard include setting up a transaction monitoring group within the fraud risk management group, alert generation and redressal mechanisms, dedicated e-mail id and phone number for reporting suspected frauds, mystery shopping and reviews.
- Banks should set up a transaction monitoring unit within the fraud risk management group. The transaction monitoring team should be responsible for monitoring various types of transactions, especially monitoring of potential fraud areas, by means of which,

early alarms can be triggered. This unit needs to have the expertise to analyse transactions to detect fraud trends. This unit should work in conjunction with the data warehousing and analytics team within banks for data extraction, filtering, and sanitization for transaction analysis for determining fraud trends. Banks should put in place automated systems for detection of frauds based on advanced statistical algorithms and fraud detection techniques.

- It is widely accepted that fraud investigation is a specialized function. Thus, the fraud risk management group should undergo continuous training to enhance its skills and competencies.
- Apart from the categories of fraud that need to be reported as per RBI Master Circular on Frauds dated July 2, 2010, it is recommended that this should also include frauds in the electronic channels and the variants of plastic cards used by banks and their customers to conclude financial transactions.
- It has been noted that there is lack of uniformity regarding the amount of fraud to be reported to RBI. Some banks report the net loss as the fraud amount (i.e. fraud amount minus recovery), while others report the gross amount. Some do not report a fraud if the entire amount is recovered. In the case of credit card frauds, some banks follow the practice of reporting the frauds net of chargeback credit received while others report the amount of the original transactions. To overcome such inconsistency, a uniform rule of reporting amounts involved in frauds is being recommended.
- A special mention needs to be made of frauds done by collusive merchants who use skimmed/stolen cards at the point of sale (POS) terminals given to them by banks and then abscond with the money before the chargeback is received on the transaction. Many banks do not report such cases stating that the banks which have issued the cards are the ones impacted. However, in these cases, the merchants cause undue loss to the bank by siphoning off the credit provided. Hence such cases should be reported as frauds.
- It has been observed that in a shared ATM network scenario, when the card of one bank is used to perpetrate a fraud through another bank's ATM, there is a lack of clarity on who should report such a fraud to RBI. It is the bank acquiring the transaction that should report the fraud. The acquiring bank should solicit the help of the issuing bank in recovery of the money.
- Employee awareness is crucial to fraud prevention. Training on fraud prevention practices should be provided by the fraud risk management group at various forums.

- A positive way to create employee awareness is to reward employees who have gone beyond the call of duty and prevented frauds. Details of employees receiving such awards may be published in the fraud newsletters.
- In the case of online frauds, since the jurisdiction is not clear, there is ambiguity on where the police complaint should be filed and customers/banks have to shuttle between different police units on the point of jurisdiction. Cybercrime cells are not present in every part of the country. The matter of having a separate cell working on bank frauds in each state police department, authorized to register complaints from banks and get the investigations done on the same, needs to be taken up with respective police departments.
- To enhance investigation skills of the staff in the fraud risk management group, a training institute for financial forensic investigation may be set up by banks under the aegis of IBA.
- The experience of controlling/preventing frauds in banks should be shared between banks on a regular basis. The standing forum provided by the Indian Banks' Association (IBA) can be used to share best practices and further strengthen internal controls in respective banks.
- At each state, a Financial Crime Review Committee needs to be set up on frauds along the lines of the Security Committee that has been set up by the RBI to review security issues in banks with law enforcement authorities. The Committee can oversee the creation of awareness by banks among law enforcement agencies on new fraud types, especially technology based frauds.
- There needs to multi-lateral arrangements amongst banks to deal with on-line banking frauds. The lack of such an arrangement amongst banks may force a customer to interact with different banks/ organizations when more than one bank is involved. IBA could assist in facilitating such a mechanism.

On Business Continuity Planning (BCP):

- A bank's Board has ultimate responsibility and oversight over the business continuity planning of a bank and needs to approve the Business Continuity policy of the bank. A bank's Senior Management is responsible for overseeing the business continuity planning process which inter-alia includes determining how the institution will manage and control identified risks, prioritizing critical business functions, allocating knowledgeable personnel and sufficient financial resources to implement the BCP.
- A senior official needs to be designated as the Head of BCP function.

- Since electronic banking has functions which are spread across more than one department, it is necessary that each department understands its role in the plan and the support required to maintain the plan. In case of disaster, each department has to be prepared for the recovery process aimed at protection of the critical functions. To this end, a set up like the BCP Committee is charged with the implementation of the BCP in an eventuality and all departments are expected to fulfill their respective roles in a co-ordinated manner. Hence, a BCP/Crisis Management Committee consisting of senior officials from various departments like HR, IT, Legal, Business functions and Information Security needs to be instituted.
- There need to be adequate number of teams for handling various aspects of the BCP at the Central Office level as well as individual Zonal/ Controlling Office and branch levels.
- Banks should consider various BCP methodologies and standards, like BS 25999,as inputs for their BCP framework.
- The failure of critical systems or the interruption of vital business processes could prevent timely recovery of operations. Banks must fully understand the vulnerabilities associated with interrelationships between various systems, departments, and business processes. These vulnerabilities should be incorporated into the business impact analysis, which analyzes the correlation between system components and the services they provide.
- People aspect should be an integral part of a BCP. Too often, plans are focused on technical issues, therefore it is suggested that a separate section relating to people should be incorporated, including details on staff welfare, counseling, relocation considerations, etc.
- Pandemic planning needs to be incorporated as part of the BCP framework of banks.
- Banks must regularly test BCP to ensure that they are up to date and effective. Testing of BCP should include all aspects and constituents of the bank i.e. People, Processes and Resources (including Technology).
- Banks should involve their Internal Auditors (including IS Auditors) to audit the effectiveness of BCP and its periodic testing as part of their Internal Audit work and their findings/ recommendations in this regard should be incorporated in their report to the Board of Directors and Senior Management.
- Banks should consider having a BCP drill planned along with the critical third parties in order to derive reasonable level of assurance in ensuring continuity in respect of pre-identified minimal required processes during exigencies.
- Banks should perform the DR/BCP test without movement of bank personnel to the DR site. This will help in testing the readiness of alternative staff at the DR site.

- Business continuity plans should be maintained by atleast annual reviews and updates to ensure their continued effectiveness.
- Banks should also consider having an unplanned BCP drill, wherein only a restricted set of people and certain identified personnel may be aware of the drill and not the floor/business personnel.
- Various detailed requirements relating to procedural, infrastructural and HR related aspects of BCP have been provided so that banks can improve BCP processes and generate best outcomes.
- There are many applications and services in the banking system that are highly mission critical in nature and therefore require high availability and fault tolerance to be considered while designing and implementing the solution. This aspect is to be taken into account especially while designing and implementing the data centre solution and corporate network solution.
- The solution architectures of DC and DR are not identical for all applications and services. Generally, it is observed that critical applications and services, namely the retail, corporate, trade finance and government business solutions as well as the delivery channels have the same DR configurations whereas surround or interfacing applications do not have DR support. Banks will have to conduct periodic reviews with reference to the above aspect and upgrade the DR solutions from time to time and ensure that all critical applications and support services have perfect replicas in terms of performance and availability.
- The configurations of servers, network devices and other products at the DC and DR have to be identical at all times. This includes the patches that are applied at the DC periodically and the changes made to the software from time to time by customization and parameterization to account for regulatory requirements, system changes etc.
- Periodic checks to ensure data and transaction integrity between DC and DR are mandatory. Suitable automated tools may be leveraged in this connection.
- DR drills currently conducted periodically come under the category of planned shutdown. Banks have to evolve a suitable methodology to conduct drills which are closer to a real disaster scenario so that the confidence levels of the technical team taking up this exercise are built up to address requirements in the event of a real disaster.
- Consideration of telecom related redundancy and alternative data and voice communication channels in the event of exigencies should be incorporated as part of the business continuity planning.
- It is to be ensured that the support infrastructure at the DC and DR, namely the electrical systems, air-conditioning environment and other support systems do not have a single

point of failure and have a building management and monitoring system to continuously monitor the resources. Monitoring of uptime has to be made as per the requirements and agreements with respective vendors. The same requirements have to be taken care of in case the DC/DR set up is in an outsourced location or a common shared set up.

- Given the need for drastically minimizing data loss during exigencies and enabling quick recovery and continuity of critical business operations, banks need to consider near site DR architecture. Major banks with significant customer delivery channel usage and significant participation in financial markets/payment and settlement systems may need to consider a plan of action for creating a near site DR architecture over the medium term (say, three years).
- An industry-wide alarm and crisis forum/organization (in which the key market participants and the most important providers of financial infrastructure services are represented) may be established. The heads of BCP from the participating institutions can make up the top level of this crisis organization, with the lower levels forming a network between those responsible for the areas of liquidity, large-value payments, retail payment transactions and IT. Any of the institutions can invoke the alarm organization by activating the level affected.
- A website for industry-wide BCP related information for the benefit of the industry can be considered.
- There are programmes in the US like the Telecommunications Service Priority System (TSPS), Government Emergency Telecommunications service (GETS) and Wireless Priority Service Program (WPS) for provision of priority telecom availability and recovery services during exigencies for critical infrastructures and institutions. Similarly, the Government of India may declare the banking sector, including financial markets, as critical infrastructure and consider instituting such special measures for priority infrastructural services to enable conduct of critical banking services and financial market transactions during exigencies.

<u>On Customer Education:</u>

- The Board of Directors/Senior Management need to be committed to the process of consumer education initiatives by providing adequate resources, evaluating the effectiveness of the process and fine-tuning and improving customer education measures on an ongoing basis.
- To get desired support for the programme, it is important to identify and involve key stakeholders in decision-making, planning, implementation and evaluation. A working group or committee can be created to establish a clear goal for the endpoint in

consultation with key stakeholders, clearly define roles, responsibilities and accountabilities, communicate in an open, clear and timely manner, allowing for flexibility in approaches to suit different stakeholder needs, support training and development to ensure a change in behaviour and culture, learn from previous and ongoing experiences and celebrate achievements.

- Banks need to follow a systematic process to develop an awareness programme through the stages of planning and design, execution and management, and evaluation and course correction.
- Since awareness programmes should be customized for the specific audience, it is important to identify and segment the target users for the programmes - like bank customers, employees, law enforcement personnel, fraud risk professionals, media partners, etc.
- Building consensus among decision makers and stakeholders for financial and administrative support is an important step in the programme. In this respect, both fixed and variable costs need to be identified.
- Since the target groups obtain information from a variety of sources, more than one communication channel could be used to engage them successfully.
- A research group should be formed to continually update the communications team with the latest trends and evolving modus operandi. The team would maintain a repository of material such as case studies, sample mails, samples of fraudulent documents, international practice/developments etc.
- Evaluation of the effects of various campaigns for specific target groups can be measured through qualitative (e.g. focus groups, interviews) and/ or quantitative (e.g. questionnaires, omnibus surveys) research. Evaluation against metrics, performance objectives, etc. should also be conducted to check the campaign’s effectiveness, and to establish lessons learned to improve future initiatives.
- At the industry level, each bank should have a documented policy, training mechanisms and research units. Material can be pooled from these units to be used on a larger platform towards a common goal.

On Legal Issues:

- The Risk Management Committee at the Board level needs to put in place processes to ensure that legal risks arising from cyber laws are identified and adequately addressed. It also needs to ensure that the concerned functions are adequately staffed and the personnel handling it are trained to carry out the function efficiently. The Operational Risk Group needs to incorporate legal risks as part of the operational risk framework and take steps to mitigate the risks assessed. The legal function within the bank needs to advise business groups on legal issues arising out of the use of Information Technology.

- There should be a robust system in banks to keep track of the transactions of the nature referred to in statutory guidelines on AML (like PMLA and PMLR) and report the same within the prescribed period. Apart from the risk of penalty, this involves reputational risk for such entities.
- Under the NI Act, a cheque in the electronic form has been defined as “a mirror image” of a paper cheque. The expression ‘mirror image’ does not appear to be appropriate. The expression, “mirror image of” may be substituted by the expression, “electronic graphic which looks like” or any other expression that captures the intention adequately.
- The definition of a cheque in electronic form contemplates a digital signature with or without biometric signature and an asymmetric crypto system. Since the definition was inserted in the year 2002, it is understandable that it has captured only the digital signature and asymmetric crypto system dealt with under Section 3 of the IT Act, 2000. Since the IT Act,2000 has been amended in the year 2008 to make provision for an electronic signature also,a suitable amendment in this regard may be required in the NI Act so that the electronic signature may also be used on cheques in electronic form.
- There is uncertainty with respect to the meaning of a crucial expression like ‘intermediary” as per the IT Act 2000 and as amended by the IT Amendment Act, 2008. As such, it is necessary that clarity is brought about by a statutory amendment with regard to the meaning of the expression ‘intermediary’ in so far as banks and financial institutions are concerned.
- A combined reading of Section 2(p) and sub-sections (1) and (2) of Section 3 of the IT Act makes it clear that in terms of the Act an electronic record may be authenticated by affixing a ‘digital signature’ and if a party wants to authenticate the electronic record by affixing a digital signature, the electronic method or procedure for affixing the digital signature shall be an asymmetric crypto system and hash function. While authentication of an electronic record by affixing a digital signature is optional, the procedure for affixing the digital signature, namely, use of an asymmetric crypto system and hash function, is mandatory.
- The question that arises for consideration is whether a party may be bound by the transactions entered into through electronic means (whether through ATMs, Internet or otherwise) though the electronic records in question are not authenticated by using digital/electronic signatures. On reading Section 65B (1) of the Indian Evidence Act, it is clear that electronic records may be proved in court even though they are not authenticated by using digital or electronic signatures if the conditions mentioned therein

are satisfied. The difficulty in proving the various conditions set forth in sub-sections (2) and (3) of section 65B of the Indian Evidence Act is ameliorated to a great extent by sub-section (4) thereof under which the certificate of a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate.

- The Government should specify sufficient number of agencies under section 79A of the Indian Evidence Act to assist courts to arrive at a decision on the evidentiary value of electronic records irrespective of whether a digital or electronic signature is affixed.
- Financial transactions such as operation of bank accounts and credit card operations are being carried on by banks in a big way by using cards, pin numbers and passwords, etc. Banks are using many security features to prevent frauds to the extent possible. The proposed ‘two factor authentication method’ (2F method) is also a step in the same direction. It may not be ideal to mandate a particular technology (digital signatures with asymmetric crypto system and hash function) for authenticating all electronic transactions by banks.
- As a short term measure, it is recommended that Rules may be framed by the Central Government under Section 5 of the IT Act, to the effect that, with respect to internet or e-banking transactions, the 2F method or any other technique of authentication provided by banks and used by the customers shall be valid and binding with respect to such transactions, even if a ‘digital signature’ or ‘electronic signature’ is not affixed.
- The ISP license restricts the level of encryption for individuals, groups or organizations to a key length of only 40 bits in symmetric key algorithms or equivalents. RBI has stipulated SSL/ 128 bit encryption as a minimum level of security. SEBI has stipulated 64/128 bit encryption for Internet Based Trading and Services. Information Technology (Certifying Authorities) Rules, 2000 require’ internationally proven encryption techniques’ to be used for storing passwords. An Encryption Committee constituted by the Central Government under Section 84A of the IT Act, 2000 is in the process of formulating rules with respect to encryption. Allowance for higher encryption strength may be allowed for banks.
- Section 43A of the IT Act deals with the aspect of compensation for failure to protect data. The Central Government has not prescribed the term "sensitive personal data," nor has it prescribed a “standard and reasonable security practice”. Until these prescriptions are made, data is afforded security and protection only as may be specified in an agreement between the parties or as may be specified in any law.

- The IT Act, 2000 as amended, exposes the banks to both civil and criminal liability. The civil liability could consist of exposure to pay damages by way of compensation upto ₹ 5 crore under the amended Information Technology Act before the Adjudicating Officer and beyond ₹ 5 crore in a court of competent jurisdiction. The top management of banks could also suffer exposure to criminal liability given the provisions of Chapter XI of the amended Information Technology Act and the exposure to criminal liability could consist of imprisonment for a term which would extend from three years to life imprisonment, as also a fine. Further, various computer related offences are enumerated under various provisions of the Act.
- Of late there have been many instances of ‘phishing’ in the banking industry, posing a major threat to customers availing internet banking facilities. Though Section 66D of the amended IT Act could broadly be said to cover the offence of phishing, the attempt to commit the act of phishing is not made punishable. It is suggested that there is a need to specifically provide for punishment for an attempt to phish as well, in order to deter persons from attempting it.
- The issue of whether Section 43A read with Section 72 and 72A of the IT Act, 2000 address the issue of data protection adequately or whether they need to be supplemented by long-term provisions(which can help facilitate effective and efficient protection and preservation of data), would depend on the prescriptions of the Central Government. Various suggestions have been offered in this report in this regard.
- It is necessary to balance the interests of customers and those of banks and provide protection to banks against any fraudulent or negligent acts by the customer. It is not appropriate to leave such an important issue to be dealt with in documentation. Appropriate statutory provisions need to be enacted in this regard.
- Though there is no specific legislation in India which deals only with ‘electronic fund transfer’ and which is consumer protection driven, certain concerns have been dealt with in the Payment and Settlement Systems Act, Rules, Regulations, directions, etc. issued thereunder as well as the provisions of general law. However, it may be apposite to have some provisions similar to those in the EFT Act which exempts the bank from liability in the event of fraud by the customer or a technical failure, etc. (for eg., provisions dealing with ‘unauthorized electronic fund transfers’ and the consumer’s liability for unauthorized transfers).