Need for Strengthening the IT Governance Framework in Banking Sector for Achieving Digital Operational Resilience

Proactively, by a Master Direction issued in November 2023, the Banking Sector Regulator, the Reserve Bank of India introduced mandatory requirements for ensuring that the IT governance framework is functional and effective, and it can manage risks from cyber threats and risks emanating from third-party service providers and vendors. The RBI framework requires entities operating in the banking sector in India to identify risks, report incidents, take preventive and remedial measures and ensure business continuity. The Master Direction has already come into force with effect from 01st April 2024. At this point of time, the European union introduced the Regulations for financial sector entities for achieving digital operational resilience. These EU Regulations provide a lot of insights, especially in the areas of imposing contractual obligations on third-party service providers. This article underscores the need for benefitting from certain aspects the EU Regulations. Having been an independent director of a private sector bank, with considerable experience on the nuances of overall governance, the author highlights the need for greater attention at the level of Board of Directors on this important subject.

CS (Dr.) Ravichandran K S, FCS
Managing Partner
KSR & Co Company Secretaries LLP
Bangalore, Chennai and Coimbatore
ksr@ksrandco.in

INTRODUCTION

It is not necessary to highlight the significant presence made and predominance achieved by digital banking, its proactive and inclusive approach, its ability to promoting ease of doing business and its green quotient too. However, it comes with its own challenges and threats and therefore it is necessary to underscore the need for full-fledged board level attention on every aspect of digital banking so as to meet challenges and overcome the threats in order to be able to achieve digital operational resilience.

As per RBI's Master Direction on Information Technology, Risk, Controls and Assurance Practices, dated 07th November 2023, (the Master Direction), which came into force from the 01st April 2024, the key focus areas of IT Governance shall include strategic alignment, risk management, resource management, performance management and Business Continuity/ Disaster Recovery Management. Business continuity can be measured by the level of preparedness of a given organisation to be able to resume its normal services within the shortest possible time with continuity, and without any issues on integrity. In other words, operational resilience expects an entity in the banking sector to restore operations at the earliest if they are hit by cyberattacks to prevent or minimize financial and reputation losses to the Bank and losses to its customers, as well as preventing data theft and customer frustration. Delays in resumption of normal business activities has the potential to cause cascading losses to customers as banking system plays an important role in enabling customers to honour their commitments to their creditors, lenders, vendors, and employees.

OBJECTIVE OF THIS ANALYSIS

The liability side of the balance sheet of any banking company / entity is characterised by public interest because most of the funds in deployment are funded by deposits from public. Concomitant with growing digital banking, there has been unprecedented increase in dependence on software and hardware tools, systems, processes, and IT professionals and third-party service providers and also actual and potential cyber threats. Any major incidence such a cyber-attack on the banking system would not only jeopardize integrity and security of the network and information systems but also would create enormous difficulties to the availability, authenticity, reliability, integrity, and confidentiality of data and the ability of the Bank to resume its normal activities. Such an occurrence could cause significant financial and reputational losses. Therefore, it is necessary to look at the RBI Master Direction on IT Governance Framework objectively and consider its requirements in juxtaposition with the regulations introduced by the lawmakers in the European Union with a focus towards achieving digital operational resilience.

INTRODUCTION TO THE MASTER DIRECTION OF RBI

The Master Direction issued by RBI sets the broad but mandatory IT Governance Framework to be installed,

inter alia, by banking companies / entities (referred to as Regulated Entities or REs, in short). As per the aforesaid Master Direction, "Information Asset" includes any piece of data, device or other component of the environment that supports information-related activities. Information Assets include information system, data, hardware, and software and "Information Systems" means a set of applications, services, information technology assets or other information-handling components, which includes the operating environment and networks. The expression "IT Risk" refers to the business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise. As per the Master Direction, "Cyber-attack" are malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorized access to assets.

The Master Direction mandates REs to put in place a robust IT Governance Framework that inter alia (i) specifies the governance structure and processes necessary to meet the RE's business/ strategic objectives; (ii) specifies the roles (including authority) and responsibilities of the Board of Directors (Board) / Board level Committee and Senior Management; and (iii) includes adequate oversight mechanisms to ensure accountability and mitigation of IT and cyber/ information security risks and (iv) provides for business continuity and disaster management.

RESPONSIBILITY OWNERS IN IT GOVERNANCE STRUCTURE

The Master Direction itself provides some clarity on the above subject. Starting from the Board of Directors, it explains broadly the role of a committee to be constituted under the name and style of IT Strategy Committee. The Master Direction places certain responsibilities on senior management and requires the constitution of another committee to be styled as the IT Steering Committee. The Master Direction mandates the need for having technically competent officer of sufficient seniority, known as Chief Technology Officer or Chief Information Officer or by whatever name called with clear cut responsibilities to be designated as the Head of IT Function itself.

The roles and functions of each one of the responsibility owners are as follows:

- **Board of Directors:** The Role of Board of Directors is confined to formulating the strategies and approving policies related to IT, Information Assets, Business Continuity, Information Security, Cyber Security (including Incident Response and Recovery Management/ Cyber Crisis Management). RBI stipulates that the Board of Directors must mandatorily review the strategies and policies at least annually.

- **IT Strategy Committee:** The IT Governance Framework places a lot of weight on IT Strategy Committee. This is a Board level committee. It should have a minimum of 3 directors as its members. It should be chaired by an independent director having substantial IT Expertise in managing / guiding information technology initiatives. The most important task of this committee is to guide in preparation of IT Strategy and to ensure that the IT Strategy aligns with the overall strategy of the RE towards accomplishment of its business objectives. If this committee applies its collective mind on this task with requisite attention and care, output will be good. This committee should satisfy itself that the IT Governance and Information Security Governance structure fosters accountability, is effective and efficient, has adequate skilled resources, well defined objectives, and casts unambiguous responsibilities for each level in the organisation.

  Apart from the above two major responsibilities, this Board level committee must ensure the following too:

  1. Ensure that the RE has put in place processes for assessing and managing IT and cybersecurity risks;
  2. Ensure that the budgetary allocations for the IT function (including for IT security), cyber security are commensurate with the RE's IT maturity, digital depth, threat environment and industry standards and are utilised in a manner intended for meeting the stated objectives; and
  3. Review, at least on annual basis, the adequacy and effectiveness of the Business Continuity Planning and Disaster Recovery Management of the RE.

  An Information Security Committee (ISC), under the oversight of the IT Steering Committee, is required to be formed for managing cyber/ information security. It would be very clear that the mandate from this Master Direction of RBI is that at least on an annual basis this Board level committee is required to assess the adequacy and effectiveness of the Business Continuity Planning and Disaster Recovery Management of the RE. A note clarifies that a reference to Business Continuity/ Disaster Recovery Management in this Master Direction is limited to operational resilience focussing on People, Processes and Systems associated with the IT, IS, information / cyber security controls and operations. It is under the responsibilities of the IT Strategy Committee, the Master Direction speaks about operational resilience. Thus, the term "operational resilience" is not a new term. However, it would be useful to bring out the significance of the term "operational resilience."

- **Senior Management:** The Senior Management of the RE shall, inter alia, ensure the following:

  1. Implementation of the IT Strategy
  2. Ensuring IT/ IS and their support infrastructure are functioning effectively and efficiently;
  3. Ensuring necessary IT risk management processes are in place;
  4. Create a culture of IT risk awareness and cyber hygiene practices in the RE;
  5. Ensuring that the Cyber security posture of the RE is robust; and
  6. Ensuring IT contributes to productivity, effectiveness, and efficiency in business operations.

Of the above, the most important task of senior management is that of implementing the IT Strategy. IT Strategy itself will encompass all other items listed down. Since, this is a collective responsibility of the senior management, the Board of Directors must identify who are all the officers who will form part of the "senior management" and make it clear that there is a senior most officer who leads team and overall IT governance policy spells out these needs. It would be possible to constitute a committee which may be styled as IT Senior Management Committee and operationalize these requirements. The meetings of this executive committee could be recorded in brief so that ATR also gets generated and reviewed from time to time.

- **IT Steering Committee:** While IT Strategy Committee must review at least on annual basis the adequacy and effectiveness of the Business Continuity Planning and Disaster Management, it is the responsibility of the IT Steering Committee to oversee the processes put in place for business continuity and disaster recovery.
- **Head of IT Function:** Drilling down further, it will be clear that there must be a sufficiently senior person technically competent and experienced official who shall be the Head of the IT function and it is his responsibility to "put in place an effective disaster recovery set up and business continuity strategy / plan.

> As per the Master Direction issued by RBI "Information Asset" includes any piece of data, device or other component of the environment that supports information-related activities.

IMPORTANT AND MANDATORY STIPULATIONS OF THE IT GOVERNANCE FRAMEWORK

- **IT Service Management Framework for Disaster Management and Business Continuity:** From the angle of disaster management and business continuity, the IT Governance Framework requires REs to put in place a robust IT Service Management Framework. REs are mandated to avoid using outdated and unsupported hardware or software and shall monitor the software's end of support (EOS) date and annual maintenance contract dates of IT Hardware on an ongoing basis. REs shall develop a technology refresh plan for the replacement of hardware and software in a timely manner before they reach EOS.
- **Business Continuity Plan (BCP) and Disaster Recovery (DR) Policy :**

  1. The BCP and DR policy shall adopt best practices to guide its actions in reducing the likelihood or impact of the disruptive incidents and maintaining business continuity. The policy shall be updated based on major developments/ risk assessment.

  2. RE's BCP/ DR capabilities shall be designed to effectively support its resilience objectives and enable it to rapidly recover and securely resume its critical operations (including security controls) post cyber-attacks/ other incidents.

- **Disaster Recovery Management**

  1. Periodicity of DR drills for critical information systems shall be at least on a half-yearly basis and for other information systems, as per RE's risk assessment.

  2. Any major issues observed during the DR drill shall be resolved and tested again to ensure successful conduct of drill before the next cycle.

  3. The DR testing shall involve switching over to the DR / alternate site and thus using it as the primary site for sufficiently long period where usual business operations of at least a full working day (including Beginning of Day to End of Day operations) are covered.

  4. REs shall regularly test the BCP / DR under different scenarios for possible types of contingencies, to ensure that it is up-to-date and effective.

  5. REs shall backup data and periodically restore such backed-up data to check its usability. The integrity of such backup data shall be preserved along with securing it from unauthorised access.

  6. REs shall ensure that DR architecture and procedures are robust, meeting the defined RTO and RPO for any recovery operations in case of contingency.

  7. REs should prioritise achieving minimal RTO (as approved by the RE's ITSC) and a near zero RPO for critical information systems.

  8. In a scenario of non-zero RPO, REs shall have a documented methodology for reconciliation of data while resuming operations from the alternate location.

  9. REs shall ensure that the configurations of information systems and deployed security patches at the DC and DR19 are identical.

  10. REs shall ensure BCP and DR capabilities in critical interconnected systems and networks including those of vendors and partners. REs shall ensure demonstrated readiness through collaborative and co-ordinated resilience testing that meets the REs' RTO.

THIRD-PARTY ARRANGEMENTS

Where third-party arrangements in the Information Technology/ Cyber Security ecosystem are not within the applicability of the Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023, REs shall, put in place appropriate vendor risk assessment process and controls proportionate to the assessed risk and materiality to, inter alia:

1. mitigate concentration risk;
2. eliminate or address any conflict of interests;
3. mitigate risks associated with single point of failure;
4. comply with applicable legal, regulatory requirements and standards to protect customer data;
5. provide high availability (for uninterrupted customer service); and
6. manage supply chain risks effectively.

One of the interesting requirements is that REs shall obtain a certificate or a written confirmation from the application developer or vendor stating that the application is free of known vulnerabilities, malware, and any covert channels in the code. Such a certificate or a written confirmation shall also be obtained whenever material changes to the code, including upgrades, occur.

However, the most important part lies in understanding the need to assess carefully the gaps and slips between words orally spoken and presentations made by the third-party service providers and vendors and the words the contract speaks in writing. Many a times, REs may have ensured that the contractual covenants and obligations are captured sufficiently. However, the REs may not have put in a place responsible system to oversee the performance of the third-party service provider or vendor and their delays, deficiencies, defaults, and deviations which could constitute not only a material breach on the part of the third-party service provider or vendor but also could significantly cause risks to the REs and hamper the ability of REs to achieve operational resilience. The Senior Management or the committee of those officers who are identified by the RE as the Senior Management for this purpose must be entrusted with the task reviewing these aspects. In short, it should form part of IT Strategy.

VULNERABILITY ASSESSMENT (VA) / PENETRATION TESTING (PT)

1. For critical information systems and/ or those in the De-Militarized Zone (DMZ) having customer interface, VA shall be conducted at least once in every six months and PT at least once in 12 months. Also, REs shall conduct VA/ PT of such information systems throughout their lifecycle (pre-implementation, post implementation, after major changes, etc.).
2. For non-critical information systems, a risk-based approach shall be adopted to decide the requirement and periodicity of conduct of VA/ PT.
3. VA/ PT shall be conducted by appropriately trained and independent information security experts/ auditors.
4. In the post implementation (of IT project/ system upgrade, etc.) scenario, the VA/ PT shall be performed on the production environment. Under unavoidable circumstances, if the PT is conducted in test environment, REs shall ensure that the version and configuration of the test environment resembles the production environment. Any deviation should be documented and approved by the ISC.
5. REs shall ensure to fix the identified vulnerabilities and associated risks in a time-bound manner by undertaking requisite corrective measures and ensure that the compliance is sustained to avoid recurrence of known vulnerabilities such as those available in Common Vulnerabilities and Exposures (CVE database.
6. REs shall put in place a documented approach for conduct of VA/ PT covering the scope, coverage, vulnerability scoring mechanism (e.g., Common Vulnerability Scoring System) and all other aspects. This may also apply to the RE's information systems hosted in a cloud environment.

CYBER INCIDENT RESPONSE AND RECOVERY MANAGEMENT

1. The cyber incident response and recovery management policy shall address the classification and assessment of incidents; include a clear communication strategy and plan to manage such incidents, contain exposures, and achieve timely recovery.
2. REs shall analyse cyber incidents (including through forensic analysis, if necessary) for their severity, impact and root cause. REs shall take measures, corrective and preventive, to mitigate the adverse impact of incidents on business operations.
3. REs shall have written incident response and recovery procedures including identification of key roles of staff/ outsourced staff handling such incidents.
4. REs shall have clear communication plans for escalation and reporting the incidents to the Board and Senior Management as well as to customers, as required. REs shall pro-actively notify CERT-In and RBI17 regarding incidents, as per regulatory requirements. REs are also encouraged to report the incidents to Indian Banks – Centre for Analysis of Risks and Threats (IB-CART) set up by IDRBT.
5. REs shall establish processes to improve incident response and recovery activities and capabilities through lessons learnt from past incidents as well as from the conduct of tests and drills. REs, inter alia, shall ensure effectiveness of crisis communication plan/ process by conduct of periodic drills/ testing with stakeholders (including service providers).

IMPORTANT ASPECTS OF EU-DORA

A perusal of REGULATION (EU) 2022/2554 of the EUROPEAN PARLIAMENT and of the COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA) will be of immense benefit to enhance the depth of the governance architecture to be built by an RE in relation to digital operational resilience. While RBI has introduced the

need for a mandatory IT Governance Framework for entities of a class such as Banks, NBFCs, CICs as well as to named institutions, DORA goes by specified activities.

DORA covers the entire spectrum of Information and Communication Technology (ICT). DORA signifies the ability of a financial entity to build, assure, and review its operational integrity and reliability by ensuring, directly or indirectly through services of third-party ICT service providers, the full range of ICT related capabilities that are required to address the security of the network and information systems, for continued provisions of services of the financial entity.

DORA requires financial entities to have proper mechanisms and policies for handling all ICT related incidents and for reporting major ICT related incidents and for testing ICT systems, controls, and processes and for managing third-party risks. Nature, frequency, significance, and impact of ICT incidents must be reported. DORA says that undetected vulnerabilities pose threat and regulations are designed to remove gaps in the ICT Reporting Framework and remove existing overlaps, duplications and reduce costs.

The DORA provides and promotes a set of principles that facilitate the overall structure of ICT risk management. The functions of ICT risk management framework includes (a) identification; (b) protection and prevention; (c) detection; (d) reporting; (e) response and recovery; and (f) learning and evolving and communication. ICT systems must be reliable, agile, and capable not only for guaranteeing the processing of data required for their services but also for ensuring sufficient technological resilience to allow them to deal with additional processing needs due to stressed market conditions or other adverse situations.

The key stipulations under DORA are as follows:

1. establish a role to monitor their arrangements concluded with ICT Third Party service providers on the use of ICT services;
2. designate a member of senior management to be responsible for overseeing the related risk exposure and relevant documentation;
3. assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such control function to avoids conflicts of interests;
4. document and review at least once a year the risk management framework;
5. do internal audit on a regular basis their ICT risk management framework;
6. perform in depth assessments after every major change in their network and info system infrastructure and processes;
7. conduct regularly risk analysis on legacy ICT systems;
8. carry out internal independent review of the implementation of ICT responses and recovery plans;
9. have a crisis management function;
10. expand testing of business continuity and response and recovery plans to capture switchover scenarios between primary ICT infrastructure and redundant facilities;
11. report to competent authorities upon their request, an estimation of aggregated annual costs and losses caused by ICT related incidents;
12. identify redundant ICT capacities;
13. communicate to competent authorities implemented changes after occurrence of ICT related incidents;
14. monitor on a continuous basis relevant technological developments;
15. establish a comprehensive digital operational resilience testing programme as an integral part of ICT risk management framework;
16. adopt and regularly review a strategy on ICT third-party risks.

In so far as contractual arrangements with third-party ICT service providers, DORA stipulates that contractual arrangements must contain provisions laying down the relevant guarantees for -

1. enabling the access, recovery and return of data in the case of insolvency or discontinuation of business or winding up of the third-party service provider.
2. providing assistance upon occurrence of ICT incidents connected to the services provided, at no additional cost or at a pre-determined additional cost;
3. cooperating with competent authorities;
4. proper termination of rights subject to minimum notice period;
5. allowing the financial entity to have full control of all developments occurring at the third-party service provider which may impair the financial entity's ICT security;
6. providing a comprehensive and operational understanding of the ICT risk management of the ICT third-party service provider;
7. enable a lead overseer of the financial entity to examine their facilities from where the services are actually going to be provided, even if such facilities are located in a country other than that of the financial entity;
8. conferring powers on the lead overseer to conduct investigations, to carry out onsite and off-site inspections at the premises and locations of critical ICT third-party service providers such that the lead overseer is able to acquire a real insight into the type, dimension, and impact of the ICT third-party risk posed to the financial entity;

The contract should contain a complete description of functions and services; location where such functions are provided; locations where data (of the financial entity) are going to be processed; and must contain a clear specification of full-service level descriptions with precise quantitative and qualitative performance targets so as to be able to take appropriate corrective actions without undue delay when third-party service provider does not meet agreed service levels. DORA Regulations go to the extent of prescribing in a granular manner that the contracts must contain clauses for relevant notice periods and reporting obligations of the ICT thirty party service provider in case their ability to provide service is impaired significantly. Further, there must a stipulation in the contract that the third-party service provider agrees to implement and

test contingency plans and have ICT security measures, tools and policies allowing for secure provisions of sources. The financial entity should have the right to take copies of crucial instruments. The third-party service provider must enable right of access, inspection and audit by the financial entity or by an appropriate independent third-party inspection team. The ICT third-party service provider should agree to designate a legal person as their coordination point.

Contracts with third-party service providers must contain provisions specifying how the accessibility; availability; integrity, security and protection of personal data would be ensured by the ICT third-party service provider.

MASTER DIRECTION AND DORA

Broadly speaking, RBI's IT Governance Framework as contained in the Master Direction provides the following: illuminating requirements under five important heads viz.,

1. An extensive description of the governance structure specifying the governance organs and their hierarchy, their roles, and responsibilities.
2. Business Continuity Plan.
3. Disaster Recovery Management.
4. Third-Party Arrangements.
5. Vulnerability Assessment and Penetration Testing.
6. Cyber Incident Response and Recovery Management.

Under DORA, the comprehensive ICT risk management framework should include–

1. assessment of the internal risk profile by a comprehensive review of ICT systems, processes and people, including a study of legacy assets and redundant assets;
2. periodical review of ICT assets, people, and systems;
3. assess risks emanating from ICT third-party service providers' side;
4. robust incident reporting;
5. constant vulnerability and penetration testing; scenario-based testing; compatibility testing; performance testing;
6. assess the effectiveness of ICT risk management framework in their preventive, detective, responsive and recovery capabilities;
7. assess the effectiveness of ICT risk management framework to uncover and address potential ICT vulnerabilities and in limiting damage;
8. assess the effectiveness of ICT risk management framework to enable resumption of activities and recovery actions without jeopardizing integrity and security of the network and information systems as well as the availability, authenticity, reliability, integrity, and confidentiality of data;
9. assess the effectiveness of the ICT risk management framework to rescue operations in the shortest possible time upon occurrence of any serious disrupting ICT related incidents; and
10. assess the effectiveness of the ICT risk management framework to achieving digital operational resilience meaning thereby efficient business continuity and recovery plans.

CONCLUSION

Basically, the RBI Framework provides a robust guidance on the roles and responsibilities of various governance organs commencing from the level of Board of Directors and responsibility owners. Particularly, through the Master Direction, RBI lays emphasis on the significance of three things, viz., (1) Business Continuity Plan (BCP) and Disaster Recovery Management; (2) Vulnerability Assessment (VA) / Penetration Testing (PT) and (3) Cyber incidence reporting requirements, response and recovery management.

DORA is certainly more prescriptive than what RBI's IT Governance Framework provides. DORA lays more emphasis in underscoring the mandatory review requirements, vulnerability testing requirements and incident reporting requirements, and understanding of the risks that are likely to arise from ICT third-party service providers. DORA stresses on the need for proper and specific contractual clauses imposing a mandatory need for such service providers to sign covenants undertaking a range of obligations. It is true that on account of varied governance systems, processes and practices, systems and tools of different ages acquired, operated and used, technological developments, frequent changes in officials in charge of ICT risk management framework, increased risks from internal weaknesses, negligence in assessing risks, likely laxity in vulnerability and penetration testing, risks arising from weak contractual arrangements with third-party service providers, inadequacies in legal drafting of contracts with ICT third-party service providers, it is necessary that RBI undertakes a comprehensive review of its Master Direction on IT Governance Framework of Banks and strengthens the same wherever necessary.

In short, it is high time banking sector identifies critical ICT third-party service providers and introduces necessary contractual obligations coupled with guarantees for performance of material obligations acquiring specific rights aimed towards achieving digital operational resilience. There are definitely two areas where the RBI, the banking sector regulator in India must advise banks to gear up and take necessary measures viz., (a) in stipulating that the contracts with ICT third-party service providers must be strengthened on the lines provided under DORA, if not anything more; and (b) for augmenting the strength of the Board itself with not less than two directors having rich high level operational experience in ICT, of which one must be at least a whole-time director and the other must be an independent director. The IT Strategy Committee of a Bank could get useful insights from DORA and perform its most important task of reviewing the adequacy and effectiveness of Business Continuity Planning and Disaster Recovery Management of the Bank for ensuring operational resilience.

REFERENCES:

i. *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices issued by RBI on 7th November 2023.*

ii. *REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*