Navigating RBI's IT Master Directions: Key Insights from Mehta & Mehta Session

Information Technology (IT) governance and cybersecurity have become central to RBI's regulatory agenda, particularly for NBFCs. With the introduction of the **Master Direction on IT Governance, Risk, Controls, and Assurance Practices (2023)**, RBI has consolidated its earlier fragmented guidelines into a single, comprehensive framework.
In a recent session hosted by **Mehta & Mehta**, experts highlighted how these directions reshape compliance expectations for NBFCs—covering IT governance, documentation, vendor management, cybersecurity, and business continuity. The discussions emphasized RBI's intent to build **digital resilience, transparency, and accountability** in NBFC operations.

Compliance Beyond the Checklist

- **Letter and spirit**: RBI expects compliance not only in action but also through **proper documentation** and audit trails.
- **Audit readiness**: If processes are not recorded on paper, they may not stand scrutiny during supervisory inspections or disputes.
- **Committee documentation**: Appointment of members to IT committees must clearly mention **technical expertise**, rationale, and board approvals.

IT Governance and Committee Framework

- **IT Strategy Committee (ITSC)**
  - Minimum three directors, chaired by an Independent Director with **7+ years of IT governance experience**.
  - Meets quarterly to review IT strategy, cybersecurity, budgets, and disaster recovery.
  - Ensures IT is aligned with NBFC's business strategy.
- **IT Steering Committee**
  - Senior management-led, supports ITSC in **project oversight** and IT-business alignment.
  - Oversees business continuity and implementation of IT architecture.
- **Information Security Committee (ISC)**
  - Headed from the **risk management vertical** and includes the CISO.
  - Focuses on **cybersecurity policy, incident response, and risk mitigation**.
  - Reviews incidents, audits, and mitigation strategies, updating ITSC and the CEO periodically.

Cybersecurity and CISO's Role

- **Clear mandates**: Appointment letters for CISOs must explicitly state **roles, responsibilities, and technical expertise**.
- **Documentation**: Resolutions and HR letters should support the appointment.
- **Cyber resilience**: NBFCs must establish measurable metrics for system performance and incident recovery.

Policies and Frameworks Required

NBFCs must frame and regularly update policies including:

- **Change & Patch Management Policy** – to ensure secure upgrades without disruptions.

- **Data Migration Policy** – integrity, completeness, and audit trail during system migrations.
- **Risk Management Policy** – incorporating IT and cybersecurity risks reviewed annually.
- **Information Security & Cybersecurity Policies** – with clear crisis management and response protocols.
- **Business Continuity & Disaster Recovery Policy** – ensuring critical services remain operational during cyberattacks or disasters.
- **IS Audit Policy** – approved by the Audit Committee, reviewed annually.

Vendor and Outsourcing Risk

- RBI mandates **vendor risk assessments**, especially in IT outsourcing.
- NBFCs must conduct due diligence covering financial stability, cybersecurity maturity, and contingency planning.
- Proprietorship vendors are seen as **higher risk** compared to incorporated entities; enhanced due diligence is required if engaged.
- **Source code escrow arrangements** must be in place where vendors refuse to share source codes for critical applications.

Business Continuity and Disaster Recovery (BCP/DR)

- NBFCs must have **tested recovery mechanisms** to minimize downtime.
- Daily or periodic **data backups**, preferably stored offsite, are crucial.
- BCP ensures uninterrupted operations during disruptions, while DR focuses on **swift restoration** of systems and services.

Expert Insights and Practical Challenges

- **Independent Directors with IT expertise** are difficult to find, posing a compliance hurdle.
- Compliance now requires a **cultural shift**—beyond company secretaries, IT teams and senior management must align.
- **Documentation burden**: Even strong systems may fail regulatory scrutiny if not properly documented.
- **Cybersecurity as survival**: Experts noted that cyber risk is no longer a technical issue—it is a **business survival issue**.

Conclusion

The **RBI IT Master Directions (2023)** mark a shift from **reactive** compliance to **preventive digital governance**. For NBFCs, this is more than a regulatory mandate—it is an opportunity to strengthen resilience, safeguard customer trust, and align with global best practices.

As panelists at the Mehta & Mehta session emphasized, **"Do what you say, and say what you do."** Documentation, governance, and proactive risk management will determine which NBFCs emerge stronger in India's digital financial ecosystem.

 To access the full webinar recording and related resources, visit:
YouTube Channel: "Decoding Corporate Laws with Mehta & Mehta"