The Reserve Bank of India Master Directions Compliance

Adhering to the Reserve Bank of India (RBI) Master Directions Compliance in Banks and NBFCs with ARCON's robust IT Risk Management Solutions

Table of Content

Banks and NBFCs in India

The Banks and Non-Banking Financial Corporations (NBFCs) in India play a critical role in nation building and economic growth. These institutions provide essential financial services and products to individuals, businesses, and governments.

In the backdrop of macroeconomic stability, and positive operating environments, the nation is well positioned for a sustained economic growth outlook. However, in the age of digitalisation, where more systems are inter-connected, any IT vulnerability can lead to a catastrophe and give rise to systemic risks.

In this regard, the RBI has issued the final Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Master Directions 2023 that has come into force from April 1, 2024.

What does The Reserve Bank of India Master Directions Compliance say?

The Reserve Bank of India (RBI) issues Master Directions to consolidate instructions on rules and regulations framed under various Acts, including banking issues and foreign exchange transactions. A comprehensive guideline related to information technology (IT) governance and controls for banks and NBFCs. These Master Directions cover a wide range of subjects and provide comprehensive guidance for financial institutions and stakeholders.

What is the Purpose of the Master Directions by the RBI?

The Master Directions serve as a single reference point for regulatory matters. The RBI started issuing Master Directions in January 2016. Each of them focuses on a specific subject matter. These directions consolidate all relevant instructions, rules, and regulations related to that subject. They replace the existing set of Master Circulars issued on various subjects.

What does the Master Directions by the RBI cover?

The Master Directions cover a variety of regulatory matters, ensuring that all relevant guidelines are easily accessible to banks, financial institutions, and other stakeholders. Each Master Direction focuses on a specific subject matter, consolidating all relevant instructions. For instance, there are Master Directions related to banking, co-operative banking, commercial banking, and more.

What about the updates and changes of the Master Directions by the RBI?

Any changes in rules, regulations, or policies are communicated through circulars or press releases during the year. The Master Directions are updated accordingly and reflect the most current information. These are provided as FAQs (Frequently Asked Questions) in easy language in the circular released.

With the issuance of a Master Direction on banking regulation, the existing circulars related to the same are withdrawn automatically.

What are the baseline controls of the Master Directions?

The baseline controls of Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices revolves around the below areas:

1. IT Governance
2. IT Infrastructure and Service Management
3. IT & Information Security Risk Management
4. Business Continuity and Disaster Recovery Management
5. Information Systems (IS) Audit

When it comes to IT governance, there are several key focus areas that enterprises need to consider. Let us explore them:

Strategic Alignment: At the core of effective IT governance lies the strategic alignment of IT initiatives with the overarching business objectives. It focuses on ensuring that technological endeavors, investments, and innovations are synchronized with the organization's strategic vision.

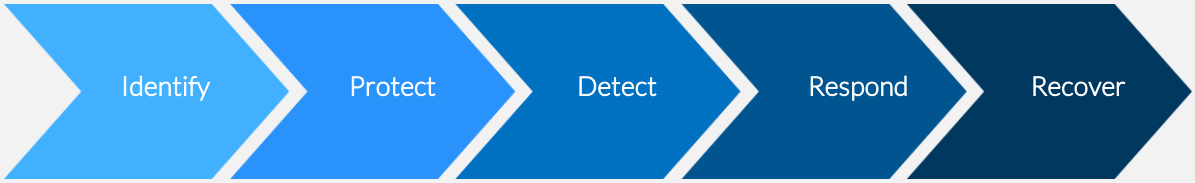
Risk Management: IT governance includes managing risks related to IT systems, data, and processes. Organizations must identify, assess, and mitigate IT-related risks to protect their assets and maintain operational continuity.

Resource Management: Effective resource management ensures that IT resources (including human resources, infrastructure, and budget) are managed effectively and appropriately. It involves optimizing resource allocation and utilization.

Business Continuity and Disaster Recovery: Ensuring business continuity during disruptions (such as natural disasters, cyberattacks, or system failures) is crucial. IT governance includes planning, testing, and implementing strategies for disaster recovery and continuity.

According to the RBI directive, "REs (regulated entities) shall put in place a robust IT Service Management Framework for supporting their information systems and infrastructure to ensure operational resilience of their entire IT environment.

Broadly, the directions ask IT security and compliance leaders to have the following mechanisms in place.

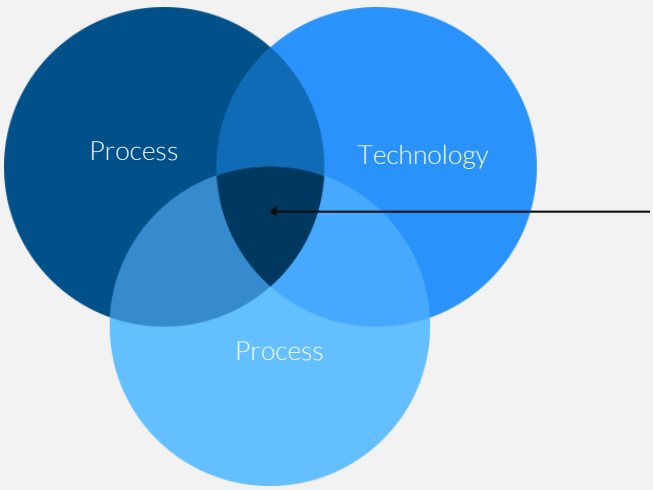


Managing People, Building Processes and Adopting Technologies

Typically, the three components- People, Process, and Technology - come into interplay when any enterprise looks to build a foundation for a strong and resilient IT infrastructure. When they work harmoniously, organizations gain efficiency and effectiveness.

- People refer to the individuals working in the organization that includes their skills, attitudes, and collaboration play a crucial role in achieving business goals.
- Processes represent the structured workflows, procedures, and methods used to accomplish tasks. By optimizing processes, organizations can streamline operations and achieve better outcomes.
- Technology encompasses the tools, systems, and software that are used to support business operations. Whether it is hardware, software, or digital platforms, technology enables automation, data analysis, and communication. Choosing the right technology for the right system with the right objective and integrating it effectively is essential for business continuity.

Managing people becomes challenging when it comes to multiple roles, multiple departments, and multiple systems where they are working. Baseline controls of the Master Directions by RBI help banks and NBFCs to manage people, build a process that these people need to follow and adopt technologies that adhere to the compliance policies.



In the diagram, the converged part (where the three components meet) is extremely important for enterprise security

In the above diagram, the area where people, process and technology converge is extremely important from an organisation's point of view. There are systematic and logical interdependencies of all the components among each other. In banks, the foundation of comprehensive security is built only when people follow the process, and the process is managed by robust technology. At the same time, it is not possible to implement technology without a well-defined process and the people following that process. Hence, banking organizations gain IT efficiency and stay compliant only when the components of people, process and technology are converged.

How does ARCON solutions help banks and NBFCs to Complying with the Reserve Bank of India (RBI) Master Directions?

Privileged Access Management (PAM) plays a pivotal role in ensuring compliance with the Reserve Bank of India (RBI) Master Directions. Let us delve into how ARCON | PAM and other ARCON solutions that help enterprise IT security, risk management and compliance leaders to comply with the RBI's Master Directive

- Mitigating Insider Threats and Third-Party Risks

ARCON's PAM solution assists organizations in proactively managing malicious insiders and third-party threats. By controlling privileged access, it helps prevent unauthorized actions and ensures that only authorized personnel can perform critical tasks.

- Robust Identity and Access Control Framework

PAM establishes a solid foundation for identity and access control. It allows or restricts commands based on servers, groups, or users, thereby enforcing granular permissions for privileged actions.

- Compliance with RBI Master Directions

RBI issues Master Directions covering various regulatory matters, including banking issues and foreign exchange transactions. PAM aligns with these guidelines by:

1) Audit trails: Capturing detailed logs of privileged activities.
2) Password management: Ensuring strong, regularly rotated passwords for privileged accounts.
3) Access Control: Access to information assets shall be allowed only where a valid business need exists.

The RBI Master Directions Checklist

While Chapter II (that covers directions 4-8) discusses IT governance around people and processes and its execution, Chapter III (that covers 9-21) and Chapter IV (that covers 22-27) of the RBI Master Directions is directed towards implementing technologies to combat information security related threats and cyber risks. In many of the directions, we believe Identity Access Management (IAM) solutions, especially Privileged Access Management (PAM), play a crucial role in complying with individual RBI directions. Here is a complete list and description of the RBI directions and how ARCON solutions help banks and NBFCs to mandate each one of them.

4 – IT Governance Framework

a) The key focus areas of IT Governance shall include strategic alignment, risk management, resource management, performance management and Business Continuity/ Disaster Recovery Management.

Solution

ARCON | PAM helps in governing identities and at the same time uses deep-learning threat detection techniques to assess the level of IT risks. It helps to manage privileged assignments, review them from time to time, allow secure privileged access, and ensure policy-based segregation of duties. As a result, business continuity/ disaster recovery management is ensured and maintained.

b) REs shall put in place a robust IT Governance Framework based on the aforementioned focus areas 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;

iii. Includes adequate oversight mechanisms to ensure accountability and mitigation of IT and cyber/ information security risks.

Solution

1. ARCON solutions offer Identity governance (IG) that helps organizations in ensuring that the right people have the right level of access to the right resources at the right time and comply with regulatory mandates at the same time.

2. Identity Governance includes the entire identity lifecycle, including identity creation, management, and deletion, as well as ongoing monitoring, review, and certification of access rights to ensure that they are appropriate and up to date.

3. Identity Governance also has a Challenge Phase where the user can view the asset details that the reviewer has preserved/revoked. In the case of revoked assets, the user will be able to challenge the reviewer by presenting a compelling reason for changing their review decision.

9 - IT Service Management

REs shall ensure identification and mapping of the security classification (in terms of Confidentiality, Integrity, and Availability) of information assets based on their criticality to the REs' operations.

Solution

The most important IT assets in any IT environment is privileged accounts. Unaccounted and dormant privileged accounts pose the biggest security threats. ARCON | Privileged Access Management (PAM) offers the most robust privileged account discovery engine. It searches and discovers all the privileged accounts in the underline privileged access environment and also scans all the assets that have privileged accounts.

ARCON | PAM offers strong integration with ARCON | EPM (Endpoint Privilege Management) which includes a powerful data-protection component/ feature known as Data Intellect. It builds a security cordon around data and builds a contextual security layer around the data. ARCON's Data Intellect enables the classification of data, itemization of the exposed data, categorization of the critical data, and proper understanding of the 'where' and 'what' of this enterprise data. Such insights on data are useful for forensic analysis and overall information security. With this, it allows banks and NBFCs to enforce data integrity, data confidentiality and data availability in the organizations.

10 – Third-party Arrangements

d) comply with applicable legal, regulatory requirements and standards to protect customer data

f) manage supply chain risks effectively.

Solution

d) In information technology, privileged Identities are more prone to misuse by third parties. Banking organizations and NBFCs face third-party threats due to access control vulnerabilities in the privileged access environment. ARCON | Privileged Access Management (PAM) offers a centralized platform that controls and manages privileged identities through multiple robust security features such as -

- MFA (Multi-factor Authentication)
- Credentials Management
- Granular-level access control
- Session Monitoring
- Just-In-Time (JIT) Privileges
- Audit Trails

f) Identities are key components for resilient supply chain. Whether normal identities, privileged identities or non-human identities, managing and governing all forms of identities are at the core of supply chain risk management. ARCON provides -

- An advanced identity governing engine for human, non-human and privileged identities
- Identity lifecycle management module for human, non-human and privileged identities
- Remove over-privileged identities on the cloud environment through Cloud Infrastructure and Entitlements Management (CIEM) solution – ARCON | Cloud Governance

15 – Audit Trails

a) Every IT application which can access or affect critical or sensitive information, shall have necessary audit and system logging capability, and should provide audit trails.

Solution

ARCON | PAM's robust reporting engine makes banks and NBFCs audit-ready by providing customized and detailed analytics of every privileged access to target systems. It helps them to make better IT privileged user decision making. It enables the auditors to assess the organization's regulatory compliance status at any given time.

b) The audit trails shall satisfy RE's business requirements apart from regulatory and legal requirements. The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes.

Solution

1. ARCON | PAM offers comprehensive security to all databases and applications as every command/query executed by end-users is captured through video/ text logs for a security assessment.

2. The reports generated provides a 360-degree view of security posture. These measures ensure better PAM decisions, build reputation, and prevent non-compliance risks.

c) REs shall put in place a system for regularly monitoring the audit trails and system logs to detect any unauthorized activity.

Solution

ARCON | PAM ensures that every privileged activity is monitored seamlessly with the help of robust session monitoring engine in real-time. It helps banks & NBFCs to detect and respond to security threats quickly and effectively. ARCON's Privileged Session Auditing proactively secures all databases and applications as every command/ query executed by end-users is captured for a security assessment to prevent unauthorized activities. This way, the Security and Risk Assessment team seamlessly manages the lifecycle of privileged accounts as every activity performed by privileged users is captured in both video and text format.

19 – Access Control

a) Access to information assets shall be allowed only where a valid business need exists. REs shall have documented standards and procedures, which are approved by the ITSC and kept up to date for administering need-based access to an information system.

Solution

ARCON offers unified admin console to manage entities, ensuring every access is happening to the target system/ application through authorization. It ensures that the access control framework is built around people and policies only on "need-to-know" and "need-to-do" basis. Hence, it helps the organization to build the foundation of robust identity and access management.

b) Personnel with elevated system access entitlements shall be closely supervised with all their systems' activities logged and periodically reviewed.

Solution

1. ARCON | PAM offers best-in-class access control features and functionalities to safeguard critical systems from insider and third-party threats.

2. An enterprise-class Unified Governing Platform offers the deepest level of granular controls and just-in-time privileged access to systems to ensure rule and role-based access to target systems.

3. With reporting mechanism, every access remains documented automatically through video/text format so that it can be reviewed sometimes.

c) REs shall adopt multi-factor authentication for privileged users of i) critical information systems and ii) for critical activities, basis the RE's risk assessment.

Solution

1. ARCON | PAM offers multi-factor authentication (MFA) that acts as a strategic entry point for system-based users. It ensures a robust user authentication mechanism to prevent unauthorized and suspicious access – both for on-prem and remote users.

2. It supports several MFA options, including ARCON Authenticator App, Email OTP, SMS OTP, hardware tokens, TOTPs like Google and Microsoft Authenticator, biometric authentication, Facial Recognition, and many more.

20 – Controls on Teleworking

a) Ensure that the systems used and the remote access from alternate work location to the environment hosting RE's information assets are secure

Solution

ARCON offers GRA (Global Remote Access) solution that allows IT administrators to establish a secure remote desktop connection and helps end-users control their own systems remotely from different locations. It provides the outside world with access to the inside infrastructure for maintenance and support in the most secure way.

b) Implement multi-factor authentication for enterprise access (logical) to critical systems

Solution

ARCON | Global Remote Access (GRA) allows the IT administrators to take control of the end-users' machines remotely and helps them to elevate admin rights, grant permissions, and change passwords, etc. This remote assistance mechanism removes the chances of unauthorized access and process delays in all end-user requirements. Indirectly, it authenticates remote users before allowing access to the critical systems or data assets.

d) Ensure that data/ information shared/ presented in teleworking is secured appropriately.

Solution

ARCON | GRA ensures safe transfer of files and critical data (requested by users) as the admin can accept/ reject the transfer process. This way data security and data privacy is maintained throughout.

25 – Risk Assessment

a) The risk assessment for each information asset within the RE's scope shall be guided by appropriate security standards/ IT control frameworks.

Solution

ARCON offers Security Compliance Management (SCM) solution that reviews and assesses risks automatically for compliance checks in banks and NBFCs. It streamlines the overall risk assessment process, providing organizations with comprehensive insights into their security posture. It effectively pinpoints critical areas that require attention and facilitates prioritization of remediation efforts. Being automated in nature, this "Risk Review" feature of SCM enhances efficiency, accuracy, and consistency in risk evaluation, empowering organizations to proactively address compliance irregularities and uphold a robust security stance.

b) REs shall ensure that all staff members and service providers comply with the extant information security and acceptable-use policies as applicable to them.

Solution

ARCON's Security Compliance Management (SCM solution encompasses a powerful array of features and functionalities specifically designed to manage and mitigate risks identified during the compliance assessment process. It goes beyond mere identification by implementing measures to tackle non-compliance issues, thereby fortifying the organization's security posture. It offers an extensive range of capabilities to bolster risk control, including remediation actions, establishment of standardized workflows, and ongoing monitoring to gauge the effectiveness of implemented security controls as applicable.

c) REs shall review their security infrastructure and security policies at least annually, factoring in their own experiences and emerging threats and risks. REs shall take steps to adequately tackle cyber-attacks including phishing, spoofing attacks and mitigate their adverse effects.

Solution

ARCON | SCM (Security Compliance Management) solution offers a unique "Policy Manager" features that serves as a dynamic and robust tool for establishing and enforcing standardized security policies throughout an organization's IT infrastructure. It empowers organizations to define security configurations and policies that align with industry best practices and regulatory requirements. With this, the IT administrators have the flexibility to create and personalize security baselines that cater to the specific needs of their organization, ensuring consistent and uniform security settings. This feature provides a centralized platform to efficiently manage and distribute these baselines to various assets and systems within the organization. Moreover, the IT administrators can effortlessly monitor compliance status, track deviations, and ensure policy adherence seamlessly with this.

Conclusion

ARCON | Privileged Access Management enables Indian banks and NBFCs to -

- Comply with the Reserve Bank of India (RBI) Master Directions
- Build a robust access control framework that demands the mandates of secure IT infrastructure in banking and financial industries
- Fulfil regulatory and audit requirements by capturing each end-user activity and generating reports whenever required to identify behavioral anomalies (if any)

about ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us