



Complying with the Reserve Bank of India (RBI) Guidelines on Cybersecurity Framework (User Access Control and Management) in Banks with ARCON | Privileged Access Management (PAM).

Table of Content

1. The Indian Banking Sector: A Key Pillar in the Nation's Development
2. Expanding IT ecosystems, and Inherent Technology Risks
3. What does the RBI circular on Cybersecurity Framework in Banks Mandate?
4. ARCON Privileged Access Management and RBI guidelines
5. The Checklist Tables - RBI guidelines
6. Conclusion

The Indian Banking Sector: A Key Pillar in the Nation's Development

As India continues to strengthen its banking system in the wake of rapid wave of digitalization, effective risk management and adapting to various economic dynamics, the banking industry is likely to play a key role in the nation's development. Furthermore, in the backdrop of macroeconomic stability, and positive operating environments, the nation is well positioned for a sustained economic growth outlook. As we update this paper in March 2024, the Indian banking industry shows immense potential to play a pivotal role in the broader APAC (Asia Pacific) banking landscape amid improving fundamentals.

Expanding Banking IT Ecosystems, and Inherent Technology Risks

In a much-interconnected system, mitigating risks emerging from technology adoption will be critical to preventing systemic risk. Indeed, in this digital era where banking organisations are increasingly exposed to IT threats and frauds, nothing is more challenging than maintaining strong information security and cyber security posture.

According to the Reserve Bank of India (RBI henceforth), as the use of technology by banks has gained further momentum, the number, frequency and impact of cyber incidents / attacks have increased manifold in the recent past, more so in the case of financial sector including banks, underlining the urgent need to put in place a robust cyber security/resilience framework at banks and to ensure adequate cyber-security preparedness among banks on a continuous basis.

Therefore, keeping this in mind, RBI mandates banks to enhance the resilience of the banking system by improving the current defenses in addressing cyber risks.

What Does the RBI circular on Cybersecurity Framework in Banks Mandate?

The RBI circular on cybersecurity framework is extremely broad and all encompassing. It includes adequate measures to prevent systemic risks arising from technological vulnerabilities. The guidelines mandate to have necessary controls around people, businesses processes, and technology interactions. According to the RBI Circular, banking organisations are expected to have the following security controls:

Baseline Controls

1. Inventory Management of Business IT Assets
2. Preventing Execution of Unauthorized Software
3. Environmental Control
4. Network Management and Security
5. Secure Configuration
6. Application Security Life Cycle
7. Patch and Vulnerability Change Management
8. User Access Control and Management
9. Authentication Framework for Customers
10. Secure mail and messaging systems
11. Vendor Risk Management
12. Removable Media
13. Advanced Real-Time Threat Defense and Management
14. Anti-phishing
15. Data-Leak Prevention Strategy
16. Maintenance, Monitoring, and Analysis of Audit Logs

17. Audit Log Settings
18. Vulnerability assessment and Penetration Test and Red Exam Exercises
19. Incident Response and Management
20. Risk based Transaction Monitoring Metrics
21. Forensics
22. User/Employee/Management Awareness
23. Customer Education and Awareness

ARCON Privileged Access Management – a comprehensive solution to comply with the RBI Guidelines on cybersecurity framework in banks (User Access Control and Management)



Every organisation is supposed to follow IT security regulations to enforce data privacy, integrity, and security. Complying with regulatory mandates becomes extremely easy if an organisation can build a security baseline with a robust access control posture as applicable. It enables an organisation to take control of the users to comply with the access control requirements and remain consistent with the regulatory standards. Towards this end, ARCON | Privileged Access Management plays crucial roles.



Identity management has been at the core of technology usage considering that there are now hundreds of applications and systems that one uses in their day-to-day operations, and this gets further complex with the interconnected technologies interacting with each other. While identity management is an issue, there are even more complex issues surrounding Privilege Identity Management. Privileged identities hold the keys to the applications and systems and have access to the heart of the various technologies.


ARCON | PAM is a Privilege Access Management Solution designed to address the challenges of privileged identities and provides an added layer of security to help build in controls that ensure access only on a "need-to-know" and "need-to-do" basis. The PAM solution has several components; and the major components are Access Control, Multifactor Authentication, Single Sign-On, Password Management, Audit Trails, and Session Monitoring. It enables IT security professionals to form impregnable perimeter security around IT systems, endpoints, and data whilst enabling them to develop a comprehensive Governance, Risks, and Compliance (GRC) framework.


Furthermore, ARCON | Privileged Access Management (PAM) comes with very solid integration with Endpoint Privilege Management (EPM). The EPM solution enables complying with RBI mandates requires Data Classification, Data Leak Prevention strategies which we have discussed below in the compliance mapping table.

RBI Guidelines- Baseline Controls- Point 8: User Access Control and Management and compliance with ARCON | PAM

RBI Statement	Compliance	ARCON Solution
<p>8.1 Provide secure access to the bank’s assets/services from within/outside bank’s network by protecting data/information at rest (e.g., using encryption, if supported by the device) and in-transit (e.g., using technologies such as VPN or other secure web protocols, etc.)</p>		<p>Data at Rest</p> <p>ARCON Vault, a critical component of PAM, holds critical information; the Vault sits deep within the database. The Vault is not a single component, i.e., it has multiple components that interact internally, and all such components are scrambled. This dramatically reduces the attack vector, as all the components must be compromised to create a single view. The data within all these components and objects is encrypted using FIPS 140-2-compliant encryption. ARCON Vault uses a layered encryption approach; in fact, there are two levels of encryption for critical elements. At the first level, ARCON Vault uses the AES-256 symmetric algorithm, and at level two, ARCON uses its proprietary encryption algorithm.</p> <p>Data in Transit</p> <p>ARCON Vault encrypts all critical data in transit. The Vault uses a TLS 1.2-compliant communication layer between systems. This is further enhanced as the data flow between the end devices is through the proprietary encrypted tunnel up to the Secured Gateway or on HTTPS. The methodology adopted significantly reduces the attack vector, especially around wiretapping or packet sniffing over the network. While an attacker inside the network may be able to see traffic between systems, the data will be indecipherable and thus useless.</p>
<p>8.3 Disallow administrative rights on end-user workstations /PCs /laptops and provide access rights on a need-to-know basis and for specific duration when it is required following an established process.</p>		<p>Authorization- One Admin Control</p> <p>Regardless of the size of banking organisation's IT infrastructure, every access to critical systems is made through one ADMIN console- an authorization engine. The secure gateway server provides a centralized control point through which all network connections and traffic is routed for management and monitoring. Unified admin console to manage entities and access the target systems/applications. Authorization ensures the</p>

		<p>implementation of an access control framework around people and policies. This way, privileged access is granted only on a “need-to-know” and “need to-do” basis, the foundation for robust identity and access control management.</p>
<p>8.4 Implement centralized authentication and authorization system or accessing and administering applications, operating systems, databases, network, and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties.</p>		<p>In the above column we have explained how One Admin Console allows security leaders to enforce authorization-centralized administration of users having privileged access to systems.</p> <p>Password Vault</p> <ul style="list-style-type: none"> ▪ Furthermore, ARCON PAM suite offers a strong password management engine- the Password Vault. This engine allows security leaders to vault and randomize passwords for privileged users. The tool allows us to enforce strong password management policy as well. The strength and number of characters can be pre-defined by PAM administrators as per the organisation policy. <p>Multifactor Authentication</p> <ul style="list-style-type: none"> ▪ The solution comes with built-in Two Factor Authentication and seamlessly integrates with third party authentication tools to provide added validation layers - Multi Factor Authentication (MFA). ▪ ARCON PAM offers the most granular access control through Access Control feature which controls and restricts users access based on roles and responsibilities including commands fired. Access Control enforces the least privilege principle.
<p>8.5 Implement appropriate (e.g., centralized) systems and controls to allow, manage, log, and monitor privileged/superuser/administrative access to critical systems (Servers/OS/DB, applications, network devices etc.).</p>		<p>ARCON PAM suite</p> <p>ARCON Privileged Access Management offers comprehensive capabilities to meet all necessary needs for ensuring a safe and secure Privileged Access environment. The solution offers a unified engine to control users’ privileged access based on ‘need-to-know’ and ‘need-to-do basis’ principle.</p> <p>An admin can restrict/control privileged users’ access to systems based on pre-defined roles and responsibilities with Access Control component.</p>

		<p>The solution’s other key components such as Session Management and Session Monitoring enforce tight control over privileged sessions while Text and Video logs provide complete visibility over Privileged Sessions.</p>
<p>8.6 Implement controls to minimize invalid logon counts, deactivate dormant accounts.</p>		<p>Discovery</p> <p>One of the major risks in privileged access environment stems from unaccounted Privileged Ids and assets. If left unaccounted and dormant, compromised insiders can misuse confidential data. To overcome this challenge, ARCON PAM offers the best-in-class discovery module. It scans the entire PAM environment and discovers all Privileged IDs and assets under the IT network. Thus, the timely discovery of all critical assets and privileged Ids ensures there are no invalid logon accounts, and if there are, an admin can quickly deactivate such accounts.</p>
<p>8.7 Monitor any abnormal change in pattern of logon.</p>		<p>Identity Threat Detection and Response (ITDR) and Adaptive Authentication</p> <p>ITDR- (knight Analytics) can be embedded with ARCON PAM. The system is designed to create risk scores for individual users from AI-based analytics on which future privileged access decisions can be made. Risky privileged entitlements ideally require both role and rule-based control over users. As soon as the tool clusters data on risky behavior profiles and users’ anomalies, AI driven analytics kick in to generate a risk score based on the historical data of users. By analyzing data in real-time privileged access management decisions are adaptive and less dependent on fixed rules.</p> <p>Likewise, adaptive Multi Authentication offered by ARCON PAM learns users log on patterns based on their past usage base, using data items like MAC Address, IP address, geo-location, typing speed etc. to determine whether the user login is happening from a known environment or not.</p>
<p>8.8 Implement measures to control installation of software on PCs/laptops, etc.</p>		<p>Endpoint Privilege Management (EPM)</p> <p>ARCON EPM solution restricts applications that pose significant risks by classifying applications based on risk levels associated with them. Application Restrictions helps to secure all the endpoints in the network by blacklisting and whitelisting applications. This way suspicious/ unauthorized installations are prevented seamlessly.</p>

<p>8.9 Implement controls for remote management/wiping /locking of mobile devices including laptops, etc.</p>		<p>Global Remote Access (GRA)</p> <p>ARCON GRA provides the outside world with access to the inside infrastructure for maintenance and support in the most secure way without the hassles of implementing VPNs or any additional installations. This solution provides third-party access to the IT infrastructure of a client in a secure manner by allowing the IT administrators to take control of the end-users' machines remotely and helps them to elevate admin rights, grant permissions, and change passwords, and other critical tasks. This remote assistance mechanism removes the chances of process delays in all end-user requirements.</p>
--	---	--

Furthermore, ARCON | EPM’s Data Intellect allows banking organisations to classify data.

Data Intellect, a component of EPM, is a robust endpoint data-centric security tool built on AI/ML driven context-aware models, and it enables the discovery, classification, and categorization of large volumes of unstructured enterprise data and helps orchestrate remedial steps to control access to data while improving compliance posture at the same time.

Conclusion

ARCON | Privileged Access Management (PAM) -

- Helps to comply with the RBI mandates and compliance guidelines (User Access Control and Management)
- Authorizes and authenticates users before allowing access to critical applications
- Builds a stringent rule and role-based access control framework
- Analyzes and categorizes access permissions and restrictions
- Mitigates the chances of data breach incidents and credential abuse

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    

All rights reserved by ARCON

This document or any part of the document may not be reproduced, distributed or published in any form without the written consent of the copyright owner under any circumstances. Any kind of infringement in the owner's exclusive rights will be considered unlawful and might be subject to penalties.