The Reserve Bank of India (RBI) Circular on Information Security

A mandate to toughen the privileged access security

Introduction

The banking industry is always a lucrative target for cyber criminals who are constantly in search of highly confidential information. National, multi-national and private banks from India and across the globe, time and again, have fallen prey to devastating cyber-attacks amid increasing pace of digitization. Many of them have been badly affected due to inadequate IT security safeguards and lack of oversight and governance.

Consequently, banking organizations felt the need for a robust security posture to mitigate emerging IT threats such as insiders' threats and third-party risks to confidential IT assets. IT heads from several banking organizations subsequently raised concerns with the Reserve Bank of India (RB, which in turn realized an urgent requirement to shore up Information Security.

The central bank came up with a control and prevention measures in its series of circulars. The RBI issued a set of stringent cyber security guidelines to help banks mitigate IT threats. The organization has even collected ample evidence, feedback, and opinions from various banks including financial institutions to identify the security risk areas and accordingly framed guidelines to secure the IT infrastructure of the banks. As per the circular, RBI has also added that IT operations team and IT security team has to have two separate entities so that the IT security factor receives exclusivity and better management.

The RBI mandates these safeguards

End to End data protection of customer data

Advanced real-time threat detection

User access control & management

Vulnerability assessments and seamless monitoring of user activities

Extra focus on extended network in shared environment

These security measures essentially demands to reinforce privileged identities as these are the most sought after target of malefactors. These are highly-elevated administrative IDs that have permission to access critical systems and highly sensitive data. Thus the security of privileged access/ identities is the core to overall IT security framework.

arcon

The Privileged Access challenge

Digitization in the banking industry created efficiency and convenience for both the customers and IT operations staff. However, new security challenges also started to emerge as the banks adopted modern technologies such as Big Data Analytics and Cloud Computing. With critical systems, database servers and applications increasing at a rapid pace, the number of IT users to maintain these systems also started to increase. Elevated privileges--privileged identities authorized to administer IT systems, root accounts, network devices, databases and applications also soared. These identities due to the intrinsic prominence in the whole IT fabric became a focal point from security perspective.

Subsequently, it became an enormous challenge for the risk management team to ensure security for multiple privileged accounts spread across shared and distributed IT environments. No matter how strong peripheral defenses a bank might maintain in its data center, the security posture is on a thin ice if a single privileged user misuses privileged credential. Attacks on privileged accounts has the capacity to bring down the entire IT infrastructure. Adding to the woes, there is always a high threat potential if the privileged accounts are shared among partners or third party users where monitoring their real-time privileged activities is extremely crucial wherein organizations need to know who all have accessed certain privileged accounts and for what purpose.

Further, an ever-increasing volume of sensitive financial database is pushing banking organizations to opt for the cloud-based infrastructure which enables them to quickly scale up (or down) storage and data processing capacity as per the requirements. The flexibility of cloud storage allows banks to choose where they wish to run their systems. However, it invites some grave security risks. Information Security remains a concern as weak access controls, inadequate authentication mechanism in the IaaS environment could inflict heavy damage.

Secure data and workloads migration to IaaS platform requires real-time monitoring, strong access mechanism procedure for mitigating risky privileged activities around databases and applications.

The Mistakes leading to Privileged Access Misuse

- Lack of IT governing framework
- Absence of real-time end-user monitoring
- Inadequate authentication mechanism
- Absence of privileged credentials management (no randomization and vaulting of passwords)
- Absence of fine-grained control over privileged users (absence of principle of least privilege)
- Absence of reporting on privileged activities

How ARCON Privileged Access Management solution do ensures robust privileged access security?

ARCON | Privileged Access Management suite (PAM) is a powerful solution to mitigate malicious insiders' and third-party threats to privileged accounts. The tool enables the IT Security and Compliance management officers to nurture best privileged access management practices, which is the stepping stone to build a robust identity & access control framework. The solution provides a secure gateway to target devices ensuring privileged entitlements are never compromised through role and rule based access control framework.

This enterprise-wide highly scalable solution seamlessly controls and restricts privileged users' access with the help of granular level access control and bifurcates IT groups/ privileged users according to their roles, functions, and departments, ensuring access is strictly based on 'need-to-know' and 'need-to-do' principle.

ARCON PAM seamlessly monitors each and every privileged session in real-time. The Session monitoring enables the IT security staff to keep a tab on all live sessions and immediately suspend suspicious privileged sessions.

Further, in order to validate every privileged access to critical systems, ARCON | PAM offers Multi-factor Authentication (MFA). The solution offers in-built dual factor authentication and seamlessly integrates with third-party authorization tools.
The Password Vault creates another crucial layer of security by helping the IT security team to frequently randomize and change passwords. Moreover, the Audit Trails feature keeps bank's IT administrators audit and compliance ready as the solution provides a detailed report of all the privileged sessions at any given date and time. This robust tool captures all logs in both text and video formats.

More than 50 banks across the globe trusted on ARCON | Privileged Access Management (PAM) to secure their privileged accounts from unauthorized access and malicious users.

Global Banks Trust ARCON | PAM Capabilities

We protect privileged accounts of
50+ Banks

Nationalized
Banks: 26 **Private Banks: 8** **Foreign Banks: 18+**

No of Geographical Regions - 4
India, South East Asia, Middle East, Africa, APAC

No of countries **10+**

No of Privileged Identities Protected **10,000+**

How ARCON PAM helps complying with the RBI Guidelines

Sl No.	RBI Guideline	What it implies	How ARCON | PAM can contribute
1	**End-to-end protection of customer data**	▪ Any customer data which is prepared and stored in servers, a systems should remain unchanged even if access to that data is after a long period of time. In other words, data privacy, data sanctity should be maintained. ▪ The functional responsibilities should also be restricted. For example, if an end-user is entitled to read a document then he/she should not be having editing rights. Any kind of violations should be brought under notice.	▪ ARCON | PAM solution ensures end-to-end protection of customer data with the help of deepest levels of granular control over critical information ▪ It offers an ability to restrict commands based on server wise/ group wise/ user wise ▪ Controls Read/ Write/ Execute permission for commands fired by users on SSH interface ▪ Segregates IT end-users based on job and responsibility profiles so that no unauthorized access is made to critical systems
2	**Advanced real-time threat detection**	▪ Malicious insiders and compromised third-party elements can misuse trusted privileges to steal confidential data ▪ Thus it is imperative to continuously detect any sort of anomaly and suspicious privileged sessions	▪ ARCON | PAM's session monitoring and session recording helps the administrator to keep an oversight on all privileged activities
3	**User Access Control & Management**	▪ Secure access to databases, applications, VMs, network devices, root accounts, administrative accounts ▪ There is always a risk of compromising systems and data if privileged credentials are managed and shared manually ▪ Segregation of roles and responsibilities ▪ Robust password management ▪ Strong authorization mechanism	▪ The password vault automates password management ▪ The vault randomizes and generates dynamic privileged passwords in frequent intervals ▪ It offers multi-factor authorization to ensure secure access to applications, databases, cloud resources, Big Data, VM instances ▪ Virtual grouping enables mapping of multiple users to devices ▪ Granular access control and command filtering capabilities helps implementing 'least privileges' 'maker-checker' and 'need-to-know' and 'need-to-do' principles

How ARCON PAM helps complying with the RBI Guidelines

Sl No.	RBI Guideline	What it implies	How ARCON | PAM can contribute
4	**Vulnerability assessment and seamless monitoring of user activities**	▪ An assessment of vulnerable areas in the enterprise network that can bring harm to the critical data ▪ Thereby continuously monitoring the activities of privileged users.	▪ ARCON | PAM reinforces enterprise security with real-time threat analytics to spot suspicious activities and stop data breach before it strikes ▪ Central logging and monitoring ensures all logs are captured both in video and text formats for forensic analysis
5	**Extra focus on extended network in shared environment**	▪ In addition to on-prem data center security, a robust network security requires foolproof privileged access control for network devices (firewalls, routers, switches) operating systems root accounts, applications, databases hosted in shared data center environments ▪ Data shared in hosted environments such as Managed Services should have access in controlled environment	▪ ARCON | Privileged Access Management serves as policy engines to manage and govern all privileged identities underlying in an IT environment ▪ Role and rule based privileged entitlements ensure every access to critical system is authorized and validated

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