To control the increasing information security related threats in the securities market, SEBI Regulated Entities (REs) are advised to implement the Annexure-A. Learn how ARCON's highly mature Privileged Access Management solution can help the Security and Risk Management leaders to comply with the SEBI Mandates.

Table of Content

Cyber Ecosystem in Securities companies

Securities companies, also known as brokerage firms or investment dealers, are financial institutions that facilitate the buying and selling of financial securities, such as stocks, bonds, and other investment products. They play a crucial role in the financial markets by connecting buyers and sellers, providing investment advice, and managing investment portfolios.

The IT environment in securities companies is complex and dynamic. It includes a vast amount of sensitive data that needs to be protected. Security leaders need to ensure that integrity of trading systems is maintained. Here are some key components and trends within this ecosystem:

- **Advanced Threat Detection:** Securities companies are investing in sophisticated threat detection systems that use artificial intelligence (AI) and machine learning (ML) to identify and respond to potential cyber threats in real-time.
- **Zero Trust Architecture:** This security model assumes that threats can come from both inside and outside the network. It requires strict verification of every user and device trying to access resources, minimizing the risk of unauthorized access.
- **Behavioral Analytics:** By analyzing user behavior, securities companies can detect unusual activities that may indicate a security breach. This proactive approach helps in identifying and mitigating threats before they cause significant damage.
- **Third-Party Risk Management:** With the increasing reliance on third-party vendors, managing the cybersecurity risks associated with these partners is crucial. This involves thorough vetting and continuous monitoring of third-party security practices.
- **Regulatory Compliance:** Securities companies must comply with various regulations and standards, such as the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), and the RBI Master Directions Compliance. Ensuring compliance helps in maintaining trust and avoiding legal penalties.

These components work together to create a resilient cyber ecosystem that can adapt to evolving threats and protect the critical infrastructure of securities companies.

What is SEBI?

The Securities and Exchange Board of India (SEBI) is the primary regulatory authority for the securities and commodity markets in India. Established in 1988 and given statutory powers in 1992, SEBI's main objectives are to protect the interests of investors, promote the development of the securities market, and regulate its functioning.
The roles and responsibilities of SEBI include:

- Regulating Stock Exchanges: Ensuring fair practices and transparency in the stock markets.
- Protecting Investors: Implementing measures to safeguard investors' interests and investments.
- Promoting and Regulating Self-Regulatory Organizations: Overseeing entities that regulate their own members.
- Prohibiting Insider Trading: Preventing unfair practices like insider trading.
- Conducting Investigations and Enforcing Regulations: Investigating violations and enforcing compliance with securities laws.

SEBI operates under the administrative control of the Ministry of Finance and has its headquarters in Mumbai, with regional offices across India.

SEBI is meant for whom?

The regulatory authority of SEBI (Securities and Exchange Board of India) serves multiple stakeholders in the securities market:

- **Investors:** SEBI protects the interests of investors by ensuring fair practices and transparency in the securities market. This helps investors make informed decisions and safeguards them from fraudulent activities.
- **Issuers:** Companies that issue securities (like stocks and bonds) benefit from SEBI's regulations, which ensure that they can raise capital in a fair and efficient manner.
- **Intermediaries:** This includes brokers, mutual funds, and other market participants who facilitate trading and investment. SEBI regulates these intermediaries to ensure they operate in a fair and transparent manner.
- **Stock Exchanges:** SEBI oversees stock exchanges to ensure they function smoothly and maintain market integrity.
- **General Public:** By maintaining a stable and transparent market, SEBI indirectly benefits the public by contributing to overall economic growth and stability.

SEBI's regulations and oversight help create a secure and efficient market environment for all these stakeholders.

What are the core objectives of SEBI regulatory compliance?

The core objectives of SEBI (Securities and Exchange Board of India) regulatory compliance are designed to ensure the smooth functioning and integrity of the securities market. Here are the core objectives:

- **Protecting Investors:** SEBI aims to safeguard the interests of investors by ensuring they have access to accurate and timely information, and by preventing fraudulent and unfair practices.
- **Ensuring Fair and Transparent Markets:** SEBI works to maintain fair, efficient, and transparent markets. This involves regulating market intermediaries, stock exchanges, and other participants to ensure they adhere to established standards and practices.
- **Reducing Systemic Risk:** By implementing robust regulatory frameworks and monitoring market activities, SEBI aims to reduce systemic risks that could lead to market instability.
- **Promoting Market Development:** SEBI encourages the development of the securities market by introducing new products, improving market infrastructure, and fostering innovation3.
- **Preventing Malpractices:** SEBI actively works to prevent malpractices such as insider trading, market manipulation, and other fraudulent activities that can harm the market and investors.

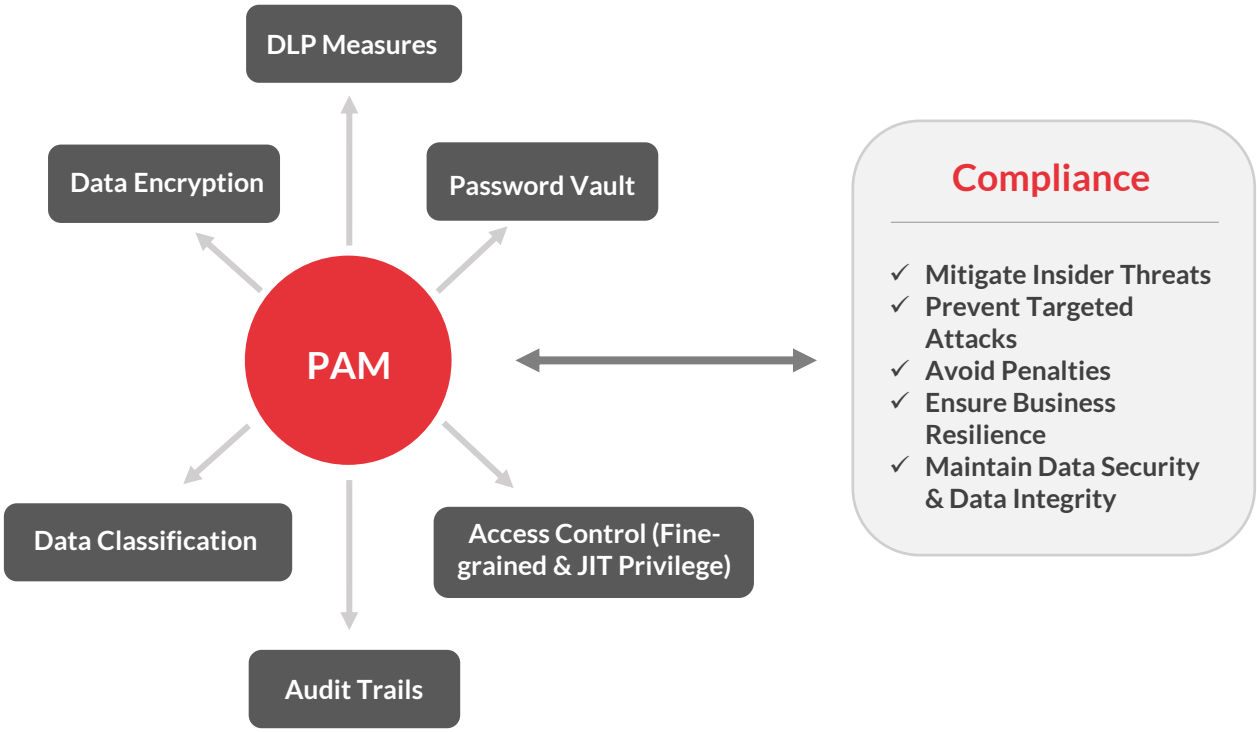
How can Privileged Access Management (PAM) help organizations to comply with SEBI mandates?

Privileged Access Management (PAM) plays a crucial role in ensuring compliance with the Securities and Exchange Board of India (SEBI) regulations. Here are some key points on how PAM contributes to SEBI compliance:

- **Enhanced Security:** PAM helps in securing privileged accounts, which are often targeted by cybercriminals. By managing and monitoring these accounts, organizations can prevent unauthorized access and potential data breaches.
- **Access Control:** SEBI regulations require strict control over who can access sensitive information. PAM enforces the principle of least privilege, ensuring that users only have access to the information necessary for their roles.

arcon

- **Audit and Monitoring:** PAM solutions provide detailed logs and audit trails of all activities performed using privileged accounts. This is essential for demonstrating compliance during SEBI audits and for investigating any suspicious activities.
- **Policy Enforcement:** PAM helps in enforcing security policies related to privileged access. This includes password management, session monitoring, and real-time threat detection, which are critical for maintaining compliance with SEBI guidelines.
- **Risk Management:** By implementing PAM, organizations can identify and mitigate risks associated with privileged access. This proactive approach helps in maintaining a secure environment and adhering to SEBI's risk management requirements.



SEBI Checklist and Role of ARCON Solutions

In this compliance mapping paper, we have discussed SEBI's Annexure – A circular in the below table and how ARCON's PAM solution along with several other access control solutions such as My Vault, Endpoint Privilege Management (EPM), Data Intellect- that are tightly integrated with PAM can help SEBI stakeholders of India to comply with the mandates.

Recommendations of SEBI Annexure - A	Does ARCON | PAM comply?	Which ARCON solution and its feature addresses it?
4. Measures for Data Protection and Data breach: ii. Enforce effective data protection, backup, and recovery measures. iii. Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data. iv. Identify and classify sensitive and Personally Identifiable Information (PII) data and apply measures for encrypting such data in transit and at rest. v. Deploy data leakage prevention (DLP) solutions / processes.	✔	▪ ARCON's My Vault solution offers a centralized repository to store, access and share all sorts of critical business information in a secure manner. ▪ The files where this information is stored remain encrypted and can be deleted easily after a preset time to avoid any unauthorized access. It also controls the end-users' activities based on the pre-configured permissions even at a granular level. ▪ ARCON My Vault can give certain privileges with regards to download, share, transfer of files/folders or access permissions that minimizes risks of data misuse. ▪ Data Intellect, a critical component of Endpoint Privilege Management (EPM), and integrated with ARCON | PAM, builds an impenetrable circumference around data and builds a contextual security layer around the data. It enables the classification of data, itemization of the exposed data, categorization of the critical data, and understanding of the 'where' and 'what' of data. ▪ ARCON | Endpoint Privilege Management (EPM) solutions DLP feature that helps mitigating security vulnerabilities by restricting mobile devices or even mobile Bluetooth connections and Bluetooth transfers. It also offers USB restriction feature that ensures copying of any sort of information/file/folder from the endpoint to USB and vice versa cannot be carried out.

Password Policy/ Authentication Mechanisms: i. Strong password policy should be implemented. The policy should include a clause for periodic review of the accounts of ex-employees. Passwords should not be reused across multiple accounts, or a list of passwords should not be stored on the system. ii. Enable multi-factor authentication (MFA) for all users that connect using online/internet facilities and for virtual private networks, webmail and accounts that access critical systems. iii. Maker and Checker framework should be implemented in a strict manner and MFA should be enabled for all user accounts, especially for user accounts accessing critical applications.		▪ ARCON's Privileged Access Management (PAM) solution offers "password vaulting" feature that ensures every password is stored and managed in a highly secure environment by providing a secure and single point of control. ▪ Such credential vaulting eliminates the need for privileged users to remember and share passwords, thus lowering the risk of password theft and misuse. ▪ It also provides an audit trail of all privileged account password access, including who accessed the password, when, and for what purpose, thereby improving the overall security posture of the organization. ▪ ARCON PAM offers Multi-Factor Authentication (MFA) that acts as a strategic, relevant, and essential engine to provide multiple forms of identity verification steps before the privileged users are allowed access to the desired network, system, or application. Along with the traditional verification methods such as SMS and Email OTP mechanisms and hardware tokens, ARCON's MFA provides integration with various third-party authentication apps, including disparate biometric and facial recognition technologies. ▪ ARCON | PAM's Granular access control and command filtering capabilities helps organizations to implement 'maker-checker' and 'need-to-know' and 'need-to-do' principles.
7. Privilege Management: i. Maker-Checker framework should be implemented for modifying the user's right in internal applications. ii. For mitigating the insider threat problem, 'least privilege' approach to provide security for both on-and off-premises resources (i.e., zero-trust models) should 7 be implemented. Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for every resource and		▪ ARCON | PAM the Maker-Checker concept is applied to manage and control access to sensitive systems and data. It ensures that any changes to security settings, access permissions, or configurations are reviewed and approved by a second individual. This helps prevent unauthorized changes and ensures that security measures are consistently applied. ▪ ARCON offers a robust access control module that ensures the deepest level of granular control. It includes – i) Fine-grained access control (Admins can control exactly which users have access to which services and resources); ii) Process and Command Restriction (Admins can restrict or elevate specific processes or commands that can be executed);

device trying to access any information on a private network, regardless of where they are situated, within or outside of a network perimeter.		iii) Critical Command Approval (Privileged user requires that certain commands be approved by the admin before they can be executed) and iv) Reporting (Admins can generate reports on the privileged user activities and access control events) ▪ ARCON | PAM also offers the principle of "least privileges" can be implemented with ARCON's Just-In-Time (JIT) privilege capabilities. It ensures that the right person has access to the right systems at the right time. 24*7 or "always on" privileges are too risky. ▪ The Zero Trust security approach of ARCON | PAM is based on the principle of "Deny Access" unless the trust is verified at every step. It helps organizations to follow the principles of Zero Trust security with the help of several advanced features such as Just-In-Time (JIT) approach, Multi-factor Authentication (MFA), Adaptive Authentication, Identity Governance and Administration (IGA) that build the foundation of a zero-trust security posture.

Conclusion

Multiple ARCON solutions help the stakeholders of SEBI to –

- Prevent unauthorized access and potential data breaches
- Ensure authorized access to the right information at right time for right reasons
- Build the foundation of security policies across the IT infrastructure
- Maintain a secure environment adhering to SEBI's risk management requirements and meet compliance

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