

Addressing The Requirements of Cybersecurity and Cyber Resilience Framework (CSCRF) by SEBI

To enhance the current cybersecurity measures in the Indian securities market and strengthen the mechanism for dealing with cyber risks or threats, the Securities and Exchange Board of India (SEBI) released the [Cybersecurity and Cyber Resilience Framework \(CSCRF\)](#) to SEBI-regulated entities (REs) on August 20th, 2024. The CSCRF framework shall supersede existing SEBI cybersecurity circulars/ guidelines/ advisories/ letters.

The Cybersecurity and Cyber Resilience Framework (CSCRF) aims to provide standards and guidelines for strengthening cyber resilience and maintaining robust cybersecurity of SEBI REs.

Approach and Structure

The CSCRF is standards-based and broadly covers the five cyber resiliency goals adopted from the Cyber Crisis Management Plan (CCMP) of the Indian Computer Emergency Response Team (CERT-In): **Anticipate, Withstand, Contain, Recover, and Evolve**.

These cyber resiliency goals have been linked with the following cybersecurity functions: **Governance, Identify, Protect, Detect, Respond, and Recover**.

Figure 1: CSCRF Overview

	Cyber Resilience Goal: Evolve						
Cyber Resilience Goal	Anticipate				Withstand & contain		Recover
Cybersecurity Function	Governance	Identify	Protect	Detect	Respond		Recover

The CSCRF is structured into four parts:

- Part I: Objectives and Standards
- Part II: Guidelines
- Part III: Structured formats for compliance
- Part IV: Annexures and References

<p>Regulated Entities:</p> <ol style="list-style-type: none"> 1. Alternative Investment Funds (AIFs) 2. Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs) 3. Clearing Corporations 4. Collective Investment Schemes (CIS) 5. Credit Rating Agencies (CRAs) 6. Custodians 7. Debenture Trustees (DTs) 8. Depositories 9. Designated Depository Participants (DDPs) 10. Depository Participants through Depositories 11. Investment Advisors (IAs)/ Research Analysts (RAs) 12. KYC Registration Agencies (KRAs) 13. Merchant Bankers (MBs) 14. Mutual Funds (MFs)/ Asset Management Companies (AMCs) 	<p>15. Portfolio Managers</p> <p>16. Registrar to an Issue and Share Transfer Agents (RTAs)</p> <ol style="list-style-type: none"> 17. Stock Brokers through Exchanges 18. Stock Exchanges 19. Venture Capital Funds (VCFs) <p>REs Categories</p> <ul style="list-style-type: none"> • Market Infrastructure Institutions (MIIs) • Qualified REs • Mid-size REs • Small-size REs • Self-certification REs
---	--

Scope

The framework shall apply to the following REs and also further sub classifies the REs into the following categories based on their operational scale, number of clients, trade volume, and assets under management, and provides for specific compliance requirements for each category:

Timeline for implementing CSCRf

- For REs where cybersecurity and cyber resilience circular already exists – by January 01, 2025.
- For other REs where CSCRf is being issued for the first time – by April 01, 2025.

How does Thales Helps with CSCRf?

Thales can help REs comply with CSCRf by addressing cybersecurity function guidelines of Governance, Identity and Protect in the framework. We provide solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.
















Standard Code & Guidelines	Thales Solutions
<p>GV.PO - 1.3.ii. Policy</p> <p>5. Clear definition of ownership, custodian of every asset and a proper chain of command</p> <p>S1, S2, S5</p> <p>5. “REs shall have policies (including but not limited to) with respect to asset management, ...authentication policies, ... encryption policies...”</p> <p>6a. ‘Identify’ critical IT assets and risks associated with such assets.</p>	<p>SafeNet Authentication Service Private Cloud Edition (PCE) is an on-premises authentication platform that makes authentication easy and cost-effective to implement and manage. It safeguards global infrastructure access points with over 200 out-of-the-box pre-tested configurations, including VPN, SSL VPN, IAM, SaaS, and VDI solutions. It supports third-party solutions via SAML, RADIUS, Agents, or APIs and offers diverse token types.</p> <p>CipherTrust Data Discovery & Classification (DDC) discovers and classifies data in all the data stores in an organization’s data estate, from structured to semi-structured to unstructured across on-premises, hybrid, cloud, and multi-cloud environments. This visibility enables organizations to build a strong data privacy and security foundation by managing assets.</p> <p>Imperva Data Security Fabric Data Activity Monitoring (DAM) allows organizations to identify risks associated with critical data. DAM captures and analyzes all data store activity by continuous monitoring in the cloud or on-premises for both application and privileged user accounts, providing detailed audit trails that show who accessed what data, when, and what was done to the data.</p>
<p>ID.AM - 2.1.ii. Asset Management</p> <p>1. Physical devices, digital assets (such as URLs, domain names, applications, APIs, etc.), shared resources (including cloud assets) and other interfacing systems within the organization are inventoried...</p> <p>2. Organizational communication, data flows and encryption methods shall be mapped and inventoried ...</p> <p>S1, S4</p> <p>4.a. Maintain a comprehensive asset inventory...</p>	<p>Imperva Data Security Fabric Data Activity Monitoring (DAM) unifies auditing across diverse on-premises platforms, providing oversight for relational databases, NoSQL databases, mainframes, big data platforms, and data warehouses. It also supports databases hosted in Microsoft Azure and Amazon Web Services (AWS), including PaaS offerings such as Azure SQL and Amazon Relational Database Services (RDS). Detailed data activity is captured automatically, making it easier to fulfill audit requests and maintain a comprehensive asset inventory.</p>

Standard Code & Guidelines	Thales Solutions
<p>ID.RA - 2.2.ii. Risk Assessment</p> <p>5. Cybersecurity and Quantum Computing...</p> <p>4. ...feasibility to adopt PQC and technologies like Quantum Key Distribution (QKD)...</p> <p>S1, S2</p> <p>1. “REs shall conduct a risk assessment (including post-quantum risks)...”</p>	<p>Thales Luna HSMs and High-speed Encryptors provide a crypto-agile approach to ensure PQC readiness for REs.</p> <ul style="list-style-type: none"> Fortify your encryption keys with Quantum-safe Thales Luna HSM which is commercially available with NIST quantum-resistant finalist algorithms added. <ul style="list-style-type: none"> Quantum-Resistant Algorithms (QRA) with PQC FM with Hash Based Signing (SP800-208) Integrated/ Custom-made PQC: Implement your own Post- Quantum Crypto using Luna’s Functionality Module (FM) or with various Partner FMs/ integrations QRNG: Inject quantum entropy with QRNG and Luna HSM’s secure key storage Secure Data in Transit with Thales High Speed Encryption (HSE) network encryption solutions that support Post-Quantum Cryptography (PQC) with a crypto-agile, FPGA-based architecture. HSE is the first commercially available quantum-resistant network encryption solution, providing REs with long-term data protection today against future quantum attacks. It offers REs a single platform to encrypt everywhere – from network traffic between data centers and headquarters to backup and disaster recovery sites, whether on-premises or in the cloud. <p>PQC starter kit allows REs to develop and build capabilities to test quantum-safe solutions safely. Thales PQC starter kit that partners with Quantinuum accelerates the process of testing quantum resilient measures in a safe environment. The kit helps you set up a trusted environment in a trusted Luna HSM to test PQC-ready keys to understand the implications of these changes for your infrastructure without impacting key management processes in production environments.</p>
<p>ID.RA - 2.2.ii. Risk Assessment</p> <p>3. Threats, vulnerabilities, their likelihoods, and impacts shall be used to understand inherent risk and develop risk response prioritization...</p> <p>S4</p> <p>1. “Measures against Phishing websites and attacks...”</p>	<p>Imperva Web Application Firewall (WAF) provides out-of-the-box security for web applications, detecting and preventing cyber threats, ensuring seamless operations and peace of mind. Our WAF solution protects against Open Worldwide Application Security Project (OWASP) Top 10 security threats, such as cross-site scripting, illegal resource access, and remote file inclusion, blocking attacks in real time. Our threat research team updates rules that are automatically pushed out daily to ensure our solution protects customers from the latest threats.</p> <p>REs can uncover hidden risks and vulnerabilities while creating reports to effectively communicate risk and ongoing activities with Imperva Data Security Fabric Data Risk Analytics, which monitors data access and activity for all databases and provides the visibility needed to pinpoint risky data access activity for all users, including privileged users. It delivers real-time alerting and user access blocking of policy violations and cost-effectively retains years of data for audits. Combining deep domain security expertise with machine learning (ML) allows organizations to identify suspicious user and computer system behaviors that violate security policies, practices, and peer group norms. Purpose-built detection algorithms instantly recognize active attack exploits and immediately send incident alerts.</p> <p>Organizations can limit access to confidential resources through the use of MFA and SSO with SafeNet Authentication Service Private Cloud Edition (PCE). SAS PCE is an on-premises authentication platform that safeguards global infrastructure access points with over 200 out-of-the-box pre-tested configurations and supports third-party solutions via SAML, RADIUS, Agents, or APIs and offers diverse token types.</p>

Standard Code & Guidelines	Thales Solutions
<p>PR.AA - 3.1.ii. Identity Management, Authentication, and Access Control</p> <p>3. ...Principle of Least Privilege shall be followed along with segregation of duties...</p> <p>5. Access rights...</p> <p>7. All critical systems shall have MFA implemented...</p> <p>8. ...comprehensive log management...</p> <p>10. Physical access to assets is managed, monitored, and protected...</p> <p>17. API Security...</p> <p>S1, S2, S3, S7, S9</p> <p>1. Access Controls, Password Policy/ Authentication Mechanism...</p> <p>1.b. ...shall be on a need-to-use basis and based on the principle of least privilege...</p> <p>1.e. ...logged for audit and review purposes...</p> <p>1.i. ...shall have multi-factor security..."</p> <p>3.d. ...deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users)...</p> <p>4.a. ...restrict access to the sensitive information, hosts and services... shall be based on strong access control policy and principle of least privilege...</p> <p>4.b. REs shall install network security devices, such as WAF...</p>	<p>Imperva Web Application Firewall (WAF) provides out-of-the-box security for web applications, detecting and preventing cyber threats, ensuring seamless operations and peace of mind. Imperva WAF solution protects against Open Worldwide Application Security Project (OWASP) Top 10 security threats, such as cross-site scripting, illegal resource access, and remote file inclusion, blocking attacks in real time. Our threat research team updates rules that are automatically pushed out daily to ensure our solution protects customers from the latest threats.</p> <p>Imperva API Security offers full API visibility, automatically discovering API endpoints and assessing risks. It classifies sensitive APIs using call data, displayed in a user-friendly interface, enabling proactive security measures to safeguard at-risk APIs. Teams can enforce policies based on risk assessment without slowing development. Continuous monitoring ensures timely responses to changes, promoting faster, secure software releases. Imperva API Security offers versatile deployment options to meet diverse operational needs available as an add-on to your Cloud WAF or as part of the API Security Anywhere offering.</p> <p>CipherTrust Transparent Encryption provides continuous file-level encryption that protects against unauthorized access by users and processes in physical, virtual, and cloud environments with centralized key management and privileged user access control. The implementation is seamless and transparent to your applications/ databases and storage, so it can work across an enterprise's entire environment, keeping both business and operational processes working without changes, even during deployment and rollout.</p> <p>CipherTrust Enterprise Key Management streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases. Leveraging FIPS 140-2-compliant virtual or hardware appliances, our key management tools and solutions deliver high security to sensitive environments and centralize key management for home-grown encryption, as well as third-party applications.</p> <p>SafeNet Authentication Service Private Cloud Edition (PCE) enables organizations to centrally manage and secure access to enterprise applications. It offers single-sign-on to multiple web-based applications with the broadest range of authentication methods, including – One-Time Passwords (OTP), PKI credentials, Kerberos, and many more. All authentication methods are available in multiple form factors, such as smart cards, USB tokens, mobile apps, and hardware tokens.</p>
<p>PR.AA - 3.1.ii. Identity Management, Authentication, and Access Control</p> <p>S10, S11, S12</p> <p>1. Physical Security...</p> <p>1.e. ...perimeter of the critical equipment's room, if any, are physically secured and monitored..."</p> <p>2. Remote Support Service Security</p> <p>2.b. ...it must employ MFA...</p>	<p>Thales OneWelcome Identity and Access Management Solutions provide both the security mechanisms and reporting capabilities organizations need to comply with data security regulations. Thales multi-factor authentication devices use current and emerging protocols to support multiple applications at the same time. Use one security key that combines support for phishing-resistant authentication, FIDO2, biometric, U2F, and Passkeys to access the B2C/ B2B applications.</p> <p>Thales OneWelcome Consent & Preference Management module enables organizations to gather the consent of end consumers so that financial institutions may have clear visibility of consented data, thereby allowing them to manage access to data they can utilize. The B2B delegation capabilities support REs in managing the delegation of rights based on users' roles and responsibilities.</p>

Standard Code & Guidelines	Thales Solutions
<p>PR.AA - 3.1.ii. Identity Management, Authentication, and Access Control</p> <p>S13, S14</p> <p>2. REs shall frame suitable policies for disposal of storage media and systems... degauss/ crypto shredding...</p>	<p>CipherTrust Manager simplifies key lifecycle management, including activities such as generation, backup and restore, deactivation, and deletion. Its key destruction phases allow organizations to achieve digital shredding of data.</p>
<p>PR.AA - 3.1.ii. Identity Management, Authentication, and Access Control</p> <p>S16, S17</p> <p>1. API Security</p>	<p>Imperva API Security enables comprehensive API visibility for security teams – without requiring development to publish APIs via OpenAPI or by adding resource-intensive workflow to their CI/CD processes. Moreover, every time an API is updated, security teams can stay on top of the change, understand any new risks, and incorporate changes, which leads to faster, more-secure software release cycles. Imperva API Security enables security teams to keep pace with innovation without impacting development velocity.</p>
<p>PR.DS – 3.3.ii. Data Security</p> <p>1. Data-at-rest and Data-in-transit shall be protected...with industry standard encryption algorithms...</p> <p>2. REs shall classify their data ...</p> <p>6. Data Classification & Data Localization “SEBI has envisaged data localization. Data localization means that all the data generated (including creation and storage) within the legal boundaries of India remains within the legal boundaries of India. Data localization ensures data sovereignty and data residency together...”</p> <p>S1, S2, S3</p> <p>1. Data and Storage Devices security</p> <p>1.a. Data shall be encrypted in motion, at rest and in-use by using strong encryption methods. Data-in-use encryption shall be applicable for cloud deployment (refer Annexure-J). Layering of Full-disk Encryption (FDE) along with File-based Encryption (FBE) shall be used wherever possible. REs shall use industry standard, strong encryption algorithms (e.g., RSA, AES, etc.) wherever encryption is implemented. Illustrative measures in this regard are given in Annexure-H and Annexure-I.</p> <p>2. Application Security in Customer Facing Applications</p>	<p>Data-at-rest</p> <p>Thales offers multiple solutions for data at rest that can coexist with native encryption provided by Cloud Service Provider (CSP).</p> <p>CipherTrust Transparent Encryption provides continuous file-level encryption that protects against unauthorized access by users and processes in physical, virtual, and cloud environments. The implementation is seamless and transparent to your applications/ databases and storage, so it can work across an enterprise’s entire environment, keeping both business and operational processes working without changes, even during deployment and rollout. CTE only employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange. The agent is FIPS 140-2 Level 1 validated.</p> <p>CipherTrust Tokenization provides tokenization, dynamic data masking for data anonymization and deidentification in the cloud.</p> <p>CipherTrust Application Data Protection provides format preserving or traditional encryption to applications using RESTful APIs. All of the above solutions can be used to provide protection for data at rest in the cloud.</p> <p>CipherTrust Manager is the central management point for the CipherTrust Data Security Platform. It manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role based access control to keys and policies, supports robust auditing and reporting, and offers developer-friendly REST API.</p> <p>Data-in-transit</p> <p>Thales High Speed Network Encryption (HSE) solutions secure data in motion as it moves across the network between data centers and headquarters, branch and satellite offices, to backup and disaster recovery sites, on premises and in the cloud.</p> <p>CipherTrust Data Discovery and Classification (DDC) enables organizations to discover and classify sensitive data – both structured and unstructured – across the cloud, big data, and traditional data stores. DDC provides a streamlined workflow from policy configuration, discovery, and classification, to risk analysis and reporting – helping to eliminate security blind spots and complexities.</p> <p>Imperva API Security provides comprehensive API visibility for security teams by automatically detecting endpoints and determining risks around sensitive data. It enhances protection against OWASP API Security Top 10 Risks for REs, allowing developers to build microservices and APIs across different environments.</p>

Standard Code & Guidelines	Thales Solutions
<p>Annexure-G: Application Authentication Security</p> <p>“Passwords, security PINs etc. ... should be one-way hashed using strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) ...”</p>	<p>CipherTrust Secrets Management (CSM) protects and automates access to secrets across DevOps tools and cloud workloads including secrets, credentials, certificates, API keys, and tokens. The solution is powered by Akeyless Vault easily integrates with other third-party applications such as GitHub, Kubernetes, OpenShift and more.</p>
<p>Annexure-I: Data Transport Security</p> <p>1...encryption mechanism such as TLS (Transport Layer Security...</p>	<p>Thales High Speed Encryptors (HSE) provide network-independent, data-in-motion encryption (layers 2, 3, and 4), ensuring data is secure as it moves from site to site or from on-premises to the cloud and back. Our network encryption solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception without performance compromise. Thales HSEs are available as both physical and virtual appliances, supporting a wide spectrum of network speeds from 10 Mbps to 100 Gbps.</p>
<p>Annexure-J: Framework for Adoption of Cloud Services</p> <p>Principle 6: Security Controls</p> <p>6.2.9.(ii) Encryption and Cryptographic Key Management:</p> <p>1a. “Bring Your Own Key” (BYOK) approach shall be adopted ... RE retains the control and management of cryptographic keys ...</p> <p>1b. “Bring Your Own Encryption” (BYOE) approach shall be followed by the RE.</p> <p>6.2.9.(ii) 3. Generating, storing and managing the keys in a Hardware Security Module (HSM) shall be implemented in a dedicated HSM to have complete control of Key management...</p>	<p>The CipherTrust Data Security Platform offers advanced encryption and centralized key management solutions, enabling REs to store sensitive data in the cloud safely. The platform offers advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to avoid cloud vendor encryption lock-in and ensure data mobility to efficiently secure data across multiple cloud vendors with centralized, independent encryption key management.</p> <p>CipherTrust Cloud Key Manager (CCKM) supports Bring Your Own Key (BYOK) use cases across multiple cloud infrastructures and SaaS applications. With the CipherTrust Data Security Platform, the strongest safeguards protect an enterprise’s sensitive data and applications in the cloud, helping the organization meet compliance requirements and gain greater control over data, wherever it is created, used, or stored. CCKM combines support for cloud provider BYOK APIs, cloud key management automation, and key usage logging and reporting, to provide cloud consumers with a cloud key management service that delivers strong controls over encryption key life cycles for data encrypted by cloud services.</p> <p>CipherTrust Transparent Encryption provides transparent encryption and access control for data residing in Amazon S3, Azure Files and more.</p> <p>CipherTrust Tokenization tokenizes the data before it is migrated to the cloud in the obfuscated form to protect the data from any breach.</p> <p>Thales Luna Hardware Security Modules (HSM) allows organizations to have a dedicated Hardware for a greater degree of control and ownership over the crypto keys rather than with the Cloud Service Provider (CSP). HSM provides a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Available in three FIPS 140-2 certified form factors, Luna HSMs support a variety of deployment scenarios.</p>

Applications		Data		Identities
 Web Application Firewall	←	 Encryption	 Data Activity Monitoring	←  Customer Identity & Access Management
 DDoS Protection		 Tokenization	 Data Discovery & Classification	 Workforce Identity & Access Management
 Bot Protection		 Key & Secrets Management	 Data Governance	
 API Security	→	 Hardware Security Modules	 Threat Detection	→  Broad Range of Authenticators

Visibility and Control: Thales and Imperva

Thales and Imperva, a Thales company, deliver a broad portfolio of complementary application security, data security, and identity & access management products to provide comprehensive solutions that help address CSCRf requirements. The portfolio delivers comprehensive data-centric security that protects data and all paths to it with platforms that reduce the complexity and risks of managing applications, data, and identities in the cloud.

About Thales

Thales is a global leader in data security, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.