sonatype

Navigating

India's Cybersecurity Guidance

for Finance Organizations

The Securities and Exchange Board of India (SEBI) is responsible for regulating India's security markets. In response to the **growing reality and evolving nature** of cybersecurity threats, SEBI introduced the Cybersecurity and Cyber Resilience Framework (CSCRF) in August 2024 with the goal of strengthening the defense of the regulated entities (RE) under its charge.

SEBI's CSCRF serves as a roadmap for **financial organizations** and sets out to establish uniform cybersecurity measures. Its stated objective is to, "address evolving cyber threats, to align industry standards, to encourage efficient audits, and to ensure compliance by SEBI REs. The CSCRF also sets out standard formats for reporting by REs."

The CSCRF is part of a larger effort within India's financial and technology sectors to increase the security and transparency of software development. For information about the Indian Computer Emergency Response Team's (CERT-In) Technical Guidelines on SOFTWARE BILL OF MATERIALS, you can download **Sonatype's Executive Summary**.

Elements of the CSCRF Framework

The framework integrates Cyber Resilience Goals with Cybersecurity Functions, further detailed into specific subsections:

- **Cyber Resilience Goals:** These outline the desired outcomes for REs to effectively manage and recover from cyber threats and include **Anticipate, Withstand, Contain, Recover,** and **Evolve**.
- **Cybersecurity Functions:** These represent the actions and processes implemented to achieve the resilience goals, which include **Governance (GV), Identify (ID), Protect (PR), Detect (DA), Respond (RS),** and **Recover (RC**).
- Each function is then broken down into specific areas. For example:
- **GV.OC (Organizational Context):** Understanding the internal and external factors affecting the organization.
- **GV.RR (Roles, Responsibilities, and Authorities):** Defining and assigning cybersecurity roles and responsibilities.
- **GV.PO (Policy):** Establishing cybersecurity policies.
- **GV.OV (Oversight):** Monitoring and reviewing cybersecurity practices.
- **GV.RM (Risk Management):** Identifying and managing cyber risks.
- **GV.SC (Supply Chain Risk Management):** Managing risks associated with third-party vendors.

The CSCRF includes 7 Cyber Resilience Goals and Cybersecurity Functions, which include:

- **Cyber Resilience Goal: Anticipate | Cybersecurity Function: Governance**
- **Cyber Resilience Goal: Anticipate | Cybersecurity Function: Identify**
- **Cyber Resilience Goal: Anticipate | Cybersecurity Function: Protect**
- **Cyber Resilience Goal: Anticipate | Cybersecurity Function: Detect**
- **Cyber Resilience Goal: Withstand and Contain | Cybersecurity Function: Respond**
- **Cyber Resilience Goal: Recover | Cybersecurity Function: Recover**
- **Cyber Resilience Goal: Evolve**

By aligning these components, the CSCRF ensures that REs have a structured approach to cybersecurity, enabling them to anticipate, withstand, contain, recover from, and evolve against cyber threats.

The number of laws, regulations, and frameworks emerging around the world on the topic of cybersecurity can be overwhelming. SEBI's CSCRF is particularly thorough, and in this executive summary, we examine the key features of these guidelines and how Sonatype can help users comply.

1. Cyber Resilience ANTICIPATE | Cybersecurity function: GOVERNANCE

CSCRF Section	CSCRF ID	Sonatype Capabilities	
GV.PO: POLICY **Organizational cybersecurity policy is established, communicated, and enforced.**	1.3	**Policy is a core feature of the Sonatype platform, and we support these functions through:** • **Centralized Governance:** Sonatype centralizes policy management, making it easier to maintain a comprehensive and enforceable cybersecurity policy. • **Scalable Compliance:** Automated enforcement and continuous monitoring help ensure ongoing compliance at scale. • **Proactive Risk Management:** Real-time updates and automated workflows enable proactive response to new risks and regulatory changes. • **Audit-Ready Reports:** Detailed reporting features facilitate audits and reviews by both internal teams and regulators.	Covers Policies GV.PO.S1-5
GV.OV: Oversight **Results of organization-wide cybersecurity risk management activities, performance, and outcomes are used to inform, improve, and adjust the risk management strategy.**	1.4	**Application Composition Reports, SBOMs, and Data Insights are key capabilities of the Sonatype platform and include:** • **Data-Driven Strategy Adjustment:** Sonatype helps organizations continuously refine their risk management strategy based on real-time data and historical outcomes. • **Improved Resilience Posture:** Through automated scanning and continuous monitoring, organizations can maintain a strong and up-to-date cyber resilience posture. • **Ease of Compliance:** Automated reporting and policy enforcement simplify the periodic reviews and assessments mandated by SEBI. • **Continuous Improvement:** By providing actionable insights and performance metrics, Sonatype enables organizations to implement a continuous improvement process for their cybersecurity strategy.	Covers Standards GV.OV.S1-4

GV.RM: Risk Management **The RE's priorities, constraints, risk tolerance and risk appetite statements, assumptions and constraints are established, communicated, and used to support operational risk decisions.**	1.5	**Application Composition Reports, SBOMs and Data Insights are key capabilities of the Sonatype platform and include:** • **Framework Implementation:** Sonatype helps establish a robust cyber risk management framework by automating key processes such as risk identification, mitigation, and monitoring. • **Real-Time Risk Visibility:** Continuous monitoring and real-time alerts ensure that risks are identified and addressed promptly. • **Policy-Driven Risk Tolerance:** Customizable policies allow organizations to define and enforce their risk tolerance and appetite effectively. • **Audit and Review Support:** Detailed reporting and audit logs support periodic reviews by IT committees and facilitate regulatory audits. • **Scenario Testing:** By enabling the creation and testing of different risk scenarios, Sonatype ensures that REs can validate their readiness to handle potential cyber threats.	Covers Standards GV.RM.S1-4
GV.SC: Cybersecurity Supply Chain Risk Management **The RE's priorities, constraints, risk tolerance, and assumptions are established and used to support decisions associated with managing supply chain risks. The RE has established and implemented the processes to identify, assess and manage supply chain risks.**	1.6	**The Sonatype platform in its entirety is a software supply chain management solution that allows broad control of third parties and continuous identification and evaluation through:** • **Comprehensive Supply Chain Risk Management:** Sonatype automates the identification, assessment, and mitigation of risks in third-party software, ensuring robust supply chain security. • **Real-Time SBOM Maintenance:** The platform provides continuous SBOM updates, ensuring compliance with SEBI's requirements for critical software. • **Periodic Compliance Reviews:** Automated monitoring and reporting support periodic reviews and help ensure ongoing compliance by third-party providers. • **Scenario Testing and Resilience Planning:** Sonatype enables response and recovery planning by simulating risk scenarios and supporting collaborative testing with third parties. • **Concentration Risk Analysis:** By mapping dependencies and identifying concentration risks, Sonatype helps organizations achieve operational resiliency.	Covers Standards GV.SC.S1-8

2. Cyber Resilience Goal: ANTICIPATE | Cybersecurity function: IDENTIFY

CSCRF Section	CSCRF ID	Sonatype Capabilities	
ID.AM: Asset Management **The data, personnel, devices, systems, and facilities that enable the RE to achieve its business purposes are identified and managed consistently in accordance with their relative importance to organizational objectives and the RE's risk strategy.**	2.1	**Using Sonatype Nexus Repository, you can manage, store, and audit each and every software asset ingested into the organization.** • **Automated Asset Inventory:** Sonatype automates the creation and maintenance of an up-to-date inventory of software assets, including APIs, libraries, and cloud-based components. • **Shadow IT Detection and Prevention:** By enforcing strict policies and continuously monitoring for unauthorized components, Sonatype helps eliminate shadow IT risks. • **Lifecycle Management:** The platform tracks software components throughout their lifecycle and provides actionable recommendations for upgrading or replacing outdated assets. • **Governance and Reporting:** Detailed reports generated by Sonatype can be used to secure board approval for critical systems and maintain auditable records of IT assets. • **Policy Enforcement:** Sonatype enables policy-driven management of IT assets, ensuring that all assets are properly managed, updated, and secured.	Covers Standards ID.AM.S1-6
ID.RA: Risk Assessment **The cybersecurity risk to the organization, assets, and individuals is assessed and understood by the RE.**	2.2	**Sonatype's Customer Success team is world-renowned for helping companies develop security policies and best practices associated with software and application asset management.** • **Automated and Continuous Vulnerability Assessment:** Sonatype provides real-time, automated identification and assessment of vulnerabilities, ensuring timely and accurate risk detection. • **Comprehensive Risk Context:** The platform enriches vulnerability data with contextual information to support informed risk prioritization and response. • **Rapid Threat Intelligence Integration:** By integrating with threat intelligence feeds and providing real-time alerts, Sonatype helps REs stay ahead of emerging threats and comply with advisory timelines. • **Risk Lifecycle Management:** Sonatype tracks risks throughout the lifecycle of IT assets, ensuring continuous risk management and compliance with SEBI's requirements. • **Policy Enforcement and Automation:** Automated policy enforcement helps reduce manual effort, ensuring consistent risk prioritization, planning, and communication.	Covers Standards ID.RA.S1-5

3. Cyber Resilience Goal: ANTICIPATE | Cybersecurity function: PROTECT

CSCRF Section	CSCRF ID	Sonatype Capabilities	
PR.DS: Data Security **Information and records (data) are managed consistent with the organization's risk strategy to protect the Confidentiality, Integrity, and Availability of information.**	3.3	**Audit and retention policies are key capabilities of Sonatype solutions.** • **Data Classification and Policy Enforcement:** Sonatype helps classify and manage IT and Cybersecurity Data, ensuring compliance with regulatory requirements for data security and accessibility. • **Environment Separation and Rigorous Testing:** The platform enforces separation of environments and ensures that rigorous testing is performed before deployment, reducing the risk of introducing vulnerabilities into production. • **Software Integrity Verification:** Sonatype provides robust integrity checks for software components, ensuring the integrity of critical systems and reducing the risk of tampered or malicious components. • **Auditability and Reporting:** Sonatype generates audit-ready reports and maintains detailed logs of all actions, supporting compliance with SEBI regulations. • **Continuous Monitoring:** By continuously scanning for vulnerabilities and integrity issues, Sonatype helps organizations maintain the ongoing confidentiality, integrity, and availability of their software assets.	Covers Standards PR.DS.S, S5, and S6
PR.IP: Information Protection Processes and Procedures **Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets.**	3.4	**Sonatype's customizable security policies and integration into existing tooling and alerting frameworks help companies manage the task of vulnerability and licensing compliance.** • **Automated Vulnerability and Malware Detection:** Sonatype scans for vulnerabilities and malicious code across all stages of the SDLC. • **Policy Enforcement:** It enforces security policies to ensure baseline configurations, secure development practices, and environment separation. • **Audit-Ready Reporting:** Sonatype provides detailed, audit-ready reports to support compliance with SEBI regulations, ISO 27001, and CIS standards. • **Third-Party Risk Management:** By scanning third-party components and generating compliance reports, Sonatype helps ensure that third-party providers meet required security standards. • **Continuous Monitoring:** The platform continuously monitors for new risks, helping organizations maintain compliance over time.	Covers Standards ID.RA.S1-5

4. Cyber Resilience Goal: ANTICIPATE | Cybersecurity function: DETECT

CSCRF Section	CSCRF ID	Sonatype Capabilities	
DE.CM: Security Continuous Monitoring **he REs' information systems and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.**	4.1	**Sonatype ensures compliance through continuous monitoring, securing third-party software, generating detailed audit reports, and integrating with SOC infrastructure for enhanced threat detection.** • **24/7 Continuous Monitoring:** Sonatype provides continuous, automated monitoring of software components and integrates with SOC tools to enhance real-time threat detection. • **Third-Party and Supply Chain Security:** Helps monitor and secure third-party software, ensuring supply chain risks are effectively managed. • **Detailed Reporting and Audit Support:** The platform generates comprehensive reports for audits, including vulnerability assessments, policy compliance, and change management, helping REs meet SEBI's audit requirements. • **Proactive Risk Mitigation:** By identifying and prioritizing risks early, Sonatype enables timely remediation, reducing the likelihood of incidents that SOC teams would need to respond to. • **Integration with Existing SOC Infrastructure:** Sonatype integrates with SIEM tools and other SOC systems to provide a unified view of software-related risks, enabling more effective monitoring and response.	Covers Standards DE.CM.S1-5
DE.DP: Detection Process **Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.**	4.2	**Sonatype provides clear accountability through role-based controls, enabling continuous detection validation in workflows, and automating compliance reporting.** • **Clear Role Assignment and Accountability:** Sonatype's role-based access control and issue assignment ensure that responsibilities for detection are well-defined and tracked. • **Continuous Process Testing:** By integrating detection processes into DevOps pipelines and SOC workflows, Sonatype enables continuous validation of detection mechanisms. • **Effective Communication of Detection Events:** Automated alerts and customized reports ensure that event information is communicated in a timely and compliant manner. • **Support for Red Teaming and Threat Hunting:** Sonatype enhances red teaming exercises by simulating software supply chain threats and aids in proactive threat hunting by monitoring open-source ecosystems for new risks. • **Enhanced SOC Capabilities:** By integrating with SIEM, SOAR, and other SOC tools, Sonatype enhances the SOC's ability to detect, investigate, and respond to software-related cybersecurity events.	Covers Standards ID.RA.S1-5

5. Cyber Resilience Goal: WITHSTAND & CONTAIN Cybersecurity function: RESPOND

CSCRF Section	CSCRF ID	Sonatype Capabilities	
RS.MA: Incident Management **Incident response plans and procedures are executed and maintained in order to ensure response to detected/ known cybersecurity incidents.**	5.1	**Enable real-time incident detection and response, automated containment, comprehensive audit trails, support for incident response drills, and integration with CERT-In threat intelligence.** • **Real-Time Incident Detection and Response:** Continuous monitoring and automatic policy enforcement ensure that incidents are detected and mitigated in real time. • **Automated Incident Containment:** Sonatype can block the use of risky components and enforce policy-based actions, ensuring rapid containment of incidents. • **Comprehensive Audit Trail:** Detailed logs of detection, mitigation, and accepted risks are maintained, supporting documentation and regulatory reporting requirements. • **Support for Incident Response Drills:** Sonatype facilitates the execution of incident response drills and playbooks, ensuring that teams are well-prepared to handle software-related incidents. • **Threat Intelligence Updates:** Integration with external threat intelligence sources, including CERT-In advisories, helps organizations stay updated on new risks.	Covers Standards RS.MA.S1-5
RS.CO: Incident Response Reporting and Communication **Response activities are coordinated with internal and external stakeholders (e.g., external support from CERT-In, law enforcement agencies, etc.). Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awarene.**	5.2	**Simplify compliance through automated incident reporting, ensuring SOP adherence, enabling real-time stakeholder coordination, maintaining comprehensive audit trails, and supporting continuous security improvement.** • **Streamlined Incident Reporting:** Automated detection and policy-driven alerts reduce the time it takes to identify, categorize, and report incidents to SEBI, CERT-In, and NCIIPC. • **Enhanced Accountability and SOP Adherence:** Role-based access and clear audit trails ensure each team member follows the documented incident response SOP. • **Rapid Stakeholder Coordination:** Integrations with collaboration and ticketing systems ensure that both internal and external stakeholders are informed and engaged in real time. • **Comprehensive Audit Trails:** Sonatype logs every action taken to remediate or respond to vulnerabilities, supporting after-action reviews and compliance audits. • **Continuous Improvement:** By analyzing incident response data, REs can refine their CCMP and detection processes, helping them improve resilience against future threats.	Covers Standards RS.CO.S1-3

RS.AN: Incident Analysis **Incident analysis is conducted to ensure effective response and support recovery activities.**	5.3	**The Sonatype platform centralizes vulnerability management, enabling forensic investigations, automating impact analysis, enforcing adaptive policies, and simplifying regulatory reporting.** • **Centralized Vulnerability and Incident Management:** Sonatype aggregates vulnerability intelligence from multiple sources and enables quick triage, root-cause analysis, and incident categorization in line with the CCMP. • **Comprehensive Forensic and RCA Capabilities:** By mapping vulnerable components to their usage across applications, Sonatype provides the traceability needed for in-depth investigations and root-cause analysis. • **Efficient Impact Analysis:** Automated mapping of components to applications reduces manual effort and speeds up impact assessments, ensuring faster incident resolution. • **Adaptive Policy Enforcement:** Insights from incident investigations can feed back into Sonatype's policy engine, enhancing future detection and reducing repeat incidents. • **Regulatory Reporting and Documentation:** Detailed logs and reports make it easier to document incidents, actions taken, and lessons learned, fulfilling SEBI's incident analysis and reporting requirements.	Covers Standards RS.AN.S1-5

7. Cyber Resilience Goal: EVOLVE

CSCRF Section	CSCRF ID	Sonatype Capabilities	
EV.ST: Strategies **A major component of cyber resilience is the ability to adapt and improve the security posture to stay ahead of threats.**	7.1	**Sonatype empowers REs to proactively mitigate threats, enhance technology diversity, refine security controls, adapt to emerging risks, and scale cyber resilience.** • **Proactive Threat Anticipation:** Sonatype's continuous scanning and real-time intelligence enable REs to discover and address new vulnerabilities before they become exploitable. • **Enforced Heterogeneity and Minimized Common Mode Failures:** By showing where component usage overlaps, Sonatype helps REs diversify their technology stack and reduce large-scale, single-point-of-failure risks. • **Incident-Driven Improvement:** Detailed tracking of incidents and vulnerabilities allows REs to refine security controls based on real-world threats, improving overall cyber resilience. • **Continuous Adaptation:** Automated policy updates and integrations with SOC/CI/CD ensure REs can swiftly respond to emerging threats and maintain an up-to-date security posture. • **Scalable for All RE Sizes:** From large Market Infrastructure Institutions (MIIs) to mid-size and small REs, Sonatype's reports and dashboards simplify periodic evaluations of cyber resilience posture.	Covers Standards EV.ST.S1-5

sonatype

Sonatype is the software supply chain security company. We provide the world's best end-to-end software supply chain security solution, combining the only proactive protection against malicious open source, the only enterprise grade SBOM management and the leading open source dependency management platform. This empowers enterprises to create and maintain secure, quality, and innovative software at scale. As founders of Nexus Repository and stewards of Maven Central, the world's largest repository of Java open-source software, we are software pioneers and our open source expertise is unmatched. We empower innovation with an unparalleled commitment to build faster, safer software and harness AI and data intelligence to mitigate risk, maximize efficiencies, and drive powerful software development. More than 2,000 organizations, including 70% of the Fortune 100 and 15 million software developers, rely on Sonatype to optimize their software supply chains. To learn more about Sonatype, please visit www.sonatype.com.

Headquarters
8161 Maple Lawn Blvd,
Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High
St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
60 Martin Place,
Level 1
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com