NOTICE

Notice No.	20260903-15
Notice Date	03 Sep 2026
Category	Compliance
Segment	General
Department	Trading Operations
Subject	Standardization Testing and Quality Certification (STQC) and other compliance requirements for Software Vendors as per Cyber Security and Cyber Resilience Framework (CSCRF) of SEBI
Attachments	No Attachment

To All Vendors,

SEBI has issued a circular with subject “Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)” vide reference no. SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024, with objective to strengthen the cybersecurity measures in Indian securities market, and to ensure adequate cyber resiliency against evolving cyber threats, cybersecurity incidents/ attacks.

Further, as per CSCRF circular, “*all software services in the form of SaaS/ Hosted services, COTS, customized COTS, in-house developed software, etc. shall be certified for application security and functional audit. COTS products empanelled by stock exchanges/ depositories shall be certified for application security testing, and functional audit by STQC at the time of empanelment.*”

Commercial Off The Shelf (COTS) being provided by empanelled vendors are covered in the aforesaid framework for Cybersecurity and Cyber Resilience Framework (CSCRF). As per standards PR.IP.S15, mentioned in the CSCRF framework, Empanelled vendors and prospective vendors are required to perform “Application security testing” and “Functional audit” through Standardisation Testing and Quality Certification (STQC) auditor.

Section A: Scope for STQC Certification:

1. **Application security testing:**
   i. Dynamic Application Security Testing (DAST) for scanning software applications in real-time against leading vulnerability sources, such as OWASP Top 10, SANS Top 25 CWE, etc. to find security flaws or open vulnerabilities.
   ii. Static Application Security Testing (SAST) for analyzing program source code to identify security vulnerabilities such as SQL injection, buffer overflows, XML external entity (XXE) attacks, OWASP Top 10 security risks, etc.

2. **Functional audit:** brief overview of the areas covered under the STQC Functional Audit:

   i. Login and Authentication
   ii. User Management
   iii. Input Validation
   iv. Navigation
   v. CRUD Operations (Create, Read, Update, and Delete)
   vi. Forms and Business Logic Validation

Notes:

- The above represents a high-level overview of the Application security testing and Functional Audit scope. To define the exact number of test cases and prepare a comprehensive functional test plan, STQC auditor would require the complete Software Requirements Specification (SRS) document, as the scope and coverage are determined based on the application's documented functional requirements.
- Refer – Annexure A “STQC – Terms of Reference”.

Section B: Process for registration of Software of Empanelled vendors:

1. Prospective Vendor:

i. At the time of empanelment (COTS) vendors are required to provide STQC certification for the software/ products (ETI, IBT, STWT, API & Back Office) solution to be registered with the Exchange as per SEBI circular no. SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024, on Cybersecurity and Cyber Resilience Framework (CSCRF).
ii. Provisional empanelment to be granted based on STQC labs' acknowledgement for completion of testing.
iii. Post submission of test report by STQC Lab, where the vulnerabilities/ observations are identified by the STQC Centre and closure is pending, the vendor shall submit a "Compensatory Control Letter" duly signed by the CTO, detailing interim controls, risk assessment, mitigation measures and target closure dates. Final empanelment to be granted after receipt of certificate from STQC regional centre.
iv. In the case of a newly empanelled vendor and product registration during the year, where the STQC certificate has already been submitted to the Exchange, the vendor shall not be required to resubmit the STQC certification at the time of annual STQC certificate submission to Exchange for that initial year.
v. From the subsequent year onwards, the vendor shall comply with the STQC certification requirements and guidelines applicable to all empanelled vendors.

2. Existing Empanelled Vendor:

i. STQC certification is required for all the latest versions of ETI, IBT, STWT, API & Back Office Softwares/Applications products which are already registered with the Exchange at the time of issuance of circular. The STQC certificate is required to be submitted by February 28, 2027.
ii. Subsequently on an annual basis, STQC certification is required to be submitted for period ending 31st March by 30th June every year. The annual submission process would become effective with effect from March 31, 2028.
iii. For registering new software/products solution/version with the Exchange, STQC certification is mandatory.
iv. New product may be registered on provisional basis after submission of STQC laboratory acknowledgment along with the other applicable documents.
v. In case of software changes, only the delta version introduced through the change may be subjected to testing by the STQC Laboratory. However, all impacted modules, interfaces, integrations and dependencies shall also be tested to ensure there is no adverse impact on application security, functionality or performance.
vi. Based on the provisional registration of the vendor product, Trading member can apply for product registration.
vii. Post submission of test report by STQC Lab, where the vulnerabilities/ observations are identified by the STQC Centre and closure is pending, the vendor shall submit a "Compensatory Control Letter" duly signed by the CTO, detailing interim controls, risk assessment, mitigation measures and target closure dates.
viii. Vendors shall submit a declaration covering all currently deployed and supported versions, confirming that such versions are covered under STQC certification. The declaration shall include product name, version number, etc (ETI, IBT, STWT, API & Back Office Softwares/Applications).
ix. Final product registration to be granted after receipt of certificate from STQC regional centre.

Further, vendors may have developed the software which are applicable for one or more Exchanges. In such cases vendor may get the STQC done for the software used in any of the Exchanges and subsequently share with all the concerned Exchanges.

Section C: Vendors seeking registration for Non-Exchange Frontend software/systems shall continue to provide the following documents to the Exchange at the time of registration:

i. Application for registration of the software with details of the product / segment / versions / applicable exchanges etc.
ii. Product write-up including write-up on Risk Management Systems.

iii. Vendor shall continue to submit a CISA / CISSP / CISM / DISA certified Auditor's certificate as per existing formats.

iv. Vendors shall also be required to provide information on the minimum software / hardware requirements for their respective versions at the time of registration. The same can be part of the product / version write-up or can be provided as a separate document to the Exchange.

v. When registering the software, vendors shall be required to:
   a. Declare the baseline requirements and security patch levels pertaining to OS, databases, enterprise mobile devices, etc. within the IT environment of member brokers. This baseline is for deployment of registered products and providing maintenance support.
   b. Ensure compatibility of the software with the specified OS, databases, enterprise mobile devices, etc.
   c. Provide a declaration that software vendors will cease maintenance support to member brokers for software that does not meet baseline requirements and alert exchange(s) immediately.

vi. Vendors developing STWT solutions shall be further required to adhere to standards PR.AA.S16 and PR.AA.S17 specified in the framework w.r.t. Mobile Application Security and API's.

vii. It may be noted that SEBI under the framework has specified Major change / Major Release and CSCRF has mandated VAPT after every major release. The following changes (including but not limited to) are broadly considered as major release(s) or major change(s):

   a. Implementation of a new SEBI circular.
   b. Changes in core versions of software (e.g., .net, SQL, Oracle, Java, etc.)
   c. Any changes in policy of login and/ or password management.
   d. Significant system modifications that alter how data is exchanged with stock exchanges (e.g., file format changes, message protocol changes, etc.).
   e. Introduction of new security protocols (e.g., switching from SSL to TLS 1.3).
   f. Expansion into new financial markets (e.g., adding currency trading).
   g. Implementation of new processes/ schema changes.
   h. Any change in the core RMS/OMS of the trading application.

Further, the empanelment and product registration shall be approved by the Stock Exchanges only after receipt of STQC certification and VAPT report from the COTS vendor.

It may be noted that members seeking registration of the software are required to provide a vendor confirmation letter. The vendor will be required to validate that the minimum software / hardware requirements including the baseline requirements and security patch levels have been met by the member where the application is being deployed and include the same in the confirmation letter being provided to members for onward submission to the Exchange.

In line with the above, the requirements specified under Section C applicable to vendors seeking registration of Non-Exchange Frontend software/systems, shall also be applicable to vendors providing Back Office software/applications. The detailed process for submission of applications and other related operational guidelines shall be communicated separately through an Exchange circular.

Section D: Reporting of Technical Glitch, Disclosures, Patch / vulnerability management and support to Stockbrokers

Any glitch which occurs in the software provided by vendors have a cascading effect on the system of stockbrokers who are availing software services from that vendor. Accordingly, all vendors are required to follow the below guidelines:

1. Vendors shall be required to have a documented process/procedure identifying, provisions for reporting, developing, testing and timely deployment of patches.

2. Vendors shall also be required to have documented processes to receive, analyze and respond to vulnerabilities/incidents disclosed to the vendor from internal and external sources (e.g. Internal Testing, Security

bulletins, Stock Exchanges, Stock Brokers, SEBI, CERT-In, any government authority and/or security researcher, etc.).

3. Vendor has to ensure all the vulnerabilities are closed before deployment at TM end. In case of non-reporting or delayed reporting appropriate disciplinary actions to be taken by the Exchange / regulators including but not limited to levy of penalties, restriction in onboarding of new members as an empanelled vendor, dis-empanelment of the Vendor, etc. in case where non compliances are observed.

4. Vendors shall also be required to communicate the vulnerabilities identified to stockbrokers. Till the time vulnerability closure patch is being developed by the vendor, the vendors shall be required to provide aid / support to the stock broker to place compensatory controls for the identified vulnerability. The closure of vulnerabilities shall also be required to be regularly tracked by technology Committee of the member.

5. For all patches / releases vendor should conduct sanity testing in UAT environment and post successful testing the same should be provided to members. Vendors should highlight and communicate the vulnerabilities as well as the risks to stockbrokers due to non updation of the latest patches.

6. Vendors should support up-to-date, stable, and actively supported releases of required software, as provided by the respective OEMs

7. Vendors and members shall be required to follow Software Change Management for such fixes / patches.

8. All deployment should be done in phased manner across stockbrokers to minimize unknown impacts occurring simultaneously.

9. Centralized update mechanism should not be followed by the vendor. The releases must be provided on sftp or any other agreeable mechanism between Member and Vendor and it will be the Members responsibility to download and update the same.

Further to ensure appropriate safeguards to avoid trading disruption in case of failure of software vendor, stockbrokers shall consider including the following in their contracts/agreements with the software vendors:

1. Agreement between the vendor and stockbroker may have the clause of compliance w.r.t. the proposed framework and for the requirement specified thereof
2. Availability of adequate skilled manpower with vendors to provide support to the stockbrokers in resolving glitch, vulnerabilities and/or patch management etc.
3. Promptness in taking action in closing reported vulnerabilities.
4. Periodic verification of compatibility of hardware/server of stockbroker with the software version of vendor's software
5. Development of expertise at the end of the stockbroker through appropriate training with regard to software usage and maintenance
6. Obligation on the part of the software vendor to cooperate in case of audit of software including forensic audit, if required.

Section E: Further strengthening of the vendor software registration framework:

1. Since the Vendors are providing services to multiple members including QSB's following may be considered which is included in the CSCRF framework for RE's
2. All vendors empanelled with the Exchange may be mandated to obtain ISO 27001 certification within 1 year of the date of issuance of applicability and the evidence of certification shall be submitted along with the periodic audit report.
3. Standard GV.SC.S7 of the SEBI CSCRF framework also addresses concentration risk arising from empanelled vendors providing services to multiple members. To mitigate such risks, empanelled vendors are required to submit an annual declaration covering key aspects such as adequacy of capacity to service subscribing members, scalability of software applications in line with Segregation and Multi-Tenancy Controls, business volumes, availability of robust backup solutions, high availability architecture/load balancers, Cybersecurity

Strengthening and defined BCP–DR mechanisms with specified recovery timelines, operational resilience, and adherence to requirements relating to data classification, localization, and storage.

4. Framework for reporting for vulnerabilities being identified / reported by market participants, Government Authorities, cybersecurity researchers, auditors, etc., for vendor products to be highlighted to all the members to whom the software solution has been provided and the Exchange and stakeholders (in line with timelines which have been specified for members/RE's). Appropriate clauses to that effect to be included in the audit report. In case of non-reporting or delayed reporting appropriate disciplinary action to be taken by the Exchange including but not limited to dis-empanelment of the Vendor.
5. Vendors must maintain a list of software versions used by member brokers. The versions can vary between member brokers only because of feature enhancement. All member brokers shall be using same latest security patched version of the software.
6. Vendor shall be required to declare to the Exchange as well as the stockbrokers end of life for their own software versions as they cease to maintain/support to stockbrokers and also place a surrender request with the Exchange for such products, after ensuring that same software versions has been surrendered by the respective members.
7. Requirement traceability matrix to be maintained by vendors.
   Under the **SEBI Cybersecurity and Cyber Resilience Framework (CSCRF)** guidelines, a software vendor shall maintain **Requirements Traceability Matrix (RTM)** for all the categories of software solutions/ applications/ products **for critical systems used by REs**. This serves as audited proof that every business/functional requirement is securely implemented, tested, deployed and followed by change management.

   Scope of the RTM as follows:

   i. Business Requirements
   ii. Functional Requirements
   iii. Non-Functional Requirements (performance, availability, usability, etc.)
   iv. Security and Cybersecurity Requirements
   v. Regulatory and Compliance Requirements
   vi. Interface and Integration Requirements
   vii. Customer-Specific Requirements

8. In case maintenance support is discontinued by the software vendor, the vendor shall be required to inform exchanges that the stockbroker is using software product without support.
9. Vendors shall be required to submit a Periodic declaration providing the list of software versions used by members. The list shall include member code, software product, versions number etc.

Section F: ***Software Bill of Materials (SBOM)***

1. As mentioned in standards GV.SC.S5 of the framework, MIIs shall include SBOM as part of their empanelment criteria for application software vendors. As defined in the framework, SBOM is a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. SBOM enumerates these components in a product. Accordingly, all vendors desirous of registering their software with the Exchange shall be required to include SBOM as part of the registration documents. The SBOM shall include (but not limited to) the following:
   a. License information
   b. Name of the supplier
   c. All primary (top level) components with all their transitive dependencies (including third-party dependencies whether in-house or open-source components) and relationships
   d. Encryption used
   e. Cryptographic hash of the components
   f. Frequency of updates
   g. Known unknown (where a SBOM does not include a full dependency graph)

h. Access control
i. Methods for accommodating occasional incidental errors.
j. SBOM shall be updated in the event of any change and accordingly vendor should ensure that all the related vulnerabilities are addressed.

2. CERT-In has issued "***Technical Guidelines on Software Bill of Materials (SBOM)"*** to be used by suppliers, developers and software consumer organizations. The guidelines highlight the following aspects:
    a. Implementation of SBOM for every new software component release and updated promptly for any updates, upgrades, releases and patches.
    b. SBOM classifications.
    c. Minimum elements of SBOM.
    d. Process and Practices of SBOM for Software Consumer/Developer/Integrator Organizations.
    e. Vulnerability Tracking and Analysis in SBOM.
    f. Recommendations and best practices for effectively managing SBOM.

    Vendors shall be required to follow the guidelines provided by CERT-In to gather SBOM and submit the same at the time of registration of the software with the Exchange.

Notes: Exchange will be sharing a separate circular for the following:

1. Standard GV.SC.S7 – Declaration covering key aspects towards Concentration risk
2. Scope for VAPT report
3. Format and procedure for disclosure of vulnerabilities to the Exchange.

For and on behalf of BSE LTD

Kaushal Mehta
VP - Trading Operations

Vinod Ibrampurkar
DVP - Trading Operations

Annexure A

STQC – Terms of Reference
(On the letterhead of STQC Laboratory)

Name of Vendor:

Software Information

Facility (ETI/IBT/STWT/Client Direct API/ Back Office)	Software Name	Software Version	Segment	Strategy Name (In-case of Algo)	Strategy Version (In-case of Algo)

SrNo.	Particulars	Audit firm
1.	All the categories of software solutions/ applications/ products for critical systems used by REs shall mandatorily pass-through the following tests/ audits and compliances:	-
a.	i. **Application security testing**: Dynamic Application Security Testing (DAST) for scanning software applications in real-time against leading vulnerability sources, such as OWASP Top 10, SANS Top 25 CWE, etc. to find security flaws or open vulnerabilities.	STQC
	ii. **Static Application Security Testing** (SAST) for analyzing program source code to identify security vulnerabilities such as SQL injection, buffer overflows, XML external entity (XXE) attacks, OWASP Top 10 security risks, etc.	STQC
b.	Functional audit	STQC

Detailed scope as follows:

Sr. No.	Area of Audit	Results & Observations	Remarks
A.	**DAST**	Results	Opinions
1.	**OWASP Top 10 (2025) – Web Application** • A01:2025 - Broken Access Control • A02:2025 - Security Misconfiguration • A03:2025 - Software Supply Chain Failures • A04:2025 - Cryptographic Failures • A05:2025 - Injection • A06:2025 - Insecure Design • A07:2025 - Authentication Failures • A08:2025 - Software or Data Integrity Failures • A09:2025 - Security Logging and Alerting Failures • A10:2025 - Mishandling of Exceptional Conditions		

Sr. No.	Area of Audit	Results & Observations	Remarks
2.	**OWASP Top 10 (2024) – Mobile Application** • M1: Improper Credential Usage • M2: Inadequate Supply Chain Security • M3: Insecure Authentication/Authorization • M4: Insufficient Input/Output Validation • M5: Insecure Communication • M6: Inadequate Privacy Controls • M7: Insufficient Binary Protections • M8: Security Misconfiguration • M9: Insecure Data Storage • M10: Insufficient Cryptography		
3.	**OWASP Top 10 (2023) – API** **API Security** • API1:2023 – Broken Object Level Authorization • API2:2023 – Broken Authentication • API3:2023 – Broken Object Property Level Authorization • API4:2023 – Unrestricted Resource Consumption • API5:2023 – Broken Function Level Authorization • API6:2023 – Unrestricted Access to Sensitive Business Flows • API7:2023 – Server-Side Request Forgery • API8:2023 – Security Misconfiguration • API9:2023 – Improper Inventory Management • API10:2023 – Unsafe Consumption of APIs **API Discovery** • Automated Discovery Tools – Use scanners and traffic monitoring to detect shadow or undocumented APIs. • Version Identification – Track all active, deprecated, and hidden API versions. • Endpoint Enumeration – Document every exposed endpoint, including test or debug endpoints.		
4.	**OWASP Top 10 (2021) – Thick Client** • DA1 - Injections • DA2 - Broken Authentication & Session Management • DA3 - Sensitive Data Exposure • DA4 - Improper Cryptography Usage • DA5 - Improper Authorization • DA6 - Security Misconfiguration • DA7 - Insecure Communication • DA8 - Poor Code Quality • DA9 - Using Components with Known Vulnerabilities • DA10 - Insufficient Logging & Monitoring		

Sr. No.	Area of Audit	Results & Observations	Remarks
5.	**SANS Top 25 – Most Dangerous Software Errors (Wherever Applicable)** • CWE-787: Out-of-bounds Write • CWE-79: Improper Neutralization of Input During Web Page Generation (XSS) • CWE-89: SQL Injection • CWE-20: Improper Input Validation • CWE-125: Out-of-bounds Read • CWE-416: Use After Free • CWE-352: Cross-Site Request Forgery (CSRF) • CWE-434: Unrestricted Upload of File with Dangerous Type • CWE-476: NULL Pointer Dereference • CWE-190: Integer Overflow or Wraparound • CWE-502: Deserialization of Untrusted Data • CWE-287: Improper Authentication • CWE-798: Use of Hard-coded Credentials • CWE-862: Missing Authorization • CWE-77: Command Injection • CWE-306: Missing Authentication for Critical Function • CWE-269: Improper Privilege Management • CWE-601: Open Redirect • CWE-732: Incorrect Permission Assignment for Critical Resource • CWE-94: Code Injection • CWE-522: Insufficiently Protected Credentials • CWE-611: Improper Restriction of XML External Entity Reference (XXE) • CWE-918: Server-Side Request Forgery (SSRF) • CWE-400: Uncontrolled Resource Consumption • CWE-426: Untrusted Search Path		
B	**SAST**	Results	Opinions
6.	**For Static Application Security Testing (SAST), you should focus on code-level vulnerabilities, secure coding practices, and proper handling of sensitive data. The checklist below highlights the most critical points to verify during SAST scans.** **Key Points to Check in SAST** **1. Injection Flaws** • **SQL Injection**: Ensure parameterized queries are used everywhere. • **Command Injection**: No unsanitized user input passed to shell/system calls. • **LDAP/XPath/XML Injection**: Validate and sanitize all inputs. • **Template Injection (SSTI)**: Avoid unsafe template rendering (e.g., Jinja2, Twig). • **Code Injection**: Prevent use of eval(), exec(), or similar with user input.		

Sr. No.	Area of Audit	Results & Observations	Remarks
	2. Cross-Site Scripting (XSS) • **Reflected XSS**: Encode all user input on output. • **Stored XSS**: Encode database-sourced values before rendering. • **DOM-based XSS**: Avoid unsafe sinks like innerHTML or document.write. • **Content Security Policy (CSP)**: Ensure CSP headers block inline scripts. **3. Sensitive Data Handling** • No **hardcoded secrets** (passwords, API keys, tokens) in source code. • No secrets in **git history** (use tools like TruffleHog). • Use **environment variables** for credentials. • Ensure .env files are excluded from version control. • Avoid logging sensitive data. **4. Authentication & Session Management** • Password hashing must use **bcrypt, scrypt, or Argon2** (not MD5/SHA1). • Session tokens should be **cryptographically random** (≥128 bits). • Password reset tokens must be **single-use** and expire quickly (≤15 minutes). • Implement **account lockout** after failed attempts. • Ensure **OAuth/OIDC** implementations follow specifications (state parameter, PKCE). **5. Code Quality & Security Practices** • **No insecure functions** (e.g., unsafe string concatenation for queries). • **Error handling**: Avoid exposing stack traces or sensitive debug info. • **Input validation**: Centralized validation for all user inputs. • **Secure dependencies**: Ensure libraries are up-to-date and free of known CVEs. **6. Tool & Environment Integration** • Ensure SAST tools support **deep language coverage** (Java, C#, Python, etc.). • Verify **compiler/embedded OS compatibility** for specialized environments. • Minimize **false positives** with actionable alerts. • Integrate SAST into **CI/CD pipelines** for continuous testing.		