



CA. Sakshi Agarwal

Member of the Institute

Cybersecurity Audit Framework: Essential Toolkit for Modern Auditors

Indian businesses face escalating cyber threats, and regulators demand robust cybersecurity audits. This article serves as a practical toolkit for auditors, especially Chartered Accountants, to navigate complex frameworks. It explains the Reserve Bank of India's (RBI) detailed cyber resilience requirements, including annexures covering baseline controls, security operations centre (SOC) guidelines, and incident-reporting templates. It also unpacks the Securities and Exchange Board of

India's (SEBI) Cybersecurity and Cyber Resilience Framework (CSCRF), introduced in August 2024 and now mandatory for all SEBI-regulated entities. Guidance is offered on global standards (ISO 27001, NIST 800-53, SOC 2) and the article structures audits around core domains such as governance, risk management, identity and access management, asset management, compliance, and business continuity. Each domain includes example controls, enabling auditors to deliver actionable insights and strengthen cyber defences¹.

Introduction: Cybersecurity as a Governance Imperative

Cyber-attacks on Indian organisations have highlighted the need for strong cyber governance. In 2018, a co-operative bank in Pune lost ₹94 crore (≈US\$13 million) after malware was used to compromise its payment system. Another incident saw 4.5 million airline passengers' data exposed after the carrier's IT vendor was hacked. These breaches prompted regulators to strengthen oversight. The RBI expanded its cyber framework to include detailed annexures specifying baseline controls, SOC requirements, and incident reporting templates. SEBI introduced the CSCRF to ensure cyber resilience across all financial-market entities. Chartered Accountants and internal auditors must therefore broaden

their role from traditional financial oversight to advising on cyber risk, compliance, and resilience².

RBI's Cybersecurity Framework: Annexures and Key Controls

The RBI's cyber security circular (2016) outlines baseline controls for banks and payment operators, expanded through annexures that apply across regulated entities. Compliance requires a board-approved cybersecurity policy and a risk management programme covering prevention, detection, and response.

Annex 1: Baseline Cybersecurity and Resilience Requirements

Annex 1 lists minimum controls that banks must implement. Key areas include:

- **Governance and risk management:** Inventory of IT assets, classification of critical information, and periodic risk assessments.
- **Protection and prevention:** Secure configuration of hardware and software, network segmentation, encryption of sensitive data, strong authentication, and multi-factor access controls.
- **Monitoring and detection:** Centralised logging, continuous security monitoring, and threat intelligence to identify anomalies.
- **Incident response and recovery:** Procedures for incident reporting within two to six hours, root-cause analysis, corrective actions, and lessons learned.

¹ RBI Cyber Security Framework in Banks (June 2, 2016) – Official RBI circular outlining the need for a board-approved cyber security policy, risk assessments, security operations centres and structured incident reporting. Available at <https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/NT41802062016.pdf#:~:text=Need%20for%20a%20Board%20approved,risk%2C%20duly%20approved%20by%20their>

² NIST Cybersecurity Framework 2.0 – Small Business Quick-Start Guide (Feb 2024) – Describes the six CSF functions and provides sample asset inventories and risk assessment questions. Available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf#:~:text=vulnerabilities%2C%20requirements%2C%20etc,MSSP>

- **Vendor management:** Due diligence of third parties and the right to audit service providers handling customer data.

These controls apply to banks, but similar principles extend to non-bank payment operators via the RBI's 2023 Master Direction on cyber resilience, which emphasises risk assessments, encryption, and digital-payment security³.

Annex 2: Setting up a Cyber Security Operations Centre (C-SOC)

Annex 2 requires banks to establish a Cyber Security Operations Centre (C-SOC) with capabilities for real-time monitoring, behaviour analytics, and incident response. The C-SOC must integrate logs from networks, servers, and applications, analyse them for anomalies and coordinate responses across the organisation. Banks may operate the SOC in-house or outsource to qualified third parties, but they remain responsible for governance and oversight. Regular drills and evaluations ensure readiness and continuous improvement⁴.

Annex 3: Cyber Incident Reporting Template

Annex 3 standardises how banks report cyber incidents to the RBI. The template requires details such as the nature of the attack, systems

affected, detection time, actions taken, root cause analysis, and measures to prevent recurrence. Banks must report incidents within six hours of discovery, aligning with CERT-In's reporting timelines, and follow up with updates as investigations progress⁵.

Third-Party Risk Management

In addition to the above, Annex 3 also includes guidelines on third-party risk management. Banks must identify critical vendors, conduct annual security assessments and include confidentiality, data-protection, and right-to-audit clauses in contracts. Outsourcing cannot absolve banks of responsibility; they must monitor vendor compliance, ensure data localisation, and maintain controls over outsourced SOC and cloud services⁶.

SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF)

SEBI released the CSCRF in August 2024 to establish uniform cyber governance across capital markets. It applies to market infrastructure institutions (stock exchanges, clearing corporations), qualified regulated entities (mutual funds, asset managers), and mid-size firms, as well as credit rating agencies, venture funds, and other regulated entities⁷.

Core Elements of CSCRF

- **Cybersecurity governance:** Entities must adopt a board-approved cybersecurity policy, define roles and responsibilities, and implement a cyber risk management framework.
- **Risk assessment and critical system identification:** Organisations must classify IT assets, identify critical systems (trading platforms, payment gateways), and conduct periodic risk assessments.
- **Cyber Capability Index (CCI):** SEBI uses a numerical score to benchmark the cybersecurity readiness of entities. Market infrastructure institutions undergo third-party assessments twice a year, while qualified entities perform annual self-assessments⁸.
- **Security Operations Centre:** All entities must establish 24×7 SOC or use shared market SOC created by exchanges. SOC efficacy must be reported periodically.
- **Vulnerability Assessment and Penetration Testing (VAPT):** Regular VAPT must cover all critical systems and be performed after major updates.

³ Conventus Law – Navigating SEBI's CSCRF – Article analysing clarifications issued in June 2025 (CISO roles, asset inventories, VAPT frequency and compliance thresholds). Available at <https://conventuslaw.com/report/india-navigating-sebis-cybersecurity-and-cyber-resilience-framework-key-clarifications-for-sebi-regulated-entities/#:~:text=The%20Securities%20and%20Exchange%20Board,compliance%20by%20SEBI%20Regulated%20Entities>

⁴ Conventus Law – Navigating SEBI's CSCRF – Article analysing clarifications issued in June 2025 (CISO roles, asset inventories, VAPT frequency and compliance thresholds). Available at <https://conventuslaw.com/report/india-navigating-sebis-cybersecurity-and-cyber-resilience-framework-key-clarifications-for-sebi-regulated-entities/#:~:text=The%20Securities%20and%20Exchange%20Board,compliance%20by%20SEBI%20Regulated%20Entities>

⁵ Simplifying RBI's Cybersecurity Mandates (InstaSafe) – White paper summarising baseline controls, SOC guidance and incident reporting requirements for banks. Available at <https://instasafe.com/docs/Brochure%20-%20RBI%20Guidelines%20for%20Cyber%20Security%20Framework.pdf#:~:text=Along%20with%20Cyber%20Security%20Framework,ty%20guidelines%20recommended%20by%20RBI>

⁶ RBI Cyber Security Framework in Banks (June 2 2016) – Official RBI circular outlining the need for a board-approved cyber security policy, risk assessments, security operations centres and structured incident reporting. Available at <https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/NT41802062016.pdf#:~:text=Need%20for%20a%20Board%20approved,risk%2C%20duly%20approved%20by%20their>

⁷ RBI Master Direction: Cyber Resilience & Digital Payment Security Controls (Jan 2023) – Master Direction detailing compliance timelines and resiliency measures for payment system operators. Available at <https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2024/10/securing-non-bank-psos-rbis-guidelines-on-cyber-resilience-and-digital-payment-security-controls.pdf.coredownload.inline.pdf#:~:text=RBI%20Master%20Direction%20on%20Cyber,for%20the%20digital%20payment%20ecosystem>

⁸ NIST Cybersecurity Framework 2.0 – Small Business Quick-Start Guide (Feb 2024) – Describes the six CSF functions and provides sample asset inventories and risk assessment questions. Available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf#:~:text=vulnerabilities%2C%20requirements%2C%20etc,MSSP>

- **Incident response and management:** Entities must maintain a documented incident response plan and cyber crisis management plan. Incidents must be reported promptly through SEBI's portal.
- **Data protection and access control:** Mandatory encryption (full-disk and file-level) and strict access controls with multi-factor authentication.
- **Backup and disaster recovery:** Entities must maintain disaster recovery plans, perform regular backups, and test restoration.
- **Red teaming and continuous improvement:** SEBI mandates periodic red-team exercises and ongoing updates to policies and staff training.
- **Compliance reporting and auditing:** Entities must submit structured reports to SEBI and undergo regular cybersecurity audits, with adoption deadlines set for January 1, 2025, or April 1, 2025, depending on previous obligations.

Why CSCRf Matters

The CSCRf emphasises both cybersecurity and resilience, requiring entities to anticipate, withstand, contain, recover from, and evolve after cyber incidents. By aligning controls to these goals, SEBI aims to ensure market stability and investor confidence. Auditors should evaluate organisations' adherence to the framework, ensuring that policies, SOC operations, data localisation, and vendor management meet SEBI's standards⁹.

Global Standards and Best Practices

Indian regulations should be benchmarked against global standards to ensure robust security:

- **ISO/IEC 27001:** Provides a structured information security management system, emphasising risk assessment, control implementation, and continual improvement.
- **NIST SP 800-53 and NIST Cybersecurity Framework:** Offer detailed control catalogues and a framework of functions (Identify, Protect, Detect, Respond, and Recover) that parallel the SEBI CSCRf goals.
- **SOC 2 (Trust Services Criteria):** Evaluates security, availability, processing integrity, confidentiality, and privacy; useful for service providers and technology firms.

By mapping Indian requirements to these global frameworks, auditors can identify gaps, adopt international best practices, and prepare organisations operating across borders.

Core Cybersecurity Audit Domains & Responsibilities

To deliver a comprehensive cybersecurity audit, auditors should structure their review around the following domains. Each domain includes example controls to guide assessment.

1. Governance & Policy

- **Responsibilities:** Verify the presence of a board-approved cybersecurity policy; evaluate management's oversight and

assignment of security roles. Ensure policies align with RBI Annex 1 and SEBI CSCRf.

- **Example controls:** Formal information security charter; senior management training; periodic policy reviews; evidence of board minutes approving security strategy.

2. Risk Assessment & Management

- **Responsibilities:** Check whether the organisation maintains an inventory of assets, assesses risks regularly, and records mitigation actions. Ensure risk appetite aligns with business objectives¹⁰.
- **Example controls:** Enterprise risk register with cyber entries; documented methodology for evaluating threats and vulnerabilities; integration of cyber risks into overall risk management; evidence of scenario-based testing¹¹.

3. Asset Management

- **Responsibilities:** Confirm up-to-date inventories of hardware, software, data, and third-party services; validate asset classification and protection commensurate with sensitivity.
- **Example controls:** Automated asset discovery; tagging of data and systems; configuration management database; secure asset decommissioning.

4. Identity & Access Management (IAM)

- **Responsibilities:** Assess user provisioning, authentication, and authorization. Check the

⁹ RBI Master Direction: Cyber Resilience & Digital Payment Security Controls (Jan 2023) – Master Direction detailing compliance timelines and resiliency measures for payment system operators. Available at <https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2024/10/securing-non-bank-psos-rbis-guidelines-on-cyber-resilience-and-digital-payment-security-controls.pdf>.coredownload.inline.pdf#:~:text=RBI%20Master%20Direction%20on%20Cyber,for%20the%20digital%20payment%20ecosystem

¹⁰ RBI Master Direction: Cyber Resilience & Digital Payment Security Controls (Jan 2023) – Master Direction detailing compliance timelines and resiliency measures for payment system operators. Available at <https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2024/10/securing-non-bank-psos-rbis-guidelines-on-cyber-resilience-and-digital-payment-security-controls.pdf>.coredownload.inline.pdf#:~:text=RBI%20Master%20Direction%20on%20Cyber,for%20the%20digital%20payment%20ecosystem

¹¹ Simplifying RBI's Cybersecurity Mandates (InstaSafe) – White paper summarising baseline controls, SOC guidance and incident reporting requirements for banks. Available at <https://instasafe.com/docs/Brochure%20-%20RBI%20Guidelines%20for%20Cyber%20Security%20Framework.pdf#:~:text=Along%20with%20Cyber%20Security%20Framework,ty%20guidelines%20recommended%20by%20RBI>

enforcement of least privilege, multi-factor authentication and monitoring of privileged accounts.

- **Example controls:** Role-based access control matrix; periodic user access reviews; multi-factor authentication for administrators; privileged access management (PAM) solutions; timely revocation of credentials when employees depart.

5. Network & System Security

- **Responsibilities:** Evaluate network segmentation, firewalls, intrusion detection systems, and endpoint protection. Ensure secure configuration of servers and devices.
- **Example controls:** Hardened system baselines; segregation of development and production networks; continuous vulnerability scanning; patch management schedules; anti-malware agents with real-time detection.

6. Application Security

- **Responsibilities:** Review the secure development life cycle (SDLC) and third-party software management. Check for regular vulnerability scans and penetration tests, particularly after major releases.
- **Example controls:** Secure coding guidelines; automated static/dynamic code analysis; penetration testing results; controls for open-source component management; change management records.

7. Data Protection & Privacy

- **Responsibilities:** Verify data classification, encryption at rest and in transit, and adherence to data minimisation and retention policies. Assess compliance with India's Digital Personal Data Protection Act and other regulations.
- **Example controls:** Encrypted databases and communication channels; data loss prevention tools; backups stored offline; secure disposal processes; privacy impact assessments for new systems¹².

8. Monitoring & Logging

- **Responsibilities:** Ensure critical systems generate logs that are consolidated and analysed. Logs should be synchronised with accurate time sources and retained in compliance with RBI and SEBI guidelines.
- **Example controls:** Centralised security information and event management (SIEM); use of behaviour analytics to flag anomalies; regular log reviews; alignment with Annex 2 SOC requirements; documented retention schedules.

9. Incident Response & Recovery

- **Responsibilities:** Review documented incident response and cyber crisis management plans. Check whether drills are conducted, and evaluate business continuity and disaster recovery capabilities.
- **Example controls:** Incident classification matrices; defined communication protocols; evidence of tabletop exercises; off-site backups; alternate

processing sites; defined recovery time and recovery point objectives.

10. Third-Party & Supply-Chain Security

- **Responsibilities:** Examine vendor risk management processes, including due diligence, contract clauses, and monitoring of service providers. Evaluate compliance with SEBI's requirements for supply-chain security (e.g., software bill of materials).
- **Example controls:** Supplier risk assessments; third-party security questionnaires; contractual terms covering confidentiality, breach notification, and audit rights; monitoring of outsourced SOC performance.

11. Compliance & Legal

- **Responsibilities:** Ensure all applicable laws and regulations (RBI, SEBI, CERT-In, DPDP Act) are identified and that policies and controls align with them. Verify timely submissions of required reports and evidence of regulatory audits.
- **Example controls:** Compliance matrix mapping controls to legal requirements; evidence of incident reports to regulators; records of external audit findings and remediation¹³.

12. Business Continuity & Disaster Recovery (BC/DR)

- **Responsibilities:** Assess preparedness to maintain operations during disruptions. Ensure business impact

¹² Conventus Law – Navigating SEBI's CSCRF – Article analysing clarifications issued in June 2025 (CISO roles, asset inventories, VAPT frequency and compliance thresholds). Available at <https://conventuslaw.com/report/india-navigating-sebis-cybersecurity-and-cyber-resilience-framework-key-clarifications-for-sebi-regulated-entities/#:~:text=The%20Securities%20and%20Exchange%20Board,compliance%20by%20SEBI%20Regulated%20Entities>

¹³ Conventus Law – Navigating SEBI's CSCRF – Article analysing clarifications issued in June 2025 (CISO roles, asset inventories, VAPT frequency and compliance thresholds). Available at <https://conventuslaw.com/report/india-navigating-sebis-cybersecurity-and-cyber-resilience-framework-key-clarifications-for-sebi-regulated-entities/#:~:text=The%20Securities%20and%20Exchange%20Board,compliance%20by%20SEBI%20Regulated%20Entities>

analysis has identified critical functions and that redundancy exists.

- **Example controls:** Documented BC/DR plans; regular disaster recovery drills; geographically separate backup sites; redundancy in power and network infrastructure; communication plans for prolonged outages.

Sample Audit Report Format

A well-structured report enhances the usefulness of audit findings. Include the following sections:

Executive Summary: Summarise scope, objectives, key findings, and overall risk assessment for board review.

Scope and Objectives: Define systems reviewed and compliance frameworks referenced (RBI, SEBI CSCRf, ISO 27001, NIST 800-53).

Methodology: Describe evidence gathered (policy review, interviews, configuration checks, VAPT results). Mention the use of automation, analytics, or red-team reports where applicable.

Detailed Findings and Recommendations: Group findings by domain; state condition, cause, and impact; assign severity; propose remediation actions.

Conclusion: Summarise overall cyber posture and highlight

priority recommendations. Provide management with a roadmap for improvement.

Appendices may include vulnerability scan reports, inventories, or compliance matrices¹⁴.

Sector-Specific Perspectives

While core controls remain consistent, different sectors warrant emphasis on certain domains:

- **Banking & Finance:** Banks must comply with RBI's annexures and the Master Direction. Auditors should scrutinise transaction monitoring, multi-factor authentication, encryption of customer data, and vendor oversight. Past heists highlight the need for strong SOC monitoring and incident reporting¹⁵.
- **Capital Markets:** For stock exchanges, asset managers, and intermediaries, adherence to SEBI's CSCRf is paramount. Emphasis should be placed on SOC operations, CCI scoring, VAPT after major system releases, and data localisation.
- **Technology & Start-ups:** Rapidly scaling firms often lack mature processes and rely heavily on cloud services. Auditors should assess cloud security posture, API security, and developer practices, ensuring vulnerability management and incident response are in place¹⁶.



- **Government & Public Sector:** These entities handle sensitive citizen data and critical infrastructure. Auditors should evaluate identity management, network segmentation, incident response readiness, and compliance with CERT-In's six-hour incident reporting rule¹⁷.

Audit-Tech Enablers and Future Considerations

Modern tools can enhance audit effectiveness:

- **AI and analytics:** Machine learning can sift through vast log data to detect anomalies. Continuous monitoring solutions such as Cloud Security Posture Management (CSPM) help maintain compliance with CSCRf's SOC requirements.
- **Automation:** Scripts can collect evidence (user lists, configuration

¹⁴ Conventus Law – Navigating SEBI's CSCRf – Article analysing clarifications issued in June 2025 (CISO roles, asset inventories, VAPT frequency and compliance thresholds). Available at <https://conventuslaw.com/report/india-navigating-sebis-cybersecurity-and-cyber-resilience-framework-key-clarifications-for-sebi-regulated-entities/#:~:text=The%20Securities%20and%20Exchange%20Board,compliance%20by%20SEBI%20Regulated%20Entities>

¹⁵ Simplifying RBI's Cybersecurity Mandates (InstaSafe) – White paper summarising baseline controls, SOC guidance and incident reporting requirements for banks. Available at <https://instasafe.com/docs/Brochure%20-%20RBI%20Guidelines%20for%20Cyber%20Security%20Framework.pdf#:~:text=Along%20with%20Cyber%20Security%20Framework,ty%20guidelines%20recommended%20by%20RBI>

¹⁶ RBI Master Direction: Cyber Resilience & Digital Payment Security Controls (Jan 2023) – Master Direction detailing compliance timelines and resiliency measures for payment system operators. Available at <https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2024/10/securing-non-bank-psos-rbis-guidelines-on-cyber-resilience-and-digital-payment-security-controls.pdf.coredownload.inline.pdf#:~:text=RBI%20Master%20Direction%20on%20Cyber,for%20the%20digital%20payment%20ecosystem>

¹⁷ Conventus Law – Navigating SEBI's CSCRf – Article analysing clarifications issued in June 2025 (CISO roles, asset inventories, VAPT frequency and compliance thresholds). Available at <https://conventuslaw.com/report/india-navigating-sebis-cybersecurity-and-cyber-resilience-framework-key-clarifications-for-sebi-regulated-entities/#:~:text=The%20Securities%20and%20Exchange%20Board,compliance%20by%20SEBI%20Regulated%20Entities>

baselines, patch status) and verify remediations. Integration with Governance, Risk, and Compliance (GRC) platforms streamlines tracking.

- **Penetration testing and red teaming:** Regular ethical hacking exercises reveal real-world vulnerabilities. Auditors should review these results and confirm remediation.

Looking ahead, threats like ransomware, supply-chain attacks, and privacy breaches will persist. Auditors must encourage resilient controls such as offline backups, vendor oversight, and data encryption. Emerging technologies (AI, quantum computing) will bring both opportunities and risks; staying informed of evolving standards and regulations is critical¹⁸.

Conclusion

Cybersecurity auditing is now integral to corporate governance. For Chartered Accountants and internal auditors, mastering this domain is essential to protect organisations and uphold investor confidence. By understanding and applying the RBI's annexures, SEBI's CSCRF, and global frameworks, auditors can structure comprehensive reviews across key domains. Incorporating example controls and leveraging modern tools ensures audits are thorough, practical, and aligned with regulatory expectations. Continuous learning and adaptation will enable auditors to help organisations anticipate, withstand, contain, and recover from cyber threats, ensuring resilience in an increasingly digital world.

References

- **RBI Notification on Cyber Security Policy** – RBI page emphasising separate cyber security policies, risk classification and SOC establishment.

Available at <https://www.rbi.org.in/commonperson/english/scripts/Notification.aspx#:~:text=the%20other%20hand%2C%20the%20number%2C,if%20and%20when%20they%20occur>

- **ReBIT Key Baseline Security Controls for Banks** – Guide listing asset management, governance, network segmentation, data protection, IAM, third-party risk management and more. Available at <https://pub.rebit.org.in/inline-files/02%20-%20Key%20Baseline%20Security%20Controls-REBIT-2018-CBI-RI-102.pdf#:~:text=Table%20of%20Contents%20I,Third%20Party%20Risk%20Assessment%20Framework>
- **SEBI Cybersecurity and Cyber Resilience Framework (CSCRF)** – Uniquis – PDF detailing the CSCRF goals, Cyber Capability Index, SOC requirements and implementation timelines. Available at <https://uniquis.com/wp-content/uploads/2025/04/Cybersecurity-and-Cyber-Resilience-Framework-for-SEBI-Regulated-Entities.pdf#:~:text=The%20CSCRF%20applies%20to%20a,continuous%20monitoring%20of%20security%20events>
- **SEBI CSCRF Guidance (Tikaj 2025)** – Blog explaining governance, risk assessment, SOC, VAPT, incident response, data protection, backup, red teaming and compliance reporting under CSCRF. Available at <https://www.tikaj.com/blog/sebi-csrf-cybersecurity-guideline/#:~:text=follow%20SEBI%E2%80%99s%20New%20Cybersecurity%20Guidelines>
- **Conventus Law** – Navigating SEBI's CSCRF – Article analysing clarifications issued in June 2025 (CISO roles, asset inventories, VAPT frequency and compliance thresholds). Available at <https://conventuslaw.com/report/india-navigating-sebis-cybersecurity-and-cyber-resilience-framework-key-clarifications-for-sebi-regulated-entities/#:~:text=The%20Securities%20and%20Exchange%20Board,compliance%20by%20SEBI%20Regulated%20Entities>
- **Sonatype** – SEBI CSCRF Explained – Overview of CSCRF combining resiliency goals with cybersecurity functions and emphasising supply chain risk management. Available at <https://www.sonatype.com/resources/guides/sebi-cyber-resilience-framework#:~:text=Cyber%20>

[Resilience%20Goals%20and%20Cybersecurity,Functions](#)

- **CyberSaint** – NIST SP 800-53 Control Families – Lists control families (Access Control, Audit & Accountability, Awareness & Training, etc.) and promotes NIST as a gold standard. Available at <https://www.cybersaint.io/blog/nist-800-53-control-families#:~:text=Identification%20and%20Authentication%20IR%20,NIST%20RMF%20Control%20Families%20related>
- **NIST Cybersecurity Framework 2.0** – Small Business Quick-Start Guide (Feb 2024) – Describes the six CSF functions and provides sample asset inventories and risk assessment questions. Available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf#:~:text=vulnerabilities%2C%20requirements%2C%20etc,MSSP>
- **NIST Cybersecurity Framework 2.0** (Feb 26 2024) – Official document defining high-level cybersecurity outcomes applicable to organisations of any size. Available at <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf#:~:text=Abstract%20The%20NIST%20Cybersecurity%20Framework,0%2C%20its>
- **NIST Identity & Access Management** – Digital Identity Guidelines (SP 800-63 Rev 4) – NIST page stressing that IAM ensures the right people and devices have appropriate access, with release details of the 2025 revision. Available at <https://www.nist.gov/identity-access-management#:~:text=On%20August%2C%20A01%2C%202025%2C%20NIST%20released,published%20by%20NIST%20in%202017>

Author may be reached at
eboard@icai.in

¹⁸ Conventus Law – Navigating SEBI's CSCRF – Article analysing clarifications issued in June 2025 (CISO roles, asset inventories, VAPT frequency and compliance thresholds). Available at <https://conventuslaw.com/report/india-navigating-sebis-cybersecurity-and-cyber-resilience-framework-key-clarifications-for-sebi-regulated-entities/#:~:text=The%20Securities%20and%20Exchange%20Board,compliance%20by%20SEBI%20Regulated%20Entities>