



Cybersecurity and Cyber Resilience Framework for alternative investment funds

Foreword

Because of its fast-changing nature, cybersecurity is becoming increasingly important to businesses across sectors. With their sophisticated yet complex operations, alternative investment funds (AIFs) manage enormous amounts of sensitive data, which makes them attractive targets for cyberattacks. Emphasising the need for AIFs to improve their cybersecurity posture, the Securities and Exchange Board of India (SEBI) has made it mandatory for these funds to implement strengthened cybersecurity measures and frameworks that effectively tackle cybersecurity vulnerabilities.

The PEVCCFO Association and PwC have worked together to create this guidebook on SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF) for AIFs, which offers AIFs a comprehensive framework for cybersecurity and cyber resilience. This guidebook is designed to aid AIFs in recognising weaknesses, understanding the requirements drafted by SEBI and implementing stringent security policies. It seeks to help AIFs manage their security mechanisms in the ever-changing regulatory environment.

By defining the main regulatory obligations AIFs have to follow, the CSCRF guidebook delineates SEBI's cybersecurity expectations. AIFs are encouraged to build a proactive attitude towards cybersecurity by routinely examining and upgrading their security policies to manage emerging risks and integrating best practices. Through its oversight and enforcement actions, SEBI also significantly contributes in preventing cybercrime and holds AIFs responsible for their cybersecurity practices.

Leveraging the knowledge and experience of the subject-matter experts at the PEVCCFO Association and PwC, the CSCRF guide is a valuable tool for AIFs to improve and strengthen their cybersecurity capacity and reduce imminent risks. We believe that this structure will play a vital role in protecting investor interests and, in the long run, will uphold the ongoing development and stability of the AIF sector in India.



Contents

01

Why SEBI is interested in the
cyber posture of AIFs 04

02

About the CSCRF 08

03

What AIFs need to do 12

04

CSCRF controls 22

05

How PwC can help 30



01

Why SEBI is interested in the cyber posture of AIFs

Why is the data of AIFs critical?

Data at risk



Disclosing investor identities

Alternative investment funds (AIFs) handle significant investments from high-net-worth individuals and institutions. Revealing investor identities could expose them to targeted attacks and fraud.



Disclosing sensitive business information

Funds hold sensitive data on portfolio companies, including strategic and financial information. Breaches could lead to loss of business, reputation and market position.



Disclosing sensitive deal information

Exposure of deal details and investment strategies can lead to insider trading, give competitors an edge and potentially manipulate financial markets.

Attacks



Insider threats

Insider threats can leak investment strategies or sensitive data which can erode a fund's competitive edge and cause major financial losses.



Business email compromise

Cyberthreats such as business email compromise can lead to data breaches, huge financial losses and investment in fraudulent assets.



Ransomware

Cyberthreats such as ransomware could disrupt the operations of these funds, leading to downtime, huge financial loss and loss of data.



What is SEBI's point of view?

The Securities and Exchange Board of India (SEBI) played a pivotal role by implementing AIF regulations in 2012. The AIF industry is now poised to reach **INR 43.64** lakh crore by **2028**.

Increase in cyber incidents

India's financial sector has suffered more than **20,000 cyberattacks** – or one-fifth of the total number of cyberattacks globally – totalling almost **USD 12 billion in losses since 2004** and USD 2.5 billion since 2020.



Increased ease of attacks

Due to the advent of artificial intelligence (AI) and automation, it has become easier to orchestrate and perform sophisticated cyberattacks in organisations with complex environments.



Enhancing cybersecurity

To enhance the cybersecurity and cyber incident preparedness of regulated entities (REs), SEBI issued the Cybersecurity and Cyber Resilience Framework (CSCRF) for all AIFs on 20 August 2024, ensuring uniform guidelines.



Growth of AIFs in India



AIFs have experienced a CAGR of **26%** between FY19–24



Assets under management (AUM) of AIFs is **INR 13.74** lakh crore as of **June 2024**



CAGR of AIFS is **double** that of mutual funds



Indian private equities share **>20% of the APAC funds**

Source: Mint, 2 Nov 2023. 'AIF industry estimated to expand at 26% CAGR to ₹43 lakh crore by 2028'
IMF, April 2024. Global Financial Stability Report, Chapter 3: 'Cyber risk a growing concern for macrofinancial stability'
AMFI, 'Indian Mutual Fund Industry's Average Assets Under Management (AAUM) stood at ₹ 66.04 Lakh Crore (INR 66.04 Trillion)'

Global cyber incidents

In recent years, the private equity (PE) and venture capital (VC) sectors have experienced a significant increase in cybersecurity incidents, reflecting the growing threats in the broader business environment. These incidents include business email compromise, data breaches, ransomware attacks, and other forms of cyber intrusion that have targeted PEs, AIFs, VCs and their portfolio companies.

Data breach

In 2021, a US-based VC experienced a cybersecurity incident due to a successful phishing attack on an employee's email. As a result, personal and financial information of investors may have been accessed by a third party.

01

Cyber fraud

A Norway-based investment fund fell victim to a sophisticated social engineering attack known as business email compromise, resulting in significant losses in 2020. The attackers manipulated and falsified communication between the fund and a microfinance institution, leading the fund to mistakenly transfer the loan to an account controlled by cybercriminals.

02

Ransomware attack

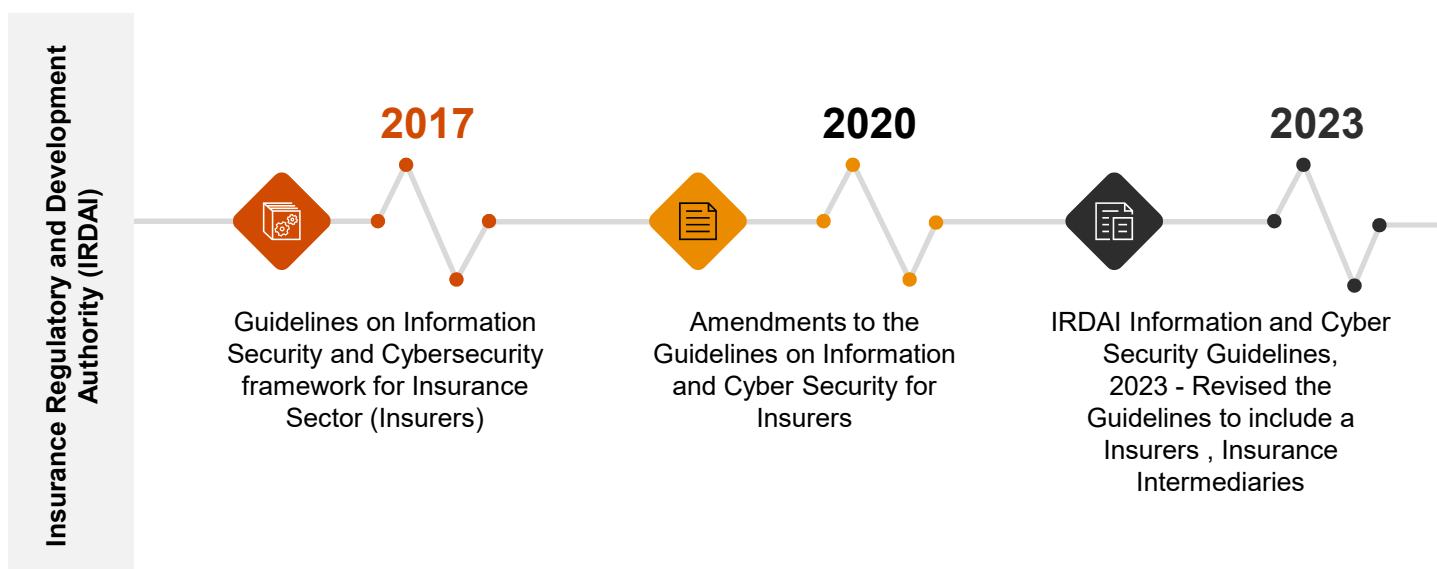
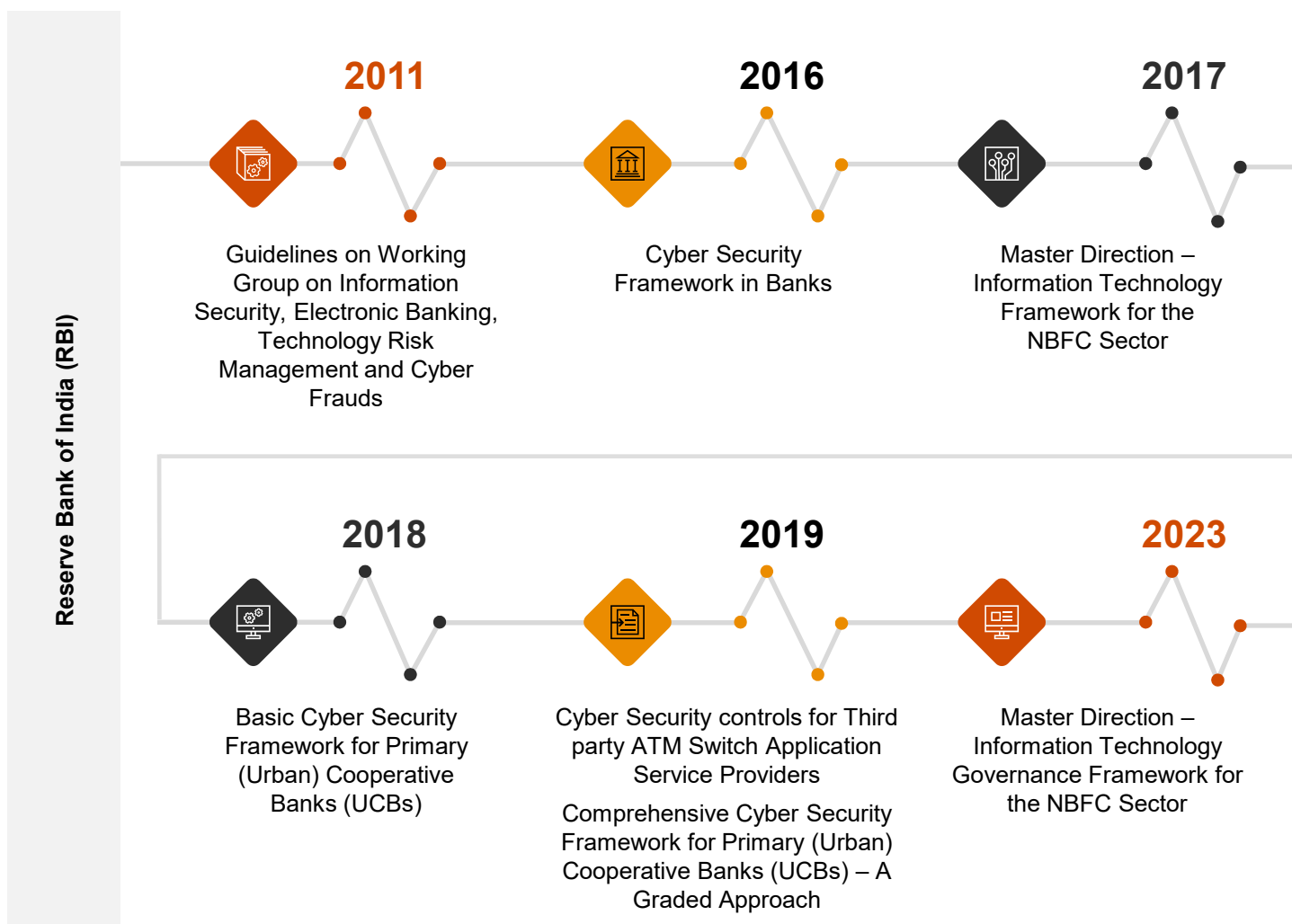
A Silicon Valley based VC firm suffered a ransomware attack in 2021. Attackers used a 'double extortion' tactic by encrypting data on two servers while also stealing sensitive information before encryption. The compromised data included the names, emails, phone numbers and social security numbers of private investors.

03



Evolution of the guidelines issued for cybersecurity by financial services regulators

Over the years, the regulatory landscape for cybersecurity has evolved. Below are the key milestones:



02

About the CSCRf

Overview of the CSCRf


To enhance cybersecurity in the Indian securities market and ensure resilience against cyber incidents, on 20 August 2024, SEBI issued the CSCRf in consultation with stakeholders for all regulated entities.


The framework is broadly based on two approaches: cybersecurity and cyber resilience. The cybersecurity approach covers various aspects of National Institute of Standards and Technology (NIST)-Cybersecurity from governance measures to operational controls and the cyber resilience goals based on CERT-In's Cyber Crisis Management Plan which includes the five goals of Anticipate, Withstand, Contain, Recover, and Evolve.


The CSCRf provides standards and guidelines to strengthen cyber resilience, align with industry norms and support efficient audits. It also establishes standard reporting formats for these entities.

Key pillars of the CSCRf

- 01 Governance
- 02 Risk management
- 03 Data protection
- 04 Application security
- 05 Monitoring and alerting
- 06 Cyber audits

The **key objective Of CSCRf** is to address evolving cyberthreats, align with the industry standards, encourage efficient audits, and ensure compliance by SEBI REs. 

It aims to ensure that even **smaller REs are equipped** with adequate cybersecurity measures and achieve resiliency. 

This framework shall **supersede existing SEBI cybersecurity circulars/guidelines/advisories/letters.** 

- ▶ **AIFs need to put in place appropriate systems and procedures to ensure compliance with the provisions of CSCRf by 1 April 2025.**
- ▶ **Cyber audit reports along with other required documents shall be submitted to SEBI by 1 April 2026.**
- ▶ **The CSCRf mandates all AIFs to establish appropriate security monitoring mechanisms through a security operation centre (SOC) for continuous monitoring of security events and timely detection of anomalous activities.**

Evolution of the CSCRf

- CSCRf for market infrastructure institutions (MII) (stock exchanges, clearing corporations and depositories)

2015



- CSCRf for qualified registrars to an issue/share transfer agents (QRTAs)

2017



2018

- CSCRf for stockbrokers/ depository participants
- SOC guidelines for stock exchanges, clearing corporations and depositories (except commodities derivatives exchanges and their clearing corporations)

2019

- Clarification of CSCRf for stockbrokers/ depository participants
- CSCRf for mutual funds/asset management companies (AMCs)
- CSCRf for KYC registration agencies (KRAs)
- CSCRf for qualified registrars to an Issue



2022

- Modification in CSCRf for MIIs
- Modification in CSCRf for stockbrokers/depository participants
- Modification of CSCRf for mutual funds/AMCs
- Modification in CSCRf for KRAs
- Modification in CSCRf for QRTAs

2023

- Guidelines and modification in the CSCRf for MIIs
- CSCRf for portfolio managers
- Cybersecurity best practices for all REs



2024

- CSCRf for all REs including AIFs



Note: The 2024 CSCRf framework shall supersede existing SEBI cybersecurity circulars/guidelines/advisories/ letters.

Applicability of the CSCRF

The applicability of various standards and guidelines of the CSCRF is based on different categories of REs. This CSCRF framework classifies AIFs in the following four categories based on AUM.

REs	Criteria	Self-certification REs	Small-size REs	Mid-size REs	Qualified REs
AIF	AUM	Less than INR 100 crore	INR 100 crore and above but less than INR 500 crore	INR 500 crore and above but less than INR 1,000 crore	INR 1,000 crore and above

The category of REs shall be decided at the beginning of the financial year based on the data of the previous financial year. Once the category of RE is decided, RE shall remain in the same category throughout the financial year irrespective of any changes in the parameters during the financial year.

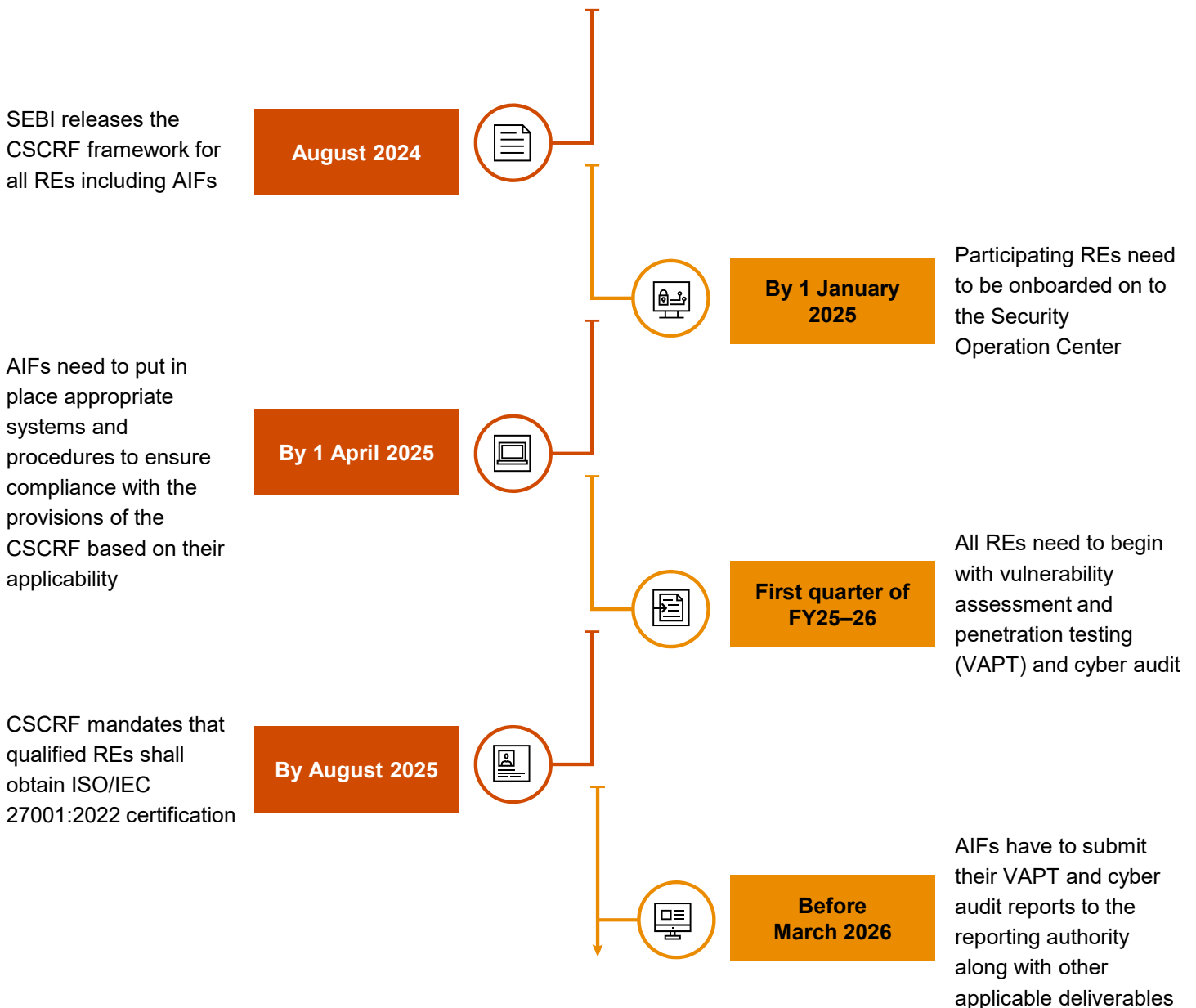
In case an RE is registered under more than one category, then the provisions of the highest category under which such an RE falls shall be applicable to that RE.



03

What AIFs need to do

Important dates



What AIFs need to do

Based on the categorisation of the AIF and VCF, each of these entities must do the following to ensure compliance with the CSCRF guidelines rolled out by SEBI:

	Self-certification REs (less than INR 100 crore)	Small-size REs (between INR 100 to 500 crore)	Mid-size REs (between INR 500 to 1,000 crore)	Qualified REs (above INR 1,000 crore)
1 Setting up an IT committee	Not mandatory	Not mandatory	Yes	Yes
2 ISO/IEC 27001:2022 audit and certification	No	No	No	Yes
3 Vulnerability assessment and penetration testing	Yes (annually in Q1)	Yes (annually in Q1)	Yes (annually in Q1)	Yes (annually in Q1)
4 Cyber audit	No	Yes (at least once a year)	Yes (at least twice a year)	Yes (at least twice a year)
5 Security operations centre (SOC)	Yes	Yes	Yes	Yes
6 Cyber Capability Index (CCI) Score	No	No	No	Yes – self-assessment

Setting up an IT committee

AIFs categorised as **qualified REs and mid-size REs** shall constitute an 'IT committee' which shall **mandatorily include at least one external independent expert on cybersecurity.**

Small-size REs and self-certification REs do not have to mandatorily setup an IT Committee. Compliance with CSCRF shall be reviewed and approved by the MD/CEO/board member/ partners/ proprietor.

Responsibilities of the IT committee

Undertake **periodic reviews of the implementation of the cybersecurity and cyber resilience policy** of the RE.

- Perform **periodic reviews of a cybersecurity incident (if any), its impact, root cause analysis (RCA) and plans** to strengthen the cyber resilience to mitigate re-occurrence of such incidents in future.
- **Deliberate on matters** which may be **referred** by the **board/partners/proprietor of the RE and/or SEBI.**
- **Review various compliances** as part of the CSCRF and **make recommendations** to the **board/partners/proprietor of the RE.**

ISO audit and certification

▶ Only **qualified REs** are required to obtain **ISO/IEC 27001:2022** Information security, cybersecurity and privacy protection – Information security management systems – requirements certification.

▶ For **qualified REs with existing ISO/IEC 27001:2013 certification**, it is mandated that by August 2025 they must migrate to the latest version and obtain ISO 27001:2022 certification.

▶ **Evidence of certification** should be **submitted** with the **cyber audit report** to SEBI.

▶ This certification must be achieved by qualified REs **within one year of issuance of CSCRF circular - August 2025.**



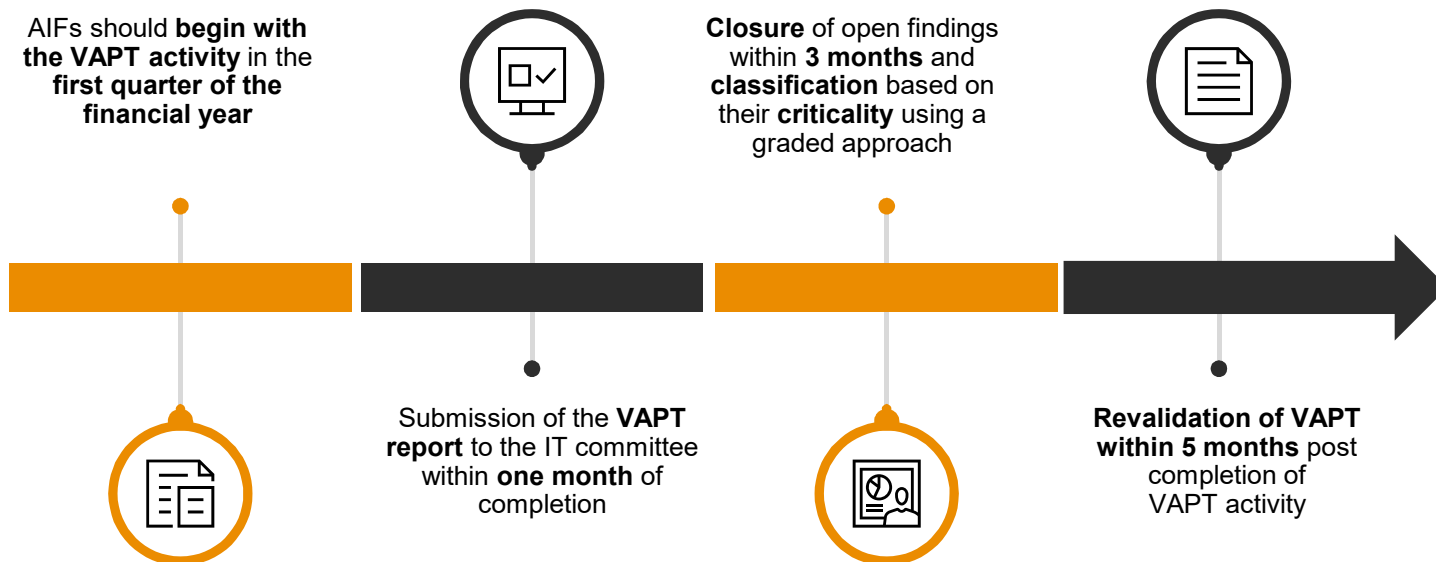
VAPT

- All **AIFs** need to **submit VAPT reports** to **SEBI** as per the format defined in the CSCRF.
- Along with the report, a **declaration** by the **MD/CEO** must also be submitted.
- Report of revalidation of the VAPT exercise and **open observations** must be placed before the respective IT committee for their confirmation and appropriate directions.
- If there are any **open vulnerabilities after 3 months of VAPT activity**, they shall be approved by the IT committee for REs and shall be **closed before the start of the next VAPT exercise**.
- **Maintain a risk register** and review it with the IT committee.

VAPT periodicity for REs

RE	Periodicity
REs which have been identified as 'protected systems' and/or critical information infrastructure (CII) by the National Critical Information Infrastructure Protection Centre (NCIIPC)	At least twice One VAPT activity shall be completed (including report submission, closure and revalidation) in each half of the financial year (April to September and October to March)
Rest of the REs	At least once VAPT activity shall commence in the first quarter of the financial year

Implementation timeline



Detailed scope of VAPT

The VAPT should provide in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks. The scope includes:

- vulnerability assessment of internal and external applications and infrastructure
- external penetration testing of applications and infrastructure
- Wi-Fi testing
- API security testing
- VA and PT of mobile applications
- network segmentation testing
- operating system and database assessment
- VAPT of cloud implementation
- configuration audit.

The testing methodology should be adapted from the NCIIPC, CERT-In Guidelines, NIST 800-115, ISO 27001:2022, Payment Card Industry Data Security Standard (PCI-DSS), Open-Source Security Testing Methodology Manual (OSSTMM) and Open Worldwide Application Security Project (OWASP) Testing Guide.

Cyber audit

A cyber audit pertains to the audit conducted for verifying compliance with the CSCRF. **Qualified REs** shall strive to **build an automated tool** and **suitable dashboards** (preferably integrated with log aggregator) for submitting compliance with the CSCRF.

The **dashboard** shall be **available at the time of cyber audit**. Along with the cyber audit report, SEBI REs shall also submit the required declaration from the MD/CEO.

REs shall ensure that no audit cycle shall be left unaudited (if any) due to the change in category in the beginning of the financial year. In all such cases, the unaudited period shall be included in the current audit cycle.

Cyber audit report submission and observations closure timeline

Cyber audit report submission

The **final cyber audit report shall be submitted** after approval from the respective IT committee for REs, within 1 month of completion of cyber audit.

Closure of findings identified during cyber audit

Within 3 months of cyber audit report submission, a graded approach (based on criticality of observations) shall be followed for closure of observations found during the cyber audit.

Follow-on audit

The follow-on audit shall be completed within 5 months of completion of the cyber audit.

REs categorised as self-certification shall be required to conduct only VAPT audit through a CERT-In empanelled IS auditing organisation and no other audit is required to be conducted.

Additionally, all open observations after 3 months of completion of a cyber audit shall be approved by the IT committee for REs and shall be closed before the start of the next audit exercise. The follow-on audit report and open observations must be placed before their respective IT committee for their confirmation and appropriate directions.

Cyber audit periodicity for REs

At least twice in a year

Qualified REs

At least twice in a year

Mid-size REs

At least once a year

Rest of the REs


Reporting authority for cyber audit report submission

Regulated entity

REs

Reporting authority

SEBI




The cyber audit shall cover 100% of the critical systems and 25% of the non-critical systems (chosen on a sample basis).

The scope of the audit includes:

- cybersecurity and cyber resilience policy
- asset inventory
- risk assessment and risk management
- supply chain risk management
- awareness and training
- data security
- Security continuous monitoring
- SOC efficacy
- incident management and response
- incident recovery planning.

Control-wise compliance with the CSCRF also needs to be documented in the audit report along with the gaps.



The activities below need to be conducted by the AIFs as per the give periodicity. Compliance with the same will be checked during the cyber audit.

Sr. no.	Standard/guidelines and clause	Applicability	Periodicity
1	Cyber resilience self-assessment using CCI (GV.OV.S4)	Qualified REs	Annually
2	Submission of CCI self-assessment evidence by Qualified REs (GV.OV.S4)	Qualified REs	Within 15 days of completion of CCI assessment (based on the applicability defined above in point 1 and 2)
3	REs Cybersecurity and cyber resilience policy review (GV.PO.S2)	All REs	Annually
4	REs Cybersecurity risk management policy (GV.PO.S4)	All REs	Annually
5	IT Committee for REs meeting periodicity (Guidelines for GV.PO Guideline 9)	All REs except small-size and self-certification Res	Quarterly
6	REs' risk assessment (threat-based) (ID.RA.S2)	Qualified, mid-size Res	Annually
7	User access rights, delegated access and unused tokens review (PR.AA.S5)	Qualified Res	Quarterly
		Other Res	Half-yearly
8	Review of privileged users' activities (PR.AA.S11)	Qualified REs	Quarterly
		Other Res	Half-yearly
9	Cybersecurity training program (PR.AT.S1)	All Res	Annually
10	Review of RE's systems managed by third-party service providers (GV.SC.S4)	Qualified REs	Half-yearly
		Other REs	Annually
11	Functional Efficacy of SOC (DE.CM.S1 – Guideline 4)	Qualified REs	Half-yearly
		Other REs who are utilising third-party managed SOC or market SOC services	Annually
12	Red Teaming exercise (DE.DP.S4)	Qualified REs	Half-yearly
13	Threat hunting (DE.DP.S5)	Qualified REs	Quarterly
14	Cybersecurity scenario-based drill exercise for testing adequacy and effectiveness of recovery plan (RC.RP.S3)	Qualified REs	Half-yearly
		Other Res	Annually
15	Review of periodically and update their contingency plan, continuity of operations plan (COOP) (RS.MA.S3)	Qualified REs	Half-yearly
		Mid-size and small-size REs	Annually
16	Evaluation of cyber resilience posture (EV.ST.S5)	Mid-size and Small-size Res	Annually

SOC

To enhance the cybersecurity posture of REs, the **CSCRF mandates** the establishment of an **SOC** for **all REs**, in accordance with its requirements.

The CSCRF allows REs to choose any one of the models below to utilise SOC services:



Small-size and **self-certification** REs are **mandated** to be on-boarded on the above-mentioned **market SOC**.

The **report** of the **functional efficacy of the market SOC** shall be provided by the SOC provider to **SEBI** on a periodic basis.

The timeline for setting-up of the SOC shall be **1 January 2025**.

CCI

The CCI is an index framework to rate the preparedness and resilience of the cybersecurity framework of qualified REs. These REs are directed to conduct self-assessment of their cyber resilience on an annual basis.

Index calculation methodology

- **The index is calculated based on 23 parameters.** These parameters have been given different weightages. More details are available in Annexure K of the CSCRF circular.
- **Evidence is to be submitted to SEBI** only on demand.
- **Qualified REs shall strive for building an automated tool and suitable dashboards.**
 - The dashboard shall be available at the time of cyber audit, onsite inspection/audit by SEBI or any agency appointed by SEBI.

Based on the value of the index, the cybersecurity maturity level of the qualified REs shall be determined as follows:

Sr. no.	Rating	Index score rating
1	Exceptional Cybersecurity Maturity	100-91
2	Optimal Cybersecurity Maturity	90-81
3	Manageable Cybersecurity Maturity	80-71
4	Developing Cybersecurity Maturity	70-61
5	Bare Minimum Cybersecurity Maturity	60-51
6	Fail	<=50 (The RE has scored below the cut-off in at least one domain/sub-domain.)

Auditor selection norms for VAPT and cyber audit

Auditors must mandatorily be CERT-In empaneled.

The auditor must have a minimum three years of experience in IT audit of banking and financial services, preferably in the securities market. The audit experience should have covered various cybersecurity frameworks and guidelines issued by SEBI. Auditing experience of ISO 27001 for an organisation will be an added advantage.

The auditor must have experience in/direct access to experienced resources in the areas covered under the CSCRf. It is recommended that resources have relevant industry recognized certifications, e.g. Certified Information Systems Auditor (CISA) from ISACA, Certified Information Securities Manager (CISM) from ISACA, GIAC Systems and Network Auditor (GSNA), Certified Information Systems Security Professional (CISSP) from the International Information Systems Security Certification Consortium, commonly known as (ISC)2.

The auditor shall have an information security management system (ISMS)/IT audit/governance frameworks and processes conforming to leading industry practices like Control Objectives for Information and Related Technology (COBIT).

The auditor must not have any conflict of interest in conducting a fair, objective and independent audit of the REs. It shall not have been engaged over the last two years in any consulting engagement with any departments/units of the RE being audited.

The auditor may not have any cases pending with its previous auditees which fall under SEBI's jurisdiction and point to its incompetence and/or unsuitability to perform the audit task.

The auditor must have experience of performing VAPT.

The auditor must compulsorily use only licensed tools.

The auditor must compulsorily enter into a non-disclosure agreement (NDA) with the auditee. Under no circumstances, the data sought during the review or the audit report should leave the jurisdiction of India.



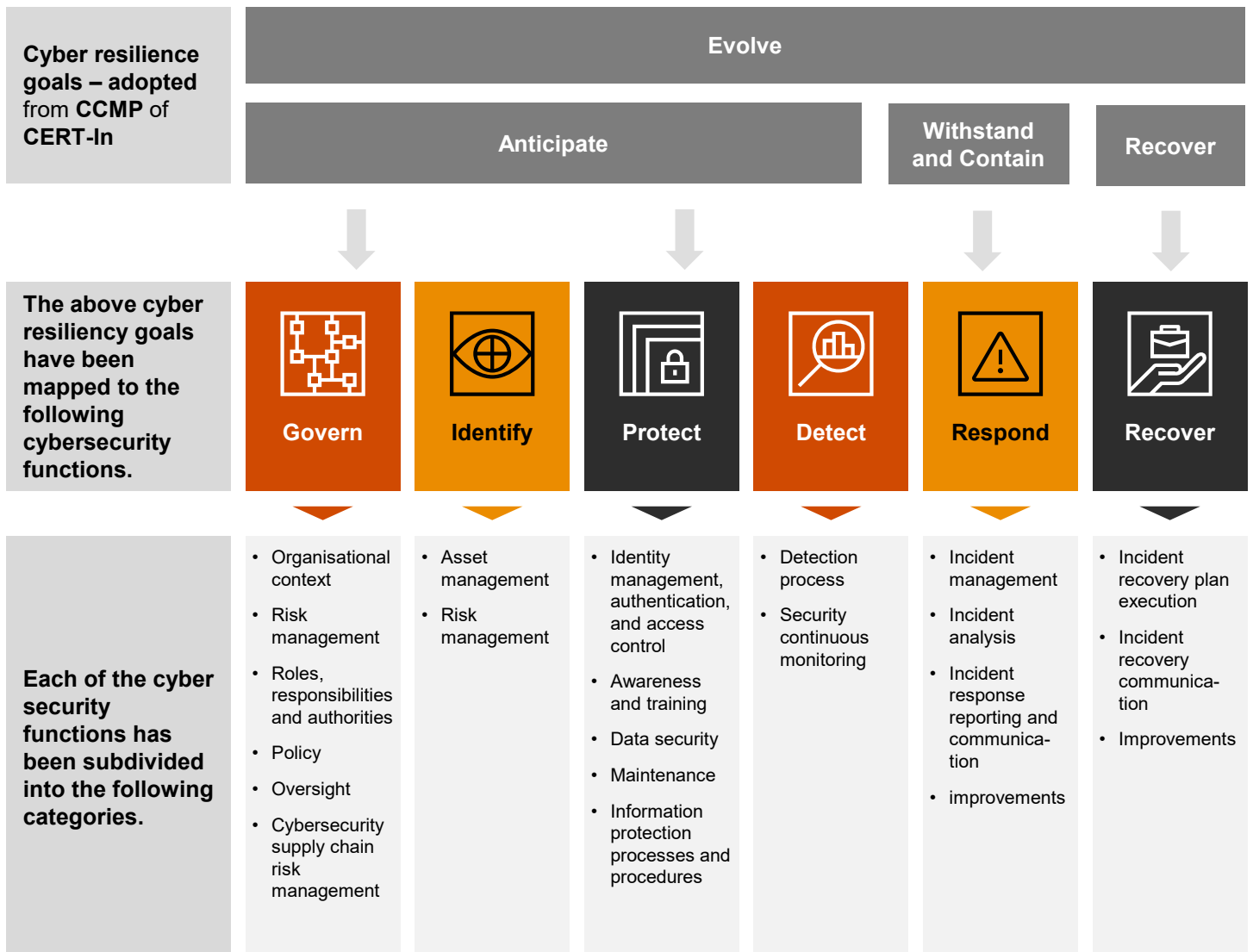


04

CSCRF controls

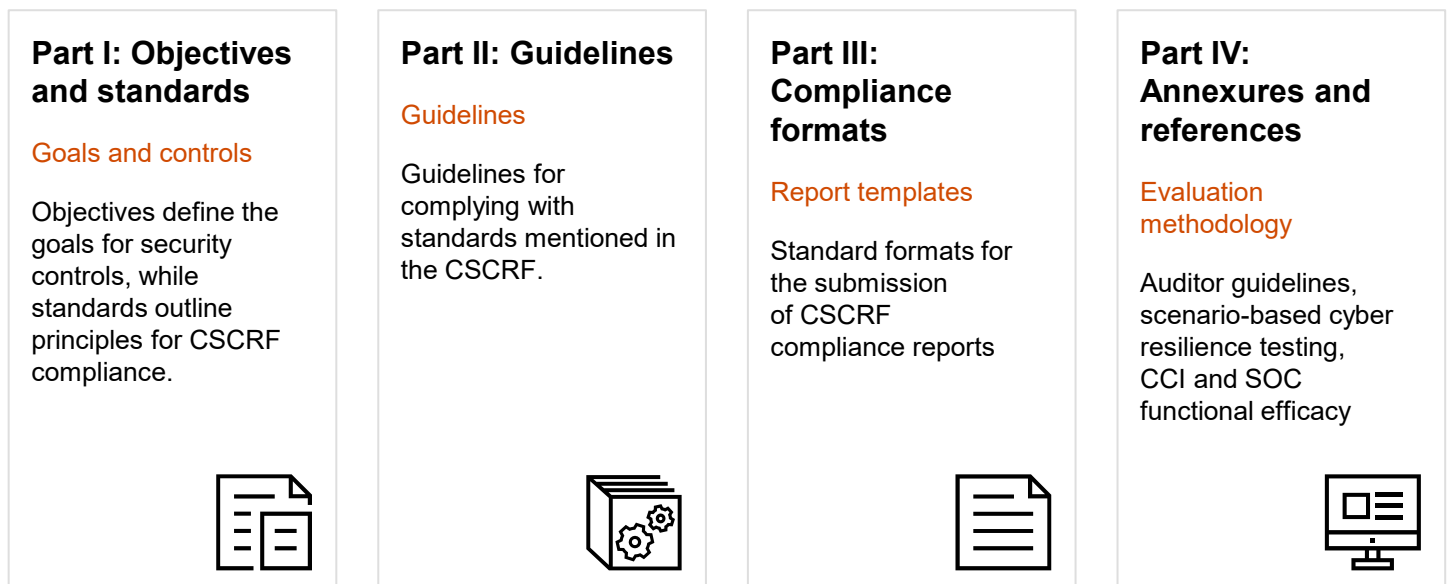
About the CSCRF

The CSCRF incorporates five cyber resiliency goals from CERT-In's Cyber Crisis Management Plan (CCMP): Anticipate, Withstand, Contain, Recover and Evolve. These goals align with the NIST's cybersecurity functions of Identify, Detect, Protect, Respond, Recover and Governance.



Structure of the CSCRF

The cyber resiliency goals cover different cybersecurity functions. These functions are to be implemented through various cybersecurity controls. The controls are divided into objectives, standards and guidelines.



Each of the REs, based on their categorisation, needs to implement the following set of controls mentioned in the subsequent pages:

Qualified REs

Mid-size REs

Small-size REs

Self-certification REs



Self-certified REs need to implement the following controls



Govern

- Comply with IT Act and Digital Personal Data Protection Act (DPDP)
- Conduct audits
- Use forensics
- Document a cybersecurity and cyber risk resiliency policy
- Document topic-wise policies
- Third-party risk management
- Maintain software bill of materials (SBOM) for existing critical systems
- Assign a designated officer



Identify

- Asset management
- Network architecture diagram
- Identify phishing websites
- Implement risk-based authentication solutions



Protect

- Use multi-factor authentication (MFA), intrusion prevention system (IPS) and anti-virus; ensure logging, monitoring and email security
- Implement physical and remote security, data management policies, and cybersecurity training
- Include tech issue and fraud reporting in apps; follow regulatory data protocols
- Apply secure design principles, harden hardware/software, and adopt defence-in-depth
- Conduct secure software development lifecycle (SSDLC), application security testing, VAPT, configuration audits, and patch management



Detect

- Use SOC services
- Conduct cybersecurity audits and VAPT
- Obtain SOC efficacy report



Respond

- Update and maintain a CCMP and Incident Response Plan
- Report cyber attacks to CERT-In, SEBI, or NCIIPC within 6 or 24 hours, and submit incident reports to SEBI.
- Set up communication channels
- Conduct root cause analysis and investigate alerts
- Collect and preserve data
- Analyze the incident's scope, cause, and impact
- Conduct compromise assessments
- Review and update the contingency plan
- Conduct training exercise



Recover

- Scenario-based classifications in recovery plans and timely restoration of affected systems
- Declare disaster within 30 minutes for critical systems
- Resume critical operations within 2 hours (RTO); recover data within 15 minutes (RPO)
- Regularly test and update plans, obtain IT Committee approval, and store backups off-site
- Business continuity plan-disaster recovery (BCP-DR) to match cyber resilience goals

Note: Please note that the controls outlined above are a summary of those detailed in the CSCRF circular. For comprehensive guidelines, refer to the full CSCRF for SEBI-regulated entities.

Small REs need to implement the following controls



Govern

- Comply with IT Act and DPDP
- Conduct audits
- Use forensics
- Document a cyber security and cyber risk resiliency policy
- Document topic-wise policies
- Third party risk management
- Maintain SBOM for existing critical systems
- Assign a designated officer



Identify

- Asset management
- Network architecture diagram
- Identify phishing websites
- Implement risk-based authentication solutions



Protect

- Use MFA, IPS, and anti-virus; ensure logging, monitoring, and email security
- Implement physical and remote security, data management policies, and cybersecurity training
- Include tech issue and fraud reporting in apps; follow regulatory data protocols
- Apply secure design principles, harden hardware/software, and adopt defense-in-depth
- Conduct secure SDLC, application security testing, VAPT, configuration audits, and patch management
- Application Security for Customer-Facing Apps
- Capacity Monitoring
- Conduct IS audits.



Detect

- Use SOC services
- Conduct cybersecurity audits and VAPT
- Obtain SOC efficacy report



Respond

- Update and maintain an CCMP and incident response plan
- Report cyberattacks to CERT-In, SEBI or NCIIPC within 6 or 24 hours, and submit incident reports to SEBI
- Set up communication channels
- Conduct root cause analysis and investigate alerts
- Collect and preserve data
- Analyse the incident's scope, cause and impact
- Conduct compromise assessments
- Conduct training exercise
- Review and update their contingency plan, continuity of operations (COOP), and training exercises



Recover

- Scenario-based classifications in recovery plans and timely restoration of affected systems
- Declare disaster within 30 minutes for critical systems
- Resume critical operations within 2 hours (recovery time objective); recover data within 15 minutes (recovery point objective)
- Regularly test and update plans, obtain IT committee approval and store backups off-site
- BCP-DR to match cyber resilience goals.

Note: Please note that the controls outlined above are a summary of those detailed in the CSCRF circular. For comprehensive guidelines, refer to the full CSCRF for SEBI-regulated entities.

Mid-size REs need to implement the following controls



Govern

- Comply with IT Act and DPDP; follow SEBI circulars on outsourcing
- Conduct audits, use forensics and document cybersecurity policies
- Manage third-party risks and maintain SBOM for critical systems
- Assign a cybersecurity officer, define roles and allocate a budget
- Build and train a cybersecurity team; manage HR and third-party security risks
- Apply Plan-Do-Check-Act; establish compliance management and an IT committee
- Follow best practices (ISO 27001), develop a risk management strategy and perform scenario-based testing



Identify

- Asset management
- Network architecture diagram
- Identify phishing websites
- Implement risk-based authentication solutions
- Use an Information Technology Service Management (ITSM) tool
- Integrate cybersecurity into product lifecycle
- Conduct risk assessments on a yearly basis



Protect

- Log and monitor systems; ensure physical, remote and email security
- Follow data policies, train on cybersecurity and implement access controls (Multifactor authentication, Role-based access control)
- Include tech issue reporting in apps; use secure design principles
- Harden hardware/software, apply secure SDLC and adopt defence-in-depth
- Perform security testing, manage patches and secure the network
- Use Endpoint Protection Platform, Endpoint Detection and Response, Extended Detection and Response (EPP, EDR, XDR), anti-malware, and Intrusion Prevention System (IPS/NG-IPS); secure Active Directory and restrict removable media
- Apply API, mobile app security, data encryption and Data Loss Prevention (DLP)
- Monitor capacity
- Change management
- Conduct audits and set a remote access policy





Detect

- Use SOC services
- Conduct cybersecurity audits and VAPT
- Obtain SOC efficacy report
- Capacity monitoring of network and systems
- Track and project IT asset usage
- Ensure adequate data storage, processing power, and bandwidth to meet performance and communication needs
- Capacity planning



Respond

- Update and maintain a incident response plan
- Report cyberattacks to CERT-In, SEBI or NCIIPC within 6 or 24 hours, and submit incident reports to SEBI
- Set up communication channels
- Conduct root cause analysis and investigate alerts
- Collect and preserve data
- Analyse the incident's scope, cause and impact
- Conduct compromise assessments
- Review and update the contingency plan
- Conduct training exercises
- Ensure timely and appropriate incident response
- Review and update their contingency plan and training exercises



Recover

- Scenario-based classifications in recovery plans and timely restoration of affected systems
- Declare disaster within 30 minutes for critical systems
- Resume critical operations within 2 hours (RTO); recover data within 15 minutes (RPO)
- Regularly test and update plans, obtain IT committee approval, and store backups off-site
- BCP-DR to match cyber resilience goals



Evolve

- Threat modelling
- Assess controls and practices for emerging threats
- Use mathematical models and machine learning to rapidly analyse data and make decisions
- Implement auditing/logging systems across different OS to capture and store data
- Apply varied audit/logging methods at different architectural layers
- Consider deploying multiple OS to prevent a single compromise from affecting all systems
- Maintain additional IT assets for storage, processing or communications

Note: Please note that the controls outlined above are a summary of those detailed in the CSCRF circular. For comprehensive guidelines, refer to the full CSCRF for SEBI-regulated entities.

Qualified REs need to implement the following controls



Govern

- Comply with IT Act and DPDP; follow SEBI circulars on outsourcing
- Conduct audits, use forensics and document cybersecurity policies
- Manage third-party risks and maintain SBOM for critical systems
- Assign a cybersecurity officer, define roles and allocate a budget
- Build and train a cybersecurity team; manage HR and third-party security risks
- Apply Plan-Do-Check-Act; establish compliance management and an IT committee
- Follow best practices (ISO 27001), develop a risk management strategy and perform scenario-based testing
- Designate a senior official as chief information security officer (CISO)
- Conduct self-assessment of their cyber resilience using CCI
- Check for third-party compliance with CSCRF



Identify

- Asset management
- Network architecture diagram
- Identify phishing websites
- Implement risk-based authentication solutions
- Use an ITSM tool
- Integrate cybersecurity into product lifecycle
- Conduct risk assessments on a yearly basis
- Implement threat intelligence, dark web monitoring and anti-phishing app services



Protect

- Log and monitor systems; ensure physical, remote and email security
- Follow data policies, train on cybersecurity and implement access controls (MFA, RBAC)
- Include tech issue reporting in apps; use secure design principles
- Harden hardware/software, apply secure SDLC and adopt defence-in-depth
- Perform security testing, manage patches and secure the network
- Use EPP, EDR, XDR, anti-malware and IPS/NG-IPS; secure AD and restrict removable media
- Apply API, mobile app security, data encryption and DLP
- Monitor capacity
- Change management
- Conduct audits and set a remote access policy
- Follow a zero-trust model, review access and tokens quarterly, and segregate environments
- Prepare SOPs for open-source and emerging tech and security, and adopt DevSecOps
- Maintain applications, build automated compliance tools and get ISO 27001 certified
- Follow CIS controls, review patch policies annually and ensure resources for updates
- Track patch compliance quarterly and apply patches to both production and DR sites as needed



Detect

- Use SOC services
- Conduct cybersecurity audits and VAPT
- Obtain SOC efficacy report
- Capacity monitoring of network and systems
- Track and project IT asset usage
- Ensure adequate data storage, processing power, and bandwidth to meet performance and communication needs
- Capacity planning
- Deploy solutions such as Breach and Attack Simulation (BAS), Continuous Automated Red Teaming (CART), decoy, vulnerability management, etc., to enhance their cybersecurity posture
- Review SOC efficacy every six months
- Conduct red teaming exercises as part of their cybersecurity framework on a half-yearly basis through use of red/ blue teams
- Deploy CART for continuous, automated security testing and visibility into attack surfaces
- Regularly search for hidden cyberthreats in the network
- Use threat intelligence, IOCs, IOAs, etc., to conduct threat hunting every quarter



Respond

- Update and maintain an CCMP and incident response plan
- Report cyberattacks to CERT-In, SEBI or NCIIPC within 6 or 24 hours, and submit incident reports to SEBI
- Set up communication channels
- Conduct root cause analysis and investigate alerts
- Collect and preserve data
- Analyse the incident's scope, cause, and impact
- Conduct compromise assessments
- Review and update the contingency plan
- Conduct training exercises
- Ensure timely and appropriate incident response
- Review and update their contingency plan and training exercises
- Collaborate with Cyber Swachhta Kendra (CSK) operated by CERT-In.
- Regularly update contact details for service providers, intermediaries and other stakeholders



Recover

- Scenario-based classifications in recovery plans and timely restoration of affected systems
- Declare disaster within 30 minutes for critical systems
- Resume critical operations within 2 hours (RTO); recover data within 15 minutes (RPO)
- Regularly test and update plans, obtain IT committee approval and store backups off-site
- BCP-DR to match cyber resilience goals
- Regularly updated 'golden images' of critical systems at offsite location
- Retain spare hardware in an isolated environment
- Create isolated, immutable backup
- Conduct regular business continuity drills
- Conduct scenario-based cyber resilience tests twice in a financial year (every 6 months)
- Regularly test and restore backup data
- Keep offline, encrypted backups and test them quarterly to ensure data confidentiality, integrity, and availability



Evolve

- Threat modelling
- Assess controls and practices for emerging threats
- Use mathematical models and machine learning to rapidly analyse data and make decisions
- Implement auditing/logging systems across different OS to capture and store data
- Apply varied audit/logging methods at different architectural layers
- Consider deploying multiple OS to prevent a single compromise from affecting all systems.
- Maintain additional IT assets for storage, processing or communications

Note: Please note that the controls outlined above are a summary of those detailed in the CSCRF circular. For comprehensive guidelines, refer to the full CSCRF for SEBI-regulated entities.

05

How PwC can help

PwC can support in setting up the CSCRf framework for your organisation along the following domains:




**CSCRf
implementation**

- CSCRf project management and governance
 - Setting up the IT committee
 - Categorisation of your company and implementing the CSCRf
- CSCRf controls implementation
- CSCRf readiness assessment




VAPT

- Support in conducting vulnerability assessment
- Support in conducting penetration testing
- Vulnerability management and remediation




Cyber audit

- Cyber audit preparedness



SOC

- Managed services for SOC operations
- Assisting in building your own SOC
- SOC advisory



ISO certification

- ISO/IEC 27001:2022 Certification
 - Support in ISO/IEC 27001:2022 readiness assessment
 - Support in ISO/IEC 27001:2022 implementation

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2024 PwC. All rights reserved.

Contact us

Siddharth Vishwanath

Partner, Risk Consulting
siddharth.vishwanath@pwc.com
+91 91671 90944

Dhruv Gupta

Director, Risk Consulting
dhruv.d.gupta@pwc.com
+91 98731 40503

Deepak Soni

Manager, Risk Consulting
deepakkumar.soni@pwc.com
+91 8320895892

Contributors:

Manasa Sanjeev

Anuja Sardesai

Editorial support:

Dion D'Souza

Design:

Praveen Pr

Vatsalya Jakheta

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2024 PricewaterhouseCoopers Private Limited. All rights reserved.

PR/September 2024-M&C 40869