Cyber Resilience goal: ANTICIPATE		
Cybersecurity control: IDENTIFY		
ID.AM: Guidelines		
ID.AM.S1, ID.AM.S4	1. All REs shall identify and classify *critical systems* as defined in this framework based on their sensitivity and criticality for business operations, services and data management. The Board/ Partners/ Proprietor of the REs shall approve the list of *critical systems*. 2. All REs shall maintain an up-to-date inventory of their (including but not limited to) hardware and systems, software, digital assets (such as URLs, domain names, application, APIs, etc.), shared resources (including cloud assets), interfacing systems (internal and external), details of its network resources, connections to its network and data flows. 3. Any additions/ deletions or changes in existing assets shall be reflected in the asset inventory within 3 working days. 4. For conducting criticality assessment of assets, REs shall take the following steps (including but not limited to): a. Maintain a comprehensive asset inventory b. Conduct threat modelling (based on risk assessment) c. Conduct vulnerability assessment 5. REs shall prepare and maintain an up-to-date network architecture diagram at the organisational level including wired and wireless networks.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	6. REs shall put in place configuration management database approach to: a. Understand and inventorise their IT assets - both logical (e.g., data, software) and physical (e.g., hardware). b. Understand which data or systems are most critical for providing critical services as well as any associated interdependencies.	MIIs (Mandatory)
ID.AM.S6	7. All IT assets shall be inventoried in ITSM tool. 8. REs shall integrate cybersecurity considerations into product life cycles.	All REs except small-size, self-certification REs (Mandatory)
ID.RA: Guidelines		
ID.RA.S1, ID.RA.S2	1. REs shall conduct a risk assessment (including post-quantum risks) of the IT environment of their organization on a half-yearly (for MIIs) and yearly (for qualified and mid-size REs) basis to acquire visibility and a reasonably accurate assessment of the overall cybersecurity risk posture. The above-mentioned risk assessment shall be utilized by the RE to develop a quantifiable cybersecurity risk score. 2. REs shall accordingly identify cyber risks[26] that they may face, along with the likelihood of associated threats and their impact on their business, and deploy controls commensurate to their criticality. 3. Risk Assessment shall include (but not limited to): a. Technology stack and solutions used b. Known vulnerabilities c. Dependence on third-party service providers d. Data storage, security and privacy protection	All REs except small-size, self-certification REs (Mandatory)

[26] Refer Definitions section for the Risk definition.

Standards	CSCRF guidelines	Applicability
	e. Threats, likelihoods and associated risks	
ID.RA.S3	1. REs shall engage Dark web monitoring (for brand intelligence, customer protection, etc.), and takedown services as a cyber-defence strategy to check for any brand abuse, data/credentials leak, combating cyber abuse etc. 2. REs shall subscribe to anti-phishing/ anti-rogue app services to mitigate potential phishing or impersonation attacks. 3. REs shall devise SOPs to implement the advisories issued by CERT-In, NCIIPC or any other government agency in their IT environment within a defined timeframe. 4. REs shall have processes in place to manage and incorporate IOAs/ IOCs/ malware alerts/ vulnerability alerts (received from CERT-In or NCIIPC (as applicable) or any other government agencies) in their systems. 5. REs shall be onboarded to CERT-In intelligence platform to receive the advisories for necessary action and implementation.	MIIs, Qualified REs (Mandatory)
	6. MIIs shall get onboarded to NCCC to generate necessary situational awareness of existing and potential cybersecurity threats, and enable timely information sharing for taking proactive, preventive, and protective actions by individual entities.	MIIs (Mandatory)
ID.RA.S4	1. <u>Measures against Phishing websites and attacks</u> a. REs need to proactively monitor the cyberspace to identify phishing websites w.r.t. REs' domains and report the same to CSIRT-Fin/CERT-In for taking appropriate action.	All REs (Mandatory)
	2. Risk assessment of authentication-based solutions shall be implemented to get insights about context behind every login. Further, when a user attempts to sign-in, risk-based	All REs

Standards	CSCRF guidelines	Applicability
	authentication solution shall analyse factors such as device, location, network, sensitivity, etc.