Standards	CSCRF guidelines	Applicability
	2. REs shall try to incorporate lessons learned from incidents reported (if any) by other REs.	
RC.IM.S2	1. RE's RTO shall be met for all interconnected systems and networks through capacity upgradations and periodic coordinated resilience testing. 2. Recovery plan shall be improved after analysing the learnings from periodic drills.	All REs (Mandatory)
Cyber Resilience goal: EVOLVE		
EV.ST: Guidelines		
EV.ST.S1, EV.ST.S2, EV.ST.S3	1. REs shall anticipate new attack vectors through threat modelling (based on risk assessment) and work to defend them. 2. REs shall strive for reducing their attack surfaces. 3. RE shall proactively examine controls, practices, and capabilities for prospective, emerging or potential threats. 4. RE shall proactively assess and take necessary actions with respect to its system's requirements, architecture, design, configuration, acquisition processes, or operational processes as a strategy for adaptation to the identified and prospective threats and vulnerabilities. 5. RE shall continuously improve upon the ability to quickly deploy and integrate existing and new services, both on-premises and in the cloud. 6. RE shall strive to rapidly correlate data using mathematical models and machine learning in order to make data-driven decisions. 7. REs shall use auditing/ logging systems on different OS to acquire and store audit/logging data.	All REs except small, self-certification REs

Standards	CSCRF guidelines	Applicability
	8. In order to include heterogeneity, apply different audit/logging regimes at different architectural layers. 9. REs shall look for feasibility of deploying diverse operating systems. Attack or compromise on one type of OS may not affect other OS deployed. 10. RE shall maintain extra capacity of IT assets for information storage, processing, or communications.	