Futurism

Level	Criteria	Regulatory Prescription	Remarks	Futurism Offering
Level 1	All UCBs	Level I control prescribed in Annex	In addition to the controls prescribed to the UCBs vide circular dated October 19, 2018, bank specific email domain with DMARC controls, two factor authentications for CBS etc., are salient controls prescribed	1. Email Domain 2. Anti-Phishing 3. DMARC 4. Anti-Malware 5. 2-Factor Authentication 6. Information Security Audit 7. Password Management
Level 2	All UCBs, which are sub-members of Centralized Payment Systems[1] (CPS) and satisfying at least one of the criteria given below: offers internet banking facility to its customers (either view or transaction based) provides Mobile Banking facility through application (Smart phone usage) is a direct Member of CTS/IMPS/UPI?	Level II controls given in Annex II, in addition to Level I controls.	Additional controls include Data Loss Prevention Strategy, Anti-Phishing, VA/PT of critical applications.	"Periodic Testing 1. VA/PT throughout all node 2. VA for DMZ at least once in every 6 months 3. PT shall be conducted at least once in year" "User Access Control/ Management 1. IAM 2. VPN 3. Encryption - e.g. Bit locker 4. PAM/PIM 5. FAM/FIM" "Authentication Framework for Customers 1. Password Management 2. 2 factor authentications 3. CA digital cert" "Anti-Phishing & Antimalware 1. Anti-Phishing 2. Anti-Malware 3. DMARC protection" Data Leak Protection (DLP) "Audit Logs 1. IAM 2. PAM"

Futurism

Level 3	UCBs having at least one of the criteria given below: Direct members of CPS having their own ATM Switch having SWIFT interface	Level III controls given in Annex III, in addition to Level I and II controls.	Additional controls include Advanced Real-time Threat Defense and Management, Risk based transaction monitoring[2]	"Network Management and Security 1. Real time systems, servers, network devices and endpoints 2. Firewall rules with the restrict access" "Secure Configuration 1. Disable Remote Desktop Protocol (RDP) on all critical systems. 2. Enable IP table to restrict access to the clients and servers in SWIFT and ATM Switch. 3. Ensure the software integrity of the ATM Switch/SWIFT related applications 4. Disable PowerShell in servers where not required and disable PowerShell in Desktop systems. 5. Restrict default shares including IPC$ share 6. (inter-process communication share)" "User Access Control 1. IAM, Strong Password policy, 2-Factor Authentication either with the in-house team managing the infrastructure or through the service provider if their infrastructure is hosted at a shared location at the service provider's end. 2. Active Directory or Endpoint management systems to whitelist/blacklist/restrict removable media use."

				"Advanced Real-time Threat Defense and Management 1. Build a robust defense 2. Implement whitelisting of internet websites / systems." "Maintenance, Monitoring, and Analysis of Audit Logs 1. IAM 2. PAM 3. Monitoring Tool 4. SIEM" "Incident Response and Management 1. BCP/DR 2. SIEM" "User / Employee/ Management Awareness 1. Security training & Awareness"
Level 4	UCBs which are members/ sub-members of CPS and satisfy at least one of the criteria given below: having their own ATM Switch and having SWIFT interface hosting data center or providing software support to other banks on their own or through their wholly owned subsidiaries	Level IV controls given in Annex IV, in addition to Level I, II and III controls	Additional controls include setting up of a Cyber Security Operation Center (C-SOC) (either on their own or through service providers), IT and IS Governance Framework	Arrangement for continuous surveillance - Setting up of Cyber Security Operation Centre (C-SOC) 1. Monitor, analyze and escalate security incidents 2. Develop Response - protect, detect, respond, recover 3. Conduct Incident Management and Forensic Analysis 4. Co-ordination with relevant stakeholders within the UCB/external agencies 5. Cost effective technology framework design & implement 6. Proactive Monitoring with risk assessment 7. SIEM with deep dive investigations security, deep packet inspection approaches

				8. Staffing of C-SOC - is it required to be 24x7x365, in shifts, business hours only, etc. 9. Model used - Finding staff with required skills /managed security service provider with required skill set 10. Metrics to measure performance of C-SOC 11. Ensuring scalability and continuity of staff through appropriate capacity planning initiatives 12. BCP/DR