		TIER ONE (1)		TIER TWO (2)		TIER THREE (3)		TIER FOUR (4)		TIER FIVE (5)	
		Banks, ARB Apex Bank, Apex Bank, DEMIs, PSP Scheme & Development Finance Institutions		Microfinance Banks (S&L, Finance Houses, MFCs, MCCs, Credit Union), Leasing Companies, PSP Enhanced, Virtual Asset Service Providers		Community Banks (RCBs), Digital Credit Service Providers		Last Mile Providers eg. (Cooperative Susu, Financial Co-operative Societies, MC Ent, FNGOs), FEBs		PSP Medium, PSPs Standards. PFTSP	
	PARAGRAPH	Key	Alternative/Comments	Key	Alternative/Comments	Key	Alternative/Comments	Key	Alternative/Comments	Key	Alternative/Comments
	PART I - PRELIMINARY MATTERS										
1	Objective	✓		✓		✓		✓		✓	
2	Applicability	✓		✓		✓		✓		✓	
3	Proportionality and Case-by-Case Assessment	✓		✓		✓		✓		✓	
4	Obligations of Regulated Entities	✓		!	An RFI may apply for exemption for 4(9)	!	An RFI may apply for exemption for 4(9)	✗		!	An RFI may apply for exemption for 4(9) and 4(10)
	PART II - GOVERNANCE										
5	The Board	✓		✓		✓	5 (3) Board Cyber and Information Security responsibilities shall be included in the Board Risk Committee charter.	✓	5 (3) Board Cyber and Information Security responsibilities shall be included in the Board charter.	✓	5 (3) Board Cyber and Information Security responsibilities shall be included in the Board charter.
6	The Senior Management	✓		✓		✓		✓		✓	
7	Internal Audits	✓		✓		✓		!	An RFI may outsource Cyber and Information Security internal audit responsibilities on case by case basis.	!	An RFI may outsource Cyber and Information Security internal audit responsibilities on case by case basis.
8	Information Security Department	✓		✓		!	An RFI may assign Information Security Department responsibilities to Risk Office/ Department or outsource on case by case basis.	!	An RFI may assign Information Security Department responsibilities to Risk Office/ Department or outsource on case by case basis.	!	An RFI may assign Information Security Department responsibilities to Risk Office/ Department or outsource on case by case basis.
9	Information Security Budget Management	✓		✓		!	An RFI may have a dedicated Information Security Budget on case by case basis.	!	An RFI may have a dedicated Information Security Budget on case by case basis.	!	An RFI may have a dedicated Information Security Budget on case by case basis.
	PART III - THE CHIEF INFORMATION SECURITY OFFICER										
10	Appointment	✓		✓		!	An RFI may assign CISO responsibilities to Risk Manager or outsource CISO function on case by case basis.	!	An RFI may outsource CISO function on case by case basis or apply for exemption.	!	An RFI may outsource CISO function on case by case basis or apply for exemption.
11	Status in the institutional Hierarchy	✓		✓		!	An RFI may assign CISO responsibilities to Risk Manager or outsource CISO function on case by case basis.	!	An RFI may outsource CISO function on case by case basis or apply for exemption.	!	An RFI may outsource CISO function on case by case basis or apply for exemption.
12	Responsibilities	✓		✓		!	An RFI may assign CISO responsibilities to Risk Manager or outsource CISO function on case by case basis.	!	An RFI may outsource CISO responsibilities on case by case basis or apply for exemption.	!	An RFI may outsource CISO responsibilities on case by case basis or apply for exemption.
	PART IV - CYBER AND INFORMATION SECURITY POLICY AND PROCEDURES										
13	Policy	✓		✓		!	RFIs shall develop broad policies to cover the requirements of cyber security risk management.	!	RFIs shall develop broad policies to cover the requirements of cyber security risk management.	!	RFIs shall develop broad policies to cover the requirements of cyber security risk management.
14	Procedures	✓		✓		!	RFIs shall develop broad procedures to cover the requirements of cyber security risk management.	!	RFIs shall develop broad procedures to cover the requirements of cyber security risk management.	!	RFIs shall develop broad procedures to cover the requirements of cyber security risk management.
15	The Cyber and Information Security Risk Management Committee	✓		✓		!	13 (3) The Committee member shall include MD, Risk Manager (CISO), IT Manager and any senior management member.	✗		!	13(3) The Committee resposibilities may be assigned to the MD on case by case basis
	PART V - CYBER AND INFORMATION SECURITY RISK MANAGEMENT										
16	Risk Management	✓		✓		✓		✓		✓	
17	Risk Identification	✓		✓		✓		✓		✓	
18	Risk Analysis	✓		✓		✓		✓		✓	
19	Risk Assessments in Cloud Environment	✓		✓		✓		✓		✓	
20	Risk Mitigation	✓		✓		✓		✓		✓	
21	Risk Evaluation	✓		✓		✓		✓		✓	
22	Risk Monitoring and Reporting	✓		✓		✓		✓		✓	
	PART VI - ASSET MANAGEMENT										
23	Inventory	✓		✓		✓		✓		✓	
24	Ownership	✓		✓		✓		✓		✓	
25	Acceptable Use	✓		✓		✓		✓		✓	
26	Asset Mapping and Classification	✓		✓		✓		✓		✓	
	PART VII - CYBER DEFENCE										
27	Security Infrastructure	✓		✓		✓		✓		✓	
28	Architecture	✓		✓		✓		✓		✓	
29	Network Elements	✓		✓		✓		✓		✓	
30	Network Management	✓		✓		!	An RFI may implement Network Management based on risk profile	!	An RFI may implement Network Management based on risk profile	!	An RFI may implement Network Management based on risk profile
31	Encryption	✓		✓		✓		✓		✓	
32	Media Encryption	✓		✓		✓		✓		✓	
33	Remote Access	✓		✓		✓		✓		✓	

		TIER ONE (1)		TIER TWO (2)		TIER THREE (3)		TIER FOUR (4)		TIER FIVE (5)	
		Banks, ARB Apex Bank, Apex Bank, DEMIs, PSP Scheme & Development Finance Institutions		Microfinance Banks (S&L, Finance Houses, MFCs, MCCs, Credit Union), Leasing Companies, PSP Enhanced, Virtual Asset Service Providers		Community Banks (RCBs), Digital Credit Service Providers		Last Mile Providers eg. (Cooperative Susu, Financial Co-operative Societies, MC Ent, FNGOs), FEBs		PSP Medium, PSPs Standards. PFTSP	
	PARAGRAPH	Key	Alternative/Comments	Key	Alternative/Comments	Key	Alternative/Comments	Key	Alternative/Comments	Key	Alternative/Comments
34	Internet Access	✓		✓		✓		!	An RFI may apply for exemption from 2 (a) (i), (ii), (iii) and 2 (b)	✓	
35	Websites and Web Applications Protection	✓		✓		✓		✓		✓	
36	Access Control and Authentication	✓		✓		✓		✓		✓	
37	Biometric Authentication	✓		✓		✓		✓		✓	
38	Compartmentalisation and Permissions	✓		✓		✓		✓		✓	
39	Servers and Workstations	✓		✓		✓		✓		✓	
40	Databases	✓		✓		✓		✓		✓	
41	Software Information Security	✓		✓		✓		✓		✓	
42	Application Programming Interface (API)	✓		✓		✓		✓		✓	
43	Auditing	✓		✓		✓		✓		✓	
44	Incident Preparedness	✓		✓		✓		✓		✓	
45	Cyber Intelligence and Research	✓		✓		✓		✗		✓	
	PART VIII - CYBER RESPONSE										
46	Structure and Hierarchy	✓		✓		!	In addition to the proportionality provisons for the CISO, an RFI shall include the cyber response function in the CISO's terms of reference.	✗		!	In addition to the proportionality provisons for the CISO, an RFI shall include the cyber response function in the CISO's terms of reference.
47	Security Information and Event Management (SIEM)	✓		✓		✓		!	An RFI shall implement alternate mechanisms to monitor system logs	✓	
48	Security Operations Centre (SOC)	✓		✓		✓		!	An RFI shall implement mechanisms for monitoring cyber and information security alerts and incidents	✓	
49	Methodology	✓		✓		✓		✗		✓	
50	Incident Handling	✓		✓		✓		✗		✓	
51	Reporting to the BoG	✓		✓		✓		✓		✓	
52	Managed Security Service Provider (MSSP)	✓		✓		✓		✓		✓	
	PART IX - HUMAN RESOURCE SECURITY, ACCESS CONTROL AND CYBER COMPETENCY FRAMEWORK										
53	Access Control	✓		✓		✓		✓		✓	
54	Hiring and Onboarding	✓		✓		✓		✓		✓	
55	New Employee	✓		✓		✓		✓		✓	
56	Sensitive Positions	✓		✓		✓		✓		✓	
57	Employee Lifecycle	✓		✓		✓		✓		✓	
58	Termination	✓		✓		✓		✓		✓	
59	Cyber Education	✓		✓		✓		✓		✓	
60	Cyber Exercise	✓		✓		✓		✓		✓	
61	Artificial Intelligence (AI) and Machine Learning (ML)	✓		✓		✓		✓		✓	
	PART X - CHANNELS OF COMMUNICATION WITH EXTERNAL ENTITIES										
62	Data Transfer between Sites and Organisations	✓		✓		✓		✓		✓	
63	Email	✓		✓		✓		✓		✓	
64	Web Access	✓		✓		✓		✓		✓	
65	Bring Your Own Device (BYOD)	✓		✓		✓		✓		✓	
66	Institutional mobile device	✓		✓		✓		✓		✓	
	PART XI - ELECTRONIC BANKING PLATFORMS										
67	General Controls	✓		✓		✓		✓		✓	
68	Subscribing to Electronic Banking Platforms	✓		✓		✓		✓		✓	
69	Identification and Authentication	✓		✓		✓		✓		✓	
70	Website	✓		✓		✓		✓		✓	
71	Mobile Applications	✓		✓		✓		✓		✓	
72	Email	✓		✓		✓		✓		✓	
73	Telephony Services	✓		✓		✓		✓		✓	
74	Customer Security	✓		✓		✓		✓		✓	
75	Passwords and Password Management	✓		✓		✓		✓		✓	
	PART XII - EXTERNAL CONNECTIONS										
76	Direct Connectivity	✓		✓		✓		✓		✓	
77	Other Financial and non-RFIs	✓		✓		✓		✓		✓	
78	Business Partners	✓		✓		✓		✓		✓	
79	Remote Access	✓		✓		✓		✓		✓	
80	External Parties	✓		✓		✓		✓		✓	
81	Data in Motion	✓		✓		✓		✓		✓	
	PART XIII - CLOUD SERVICES										
82	Corporate Governance	✓		✓		✓		✓		✓	
83	Risk Management	✓		✓		✓		✓		✓	
84	The Cloud Computing Service Contract	✓		✓		✓		✓		✓	
85	Institutional Application Development	✓		✓		✓		✓		✓	
86	Promotional Material	✓		✓		✓		✓		✓	
87	Cloud Operations, Monitoring and Resilience	✓		✓		!	An RFI may apply for exemption on a case by case basis	!	An RFI may apply for exemption on a case by case basis	!	An RFI may apply for exemption on a case by case basis

		TIER ONE (1)		TIER TWO (2)		TIER THREE (3)		TIER FOUR (4)		TIER FIVE (5)	
		Banks, ARB Apex Bank, Apex Bank, DEMIs, PSP Scheme & Development Finance Institutions		Microfinance Banks (S&L, Finance Houses, MFCs, MCCs, Credit Union), Leasing Companies, PSP Enhanced, Virtual Asset Service Providers		Community Banks (RCBs), Digital Credit Service Providers		Last Mile Providers eg. (Cooperative Susu, Financial Co-operative Societies, MC Ent, FNGOs), FEBs		PSP Medium, PSPs Standards. PFTSP	
	PARAGRAPH	Key	Alternative/Comments	Key	Alternative/Comments	Key	Alternative/Comments	Key	Alternative/Comments	Key	Alternative/Comments
88	Cloud Security Controls and Assurance	✓		✓		!	An RFI may apply for exemption on a case by case basis	!	An RFI may apply for exemption on a case by case basis	!	An RFI may apply for exemption on a case by case basis
	PART XIV - RFIs WITH INTERNATIONAL AFFILIATION										
89	Foreign RFIs in Ghana	✓		✓		✗		✗		✗	
90	Ghanaian RFIs Operating Abroad	✓		✓		✓		✓		✓	
	PART XV - PHYSICAL SECURITY										
91	General	✓		✓		✓		✓		✓	
92	Secured Zones	✓		✓		✓		✓		✓	
93	Segmentation	✓		✓		✓		✓		✓	
94	Physical Security of Hardware and Other Equipment	✓		✓		✓		✓		✓	
	PART XVI - CONTRACTUAL ASPECTS										
95	Cyber Security Contracts	✓		✓		✓		✓		✓	
96	Supply Chain Cyber Security Contracts Obligation	✓		✓		✓		✓		✓	
97	Contracts Involving AI, ML or Algorithmic Services	✓		✓		✓		✓		✓	
	PART XVII - DIGITAL INNOVATIONS										
98	General	✓		✓		✓		✓		✓	
99	Data Privacy and Confidentiality Requirements	✓		✓		✓		✓		✓	
100	AI/ML Governance and Security	✓		✓		✓		✓		✓	
	PART XVIII - DATA CENTRE MANAGEMENT										
101	Governance & Operations	✓		✓		✓		✓		✓	
102	Business Continuity & Recovery	✓		✓		✓		✓		✓	
103	Site & External Risk	✓		✓		✓		✓		✓	
104	Power & Energy	✓		✓		✓		✓		✓	
105	Cooling & Environmental Control	✓		✓		✓		✓		✓	
106	Fire Protection	✓		✓		✓		✓		✓	
107	Cabling & Connectivity	✓		✓		✓		✓		✓	
108	Physical Security	✓		✓		✓		✓		✓	
109	Segregation	✓		✓		✓		✓		✓	
110	Monitoring & Incident Response	✓		✓		✓		✓		✓	
111	Contracts & SLAs	✓		✓		✓		✓		✓	
112	Vulnerability & Maintenance of Facility Systems	✓		✓		✓		✓		✓	
113	Colocation	✓		✓		✓		✓		✓	
	PART XIX - CYBERSECURITY REQUIREMENTS FOR ARTIFICIAL INTELLIGENCE (AI) SYSTEMS										
114	General Principles	✓		✓		✓		✓		✓	
115	Reporting and Notification	✓		✓		✓		✓		✓	
	PART XX - CYBER AND INFORMATION SECURITY TESTING AND EXERCISE REGIME										
116	Vulnerability Assessment	✓		✓		✓		✓		✓	
117	Configuration Compliance Scanning	✓		✓		✓		✓		✓	
118	Patch and Configuration Compliance Validation	✓		✓		✓		✓		✓	
119	Web Application and API Testing (DAST/SAST)	✓		✓		✓		✓		✓	
120	Penetration Testing	✓		✓		✓		✓		✓	
121	Red Team Exercises and Adversarial Simulation	✓		✓		✓		✓		✓	
122	AI and ML Model-Specific Testing	✓		✓		✓		✓		✓	
123	Incident Response Plan Testing and Drills	✓		✓		✓		✓		✓	
124	Business Continuity and Disaster Recovery Testing (Including Cloud)	✓		✓		✓		✓		✓	
125	Call Centre and Telephony Security Testing	✓		✓		✓		✓		✓	
126	User Access Reviews	✓		✓		✓		✓		✓	
127	Asset Inventory Review	✓		✓		✓		✓		✓	
128	Third-Party Security Assessment	✓		✓		✓		✓		✓	
129	Physical Security Control Testing	✓		✓		✓		✓		✓	

Legend	
Key	**Description**
✓	**Full Implementation:** RFI ahall fully comply with all provisions in the paragraph
!	**Partial Implementation:** RFI shall fully comply with the alternative controls or apply for an exemption
✗	**Not Applicable**