FREE STARTER PACK

The BoG CISD 2026 Starter Pack

Bank of Ghana's March 2026 Cyber and Information Security Directive, turned into 58 controls you can assess, assign and evidence. Each one has its paragraph reference, the evidence a reviewer will expect and the matching ISO 27001 control.

Free, and no email required. Checked against the official March 2026 directive on 17 November 2026.

In Assurelo GRC the Directive is tracked paragraph by paragraph (160 rows). **Download the map** from these 58 controls to those rows.

WHAT'S INSIDE

Everything you need to start a CISD programme.

The directive applies to every institution Bank of Ghana regulates: banks, specialised deposit-taking institutions, payment service providers, forex bureaus, virtual asset service providers and others. Use this pack to see where you stand before your next BoG review.

1

Control list

58 controls across Parts I to XX and the annexures, each with the paragraph reference, expected evidence and ISO 27001:2022 mapping.

2

Reporting calendar

Every deadline in one place: immediate notifications, the monthly return by the 15th, quarterly Board reports and more.

3

Approvals tracker

What needs Board approval and what needs Bank of Ghana's prior approval, before you act.

4

Testing by tier

Annexure H testing frequencies for Tier 1 and 2, Tier 3, and Tier 4 and 5 institutions.

THE HEADLINE CHANGE

ISO 27001 certification is now a requirement for most institutions.

Paragraph 4(9) requires ISO/IEC 27001 certification and adoption of ISO/IEC 27032. Annexure A makes this mandatory for Tier 1 (banks, ARB Apex Bank, DEMIs, PSP Scheme operators, development finance institutions); Tiers 2, 3 and 5 may apply to the Bank for an exemption, and paragraph 4 does not apply to Tier 4. Card-handling institutions and their agents must also be PCI DSS certified (paragraph 4(10)); Tier 5 may apply for an exemption from that too. Certification takes months, not weeks, so plan the certification audit into your timetable now.

Proportionality: the directive applies in proportion to your size, complexity and risk (paragraph 3 and Annexure A). You assess your profile; Bank of Ghana makes the final classification. Some controls and testing frequencies depend on your tier.

REPORTING CALENDAR

Every CISD deadline, in order.

When	What	Reference
Immediately	Significant or suspected incidents, and the trigger events in paragraph 50, to Bank of Ghana. Significant incidents to the Board.	Para 5(7), 6(10), 50
Monthly, by the 15th	Incident report to Bank of Ghana covering the previous month. A NIL report if nothing happened.	Para 50
Quarterly	Board report on incidents and KPIs. Risk Management Committee meeting. Unit-level readiness exercise. Assessment of high-risk and internet-facing systems.	Para 5(6), 12(9), 15, 17(7)
Quarterly (RFIs using AI/ML)	AI/ML inventory summary and model incidents in the quarterly report to Bank of Ghana.	Para 115
Twice a year	Senior Management effectiveness review. Committee report to the Board Committee. Access review of critical systems.	Para 6, 15, Annexure H
Annually	Internal audit of cyber, including backup and recovery. Institution-wide exercise. Board discussion of policy adequacy. CISO annual report, work plan and budget. Asset register review. DR testing.	Para 5, 7, 12, Annexure H
Every two years	Review of the cyber policies. Repeat cloud provider due diligence.	Para 6, 13(2), 83
Within seven days of an	Committee debrief started immediately and completed.	Para 15(3)(b)

incident		
Within six months of a finding	Maximum repair time for assessment findings, unless Senior Management and the Board are notified.	Para 17(9)

APPROVALS TRACKER

Get approval before you act.

Several decisions need Board approval, and some need Bank of Ghana's prior approval. Starting without it is a common finding.

Decision	Approval needed	Reference
Appointing the CISO	Board appoints; Bank of Ghana gives prior written approval	Para 10
Moving to cloud services	Board preliminary approval; Bank of Ghana approval	Para 82
Engaging a managed security service provider	Formal risk assessment; Board approval; Bank of Ghana prior approval; CSA-accredited provider	Para 51, Annexure B
Adopting digital innovations (blockchain, AI, virtual assets, quantum, robotics)	Board preliminary approval before implementation	Para 98
Cyber strategy, policies, work plans and budget	Board approval	Para 5
Risk Management Committee composition and terms of reference	Board approval	Para 15(1)
Proportionality tier	Bank of Ghana makes the final classification	Para 3(3)

ANNEXURE H

Minimum testing frequency by tier.

Test	Tier 1 and 2	Tier 3	Tier 4 and 5
Vulnerability assessment	Monthly automated scanning, quarterly manual validation	Quarterly automated scanning, semi-annual manual validation	Semi-annual automated scanning
Web application testing (DAST/SAST)	Continuous for critical apps; quarterly for others	Quarterly for critical apps; semi-annual for others	Semi-annual for all apps
Penetration testing	Twice a year, internal and external	Annually, internal and external	Annually, external only

Red team or adversary simulation	Annually	Every two years	Every three years or as directed
Control effectiveness and configuration review	Semi-annually	Annually	Annually
Third-party security assessment	Annually for critical vendors	Annually for critical vendors	Every two years for key vendors
Patch and configuration compliance validation	Monthly	Quarterly	Semi-annual
Configuration compliance scanning (CIS/NIST)	Quarterly	Quarterly	Quarterly
Disaster recovery and failover testing	Annually	Annually	Annually
User access review (critical systems)	At least twice a year	At least twice a year	At least twice a year
Asset register review	Annually	Annually	Annually

Who can test: testing, monitoring and compliance assessment are cybersecurity services under Ghana's Cybersecurity Act, 2020 (Act 1038), so providers need a Cyber Security Authority licence. Ask for it before you sign.

THE CONTROL LIST

58 controls, from governance to testing.

Requirements are paraphrased summaries, not the directive's text. The CSV version adds status, owner and notes columns so you can use it as your gap assessment.

ID	Reference	Requirement	Expected evidence	ISO 27001
PART I				
CISD-01	Para 4(9)	Hold ISO/IEC 27001 certification and adopt ISO/IEC 27032 (Tier 1 must; Tiers 2, 3 and 5 may apply for an exemption; not Tier 4).	Current ISO 27001 certificate and scope statement; record showing how ISO 27032 guidance is adopted	Clauses 4 to 10 (whole ISMS)
CISD-02	Para 4(10)	Be PCI DSS certified where the RFI or its agents handle, process, store or transmit card data (debit, credit, prepaid, e-purse, ATM, POS).	PCI DSS attestation of compliance for the RFI and for card-handling agents	A.5.31, A.5.36

CISD-03	Para 4(11)	Follow an internationally recognised method (NIST or ISO) for managing and handling security events.	Incident management procedure that names the method it follows	A.5.24 to A.5.28
CISD-04	Para 4(12)	Carry out due diligence on third-party providers and suppliers against the directive's standards.	Supplier due diligence records and risk ratings	A.5.19 to A.5.22
CISD-05	Para 3, Annexure A	Assess your cyber risk profile to determine which provisions apply. Bank of Ghana makes the final classification.	Proportionality self-assessment; BoG confirmation of tier	Clauses 4.1 to 4.3
PART II				
CISD-06	Para 5(3)	Appoint a Board Committee on cyber and information security risks with a charter. At least one Board member must have verifiable cyber risk qualifications or expertise.	Committee charter; appointment minutes; member qualifications on file	Clauses 5.1, 5.3
CISD-07	Para 5(1), 5(2)	The Board approves the cyber risk strategy and the policies for security, access and authentication, outsourcing, survivability, backup, recovery and disaster events.	Board minutes; approved strategy and policy set with version history	Clause 5.2, A.5.1
CISD-08	Para 5(4), 5(5)	The Board approves the annual cyber, business continuity and disaster recovery work plans and the annual cyber budget.	Approved work plans and budget	Clauses 6.2, 7.1
CISD-09	Para 5(6), 5(7)	The Board receives quarterly reports on all incidents and cyber KPIs, and immediate reports on significant incidents.	Quarterly Board packs; significant-incident notifications to the Board	Clauses 9.1, 9.3
CISD-10	Para 5(8), 5(11)	The Board holds an annual discussion on the adequacy of cyber policies and strategy, and approves new cyber-related products and services.	Annual Board minutes; approval records for new products	Clause 9.3
CISD-11	Para 6	Senior Management reviews the cyber policies at least every two years, meets at least twice a year to review effectiveness, receives quarterly reports and appoints the Risk Management Committee.	Policy review log; minutes of the twice-yearly reviews; quarterly reports	Clauses 5.1, 9.3, A.5.1
CISD-12	Para 6(10)	Report all significant and suspected incidents to Bank of Ghana immediately.	Notification records with timestamps	A.5.5, A.5.26
CISD-13	Para 6(11)	Prepare a due diligence report before appointing an ICT outsourcing	Due diligence report signed off before contract	A.5.19, A.5.21

		provider.		
CISD-14	Para 7(1) to 7(4)	An independent internal unit audits cyber and information security at least annually (or per the risk-based plan), including survivability, backup and recovery.	Audit charter; annual audit plan; audit reports	Clause 9.2, A.5.35
CISD-15	Para 7(5) to 7(8)	Report findings to the Board and Senior Management, validate any outsourced audit findings internally, and track issues with escalation.	Findings tracker with owners, dates and escalations; minutes discussing audit reports	Clause 10.2
CISD-16	Para 8, 9	Run a dedicated Information Security Department led by the CISO, with a cyber budget that is separate from the IT budget.	Organisation chart; budget showing a separate security line	Clauses 5.3, 7.1
PART III				
CISD-17	Para 10	The Board appoints a competent CISO with Bank of Ghana's prior written approval. The CISO holds no conflicting role.	BoG approval letter; CISO CV and qualifications; role description	Clause 5.3, A.5.2, A.5.3
CISD-18	Para 11	The CISO is part of Senior Management, reports directly to the MD/CEO and has unfettered access to the Board.	Organisation chart; reporting line in the job description	Clause 5.3
CISD-19	Para 12(9)	Run readiness exercises: at least quarterly for one or more units, and once a year for the whole institution.	Exercise plans, reports and lessons learned	A.5.24, A.5.29, A.5.30
CISD-20	Para 12(13)	Form a Cyber Incident Response Team able to handle the full incident lifecycle.	CIRT charter, roster and contact list	A.5.24, A.5.26
CISD-21	Para 12(15), 12(17), 12(18)	Maintain security metrics, an annual work plan and an annual CISO report to Senior Management and the Board.	KPI dashboard; annual work plan; annual CISO report	Clause 9.1
PART IV				
CISD-22	Para 13(1), 13(2)	Keep a Board-approved cyber policy covering the threat environment, risk approach, principles and change management, aligned with the ISO/IEC 27000 family. Review it at least every two years.	Approved policy with review history	A.5.1
CISD-23	Para 13(3) to 13(5)	Senior Management writes a framework document setting objectives, the structure of responsibilities and the risk	Framework document	Clauses 4.4, 5.3, 6.1

		assessment method.		
CISD-24	Para 14	Senior Management approves detailed procedures, checks they are followed and reviews them annually.	Approved procedures; compliance checks; annual review record	A.5.37, A.5.36
CISD-25	Para 15	Set up the Cyber and Information Security Risk Management Committee: at least three members, chaired by the CEO/MD, including the CRO, CIO/CTO and CISO. It meets at least quarterly and reports to the Board Committee at least twice a year. Incident debriefs start immediately and finish within seven days.	Board-approved terms of reference; quarterly minutes; debrief reports	Clause 5.3, A.5.27
PART V				
CISD-26	Para 16(1) to 16(3)	Integrate cyber risk into enterprise risk management, including AI and ML risks, alongside operational, continuity and ICT risk.	ERM framework; risk register with cyber and AI entries	Clauses 6.1.2, 8.2
CISD-27	Para 16(6)	Map supply chain dependencies, including indirect and tier-n suppliers and concentration risk.	Dependency map; concentration analysis	A.5.19 to A.5.22
CISD-28	Para 16(8)	Evaluate the need for cyber insurance through a formal risk assessment, and review any policy periodically.	Insurance evaluation memo; policy review record	Clause 6.1.3
CISD-29	Para 17(6), 17(7)	Assess critical systems at least yearly. Systems that are high risk, internet-facing, communicate externally or use a WAN are assessed at least quarterly.	Assessment schedule; test reports	A.8.8, A.8.29
CISD-30	Para 17(8), 17(9)	The Committee sets a remediation schedule for findings. The maximum repair time is six months; anything longer must be notified to Senior Management and the Board.	Remediation tracker showing due dates within six months	Clause 10.2
CISD-31	Para 17(10)	Security-assess every new, significantly changed, repaired, outsourced or cloud system before it goes into production.	Pre-production security sign-offs	A.8.25, A.8.29, A.8.32
PART VI				
CISD-32	Para 23 to 26, Annexure H	Keep an asset inventory with owners, acceptable use rules and classification, and review the register at least annually.	Asset register; classification scheme; annual review record	A.5.9, A.5.10, A.5.12

PART VII				
CISD-33	Para 27 to 30	Maintain a layered security infrastructure, architecture and network management.	Architecture diagrams; network security standards	A.8.20 to A.8.22
CISD-34	Para 31, 32	Encrypt data and media in line with the directive.	Cryptography standard; key management records	A.8.24
CISD-35	Para 33, 36 to 38	Control remote access, authentication (including biometrics) and permissions.	Access control policy; MFA configuration; permission matrices	A.5.15 to A.5.18, A.8.2, A.8.5
CISD-36	Para 35, 39 to 42	Protect websites, web applications, servers, workstations, databases, software and APIs.	Hardening standards; secure development records; API security tests	A.8.9, A.8.25 to A.8.28
CISD-37	Para 43 to 45	Log and audit security events, prepare for incidents and maintain cyber intelligence.	Logging standard; threat intelligence sources and reports	A.5.7, A.8.15, A.8.16
PART VIII				
CISD-38	Para 46 to 48	Operate a SIEM and a Security Operations Centre with a clear structure.	SOC operating model; SIEM use cases and coverage	A.8.16, A.5.25
CISD-39	Para 49	Keep formal incident procedures, including forensic study and lessons learned after every incident.	Incident procedure; incident records; post-incident reviews	A.5.24 to A.5.28
CISD-40	Para 50	Keep a post-incident plan for notifying regulators, customers, providers and law enforcement. Send the monthly incident report to BoG by the 15th, and a NIL report when there were no incidents.	Post-incident plan; monthly returns with submission proof	A.5.5, A.5.24
CISD-41	Para 50	Notify BoG immediately of: integrity damage; production systems holding sensitive data down for over three hours (unplanned); customer data leaked; significant attack attempts or central system collapse; essential services stopped for one business day or more; other significant events.	Notification decision log; ad-hoc reports as the incident starts, unfolds and ends	A.5.26
CISD-42	Para 51, Annexure B	Before using a managed security service provider: a formal risk assessment, Board approval and BoG prior approval. Use only CSA-accredited providers, repeat due diligence at least annually and keep ownership of your logs. Tier 1 and 2 RFIs must keep significant SOC capability	Risk assessment; Board and BoG approvals; CSA accreditation proof; annual due diligence	A.5.19 to A.5.23

		in-house.		
PART IX				
CISD-43	Para 52 to 57	Apply security controls through hiring, onboarding, sensitive positions, role changes and termination.	Screening records; onboarding and leaver checklists	A.6.1 to A.6.5
CISD-44	Para 58 to 61	Run a cyber competency framework, cyber education, exercises and AI/ML awareness training.	Training plan and completion records; competency matrix	Clause 7.2, A.6.3
CISD-45	Para 126, Annexure H	Review user access to critical systems at least twice a year.	Access review records with sign-off and removals	A.5.18, A.8.2
PART X				
CISD-46	Para 62 to 66	Secure data transfers, email, web access, BYOD and institutional mobile devices.	Transfer, email and mobile device standards	A.5.14, A.8.1, A.8.23
PART XI				
CISD-47	Para 67 to 75	Apply the controls for electronic banking platforms: customer authentication, websites, mobile apps, email, telephony, customer security and passwords.	Channel security standards; mobile app security tests; customer awareness material	A.8.5, A.8.26
PART XII				
CISD-48	Para 76 to 81	Secure direct connectivity, connections with other institutions and partners, remote access and data in motion.	Connection register; interconnection agreements	A.5.14, A.8.20, A.8.21
PART XIII				
CISD-49	Para 82	Take cloud adoption to the Board first, adopt a cloud policy (including data sovereignty and exit terms) and seek BoG approval to move to cloud services.	Board minutes; cloud policy; BoG approval	A.5.23
CISD-50	Para 83 to 88, Annexure F	Do documented due diligence and risk mapping on the provider before contracting, and repeat due diligence at least every two years.	Due diligence file; cloud risk assessment; shared responsibility matrix; exit plan	A.5.19, A.5.23
PART XIV				
CISD-51	Para 89, 90	Meet the extra requirements for foreign RFIs in Ghana and Ghanaian RFIs	Group policy alignment records	Clause 4.2

		operating abroad.		
PART XV				
CISD-52	Para 91 to 94	Secure zones, segmentation and physical protection of hardware.	Physical security standard; access logs	A.7.1 to A.7.14
PART XVI				
CISD-53	Para 95 to 97, Annexure D	Put cyber clauses in contracts: audit rights, incident notification, continuity, remediation and flow-down to subcontractors, plus AI-specific terms.	Contract clause checklist; signed contracts	A.5.20
PART XVII				
CISD-54	Para 98 to 100	Take digital innovations (blockchain, AI, virtual assets, quantum, robotics) to the Board before adoption, with security policies covering the areas the directive lists.	Board approval; innovation security policy	A.5.1, A.5.8
PART XVIII				
CISD-55	Para 101 to 113	Manage data centre governance, continuity, power, cooling, fire, cabling, physical security, monitoring, SLAs and colocation.	Data centre standards; facility test records; SLAs	A.7.5, A.7.11, A.5.30
PART XIX				
CISD-56	Para 114, Annexure E	Keep an AI/ML governance and control framework covering the nine areas in the directive. Annexure E is mandatory.	AI governance framework; AI inventory; model validation records	Supported by ISO/IEC 42001
CISD-57	Para 115	Include an AI/ML inventory summary, risk profile changes and significant model incidents in the quarterly report to BoG. Notify BoG immediately of serious AI incidents.	Quarterly report section; AI incident log	A.5.24
PART XX				
CISD-58	Para 116 to 129, Annexure H	Run the testing programme at the frequency set for your tier (see the Annexure H table).	Testing calendar; reports; remediation evidence	A.8.8, A.8.29, A.5.30

HOW TO USE THIS PACK

Five steps to a CISD-ready programme.

1

2

Confirm your tier

Assess your profile against Annexure A. It decides your testing frequencies and some controls.

Score every control

Open the CSV and mark each control in place, partly in place or missing. Note the evidence you already have.

3

Plan the gaps

Assign owners and dates. Put approvals, the CISO and ISO 27001 certification first, as they take longest.

4

Build the evidence

Collect evidence as work happens, not before the review. Map each item to its control.

5

Test before Bank of Ghana does

Run an independent internal audit against the directive and close the findings before your next supervisory review.

This pack summarises the Bank of Ghana Cyber and Information Security Directive (March 2026) to help you plan. It is not legal advice and does not reproduce the directive. Read the **official directive** for the exact requirements. Bank of Ghana decides whether an institution complies. ISO references are to ISO/IEC 27001:2022. Last reviewed 17 November 2026.

Need help putting this into practice? Assurelo runs gap assessments, readiness programmes and internal audits. Email hello@assurelo.com or visit assurelo.com to book a free 30-minute call.