FREE COMPLIANCE PACK

The Act 1038 Compliance Pack

Ghana's Cybersecurity Act, 2020 in practical form: a 24-hour incident reporting playbook, a report template, a critical information infrastructure checklist and a licensing checklist for cybersecurity service providers.

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

WHAT'S INSIDE

Three duties, one pack.

Act 1038 reaches further than most organisations expect. Every institution must report incidents within 24 hours. Owners of critical information infrastructure carry extra duties. And anyone selling cybersecurity services in Ghana needs a licence.

1

24-hour reporting playbook

Hour-by-hour steps from detection to report, and how Act 1038 fits with Bank of Ghana and Data Protection Commission reporting.

2

Incident report template

The details to have ready, so your first report goes out on time.

3

CII checklist

Designation, registration, ownership changes, audits and audit reports to the Authority.

4

Licensing checklist

For providers and for buyers: which services need a licence, how to apply and when to renew.

ONE INCIDENT, THREE REPORTS

Who you may need to tell, and how fast.

A single incident at a Ghanaian bank that exposes customer data can trigger three separate

reports. Plan them together so one doesn't delay another.

Law or directive	Who it applies to	Report to	Deadline	Reference
Ghana Cybersecurity Act, 2020 (Act 1038)	Every institution	Sectoral CERT, or the National CERT	Within 24 hours of detection	s.47(5)
Bank of Ghana CISD 2026	BoG-regulated financial institutions	Bank of Ghana	Immediately for trigger events, plus the monthly return by the 15th	Para 50
Data Protection Act, 2012 (Act 843)	Data controllers, when personal data is accessed or acquired without authorisation	Data Protection Commission and the affected people	As soon as reasonably practicable	s.31

24-HOUR PLAYBOOK

From detection to report in under 24 hours.

Section 47(5) gives the person in charge of every institution no more than 24 hours after detection to report. This is a suggested sequence; adjust it to your incident plan.

Hour 0: detect and declare
Log the time of detection. The incident lead decides whether it meets your incident criteria. The 24-hour clock starts at detection, not at confirmation.

Hours 0 to 4: contain and assess
Contain the threat and preserve evidence. Work out which systems and data are affected and whether personal data is involved.

Hours 4 to 12: decide who to notify
Identify your sectoral CERT, or use the CSA point of contact for the National CERT. If you are BoG-regulated, check the paragraph 50 triggers. If personal data is affected, prepare the Data Protection Commission notice.

Before hour 24: report
Send the initial report with what you know so far. Don't wait for the full picture; say what is still being investigated.

After hour 24: update and close
Send updates as the incident unfolds, then a closing report with the root cause and actions. Run a lessons-learned review.

Incident report: details to have ready

A Assurelo template, not an official CSA form. Use the format your CERT or the Authority asks for, and keep this as your internal checklist.

1. Reporting institution, sector and the person in charge
2. Contact for follow-up (name, role, phone, email)
3. Date and time the incident was detected, and how it was detected
4. Type of incident (for example malware, ransomware, unauthorised access, data leak, denial of service, fraud)
5. Systems, services and locations affected; whether any are critical information infrastructure
6. Current impact on services, customers and data, including personal data
7. Actions taken so far to contain and recover
8. Indicators of compromise known so far
9. Other bodies notified (Bank of Ghana, Data Protection Commission, police) and when
10. Whether outside help is engaged, and their CSA licence number
11. Time the next update will be sent

THE CHECKLIST

22 checks, grouped by who they apply to.

Requirements are paraphrased summaries, not the Act's text. The CSV version adds status, owner and notes columns.

ID	Section	Requirement	Expected evidence	ISO 27001
EVERY INSTITUTION				
ACT-01	s.47(5)	The person in charge of the institution reports a cybersecurity incident to the relevant sectoral CERT, or the National CERT, no more than 24 hours after it is detected.	Incident reporting procedure naming the CERT; incident log with detection and report timestamps	A.5.24, A.5.26
ACT-02	s.47(6)	Understand that failing to report attracts the administrative penalty in the Second Schedule.	Board or management briefing record	A.5.31
INSTITUTIONS WITHOUT A SECTORAL CERT				
ACT-03	s.48(2)	Report incidents to the National CERT through the CSA's incident point of contact.	Point of contact details in the incident plan	A.5.5

EVERY INSTITUTION				
ACT-04	s.47(5)	Define what counts as 'detected' so the 24-hour clock starts consistently, and who can declare an incident.	Incident classification and declaration criteria	A.5.25
ACT-05	s.47(5)	Rehearse the 24-hour report with a tabletop exercise, including out-of-hours detection.	Exercise report and lessons learned	A.5.24, A.5.30
CII OWNERS				
ACT-06	s.35	Know whether your systems are, or could be, designated as critical information infrastructure. The Minister designates CII by Gazette, considering sectors such as communications, banking and finance, utilities, transport and public key infrastructure.	CII applicability assessment; copy of any Gazette designation	Clause 4.3, A.5.9
ACT-07	s.36(1), (2)	Register designated CII with the Cyber Security Authority, following the requirements the Authority publishes in the Gazette.	Registration confirmation	A.5.31
ACT-08	s.36(3), (4)	Tell the Authority within seven days of any change in the legal ownership of registered CII.	Change-of-ownership procedure; notification records	A.5.31
ACT-09	s.38(1)	Meet the minimum standards the Minister prescribes for managing CII.	Mapping of the prescribed standards to your controls	Clause 6.1, Annex A
ACT-10	s.38(2)	Be ready for the Authority's periodic audit and inspection of CII.	Evidence pack organised by requirement	Clause 9.2, A.5.35
ACT-11	s.39(1)(a)	Report CII incidents within 24 hours of detection to the sectoral CERT, or to the National CERT if there is no sectoral CERT.	CII incident procedure; report records	A.5.24, A.5.26
ACT-12	s.39(1)(b), (c)	Have the CII audited and send a copy of the audit report to the Authority.	Audit report and proof of submission	Clause 9.2, A.5.35
ACT-13	s.40	Prevent unauthorised access to CII.	Access control records for CII systems	A.5.15, A.8.2, A.8.5
SERVICE PROVIDERS				
ACT-14	s.49(1), First Schedule	Do not provide a cybersecurity service for reward without a CSA licence. The First Schedule includes testing, forensics, incident response, threat	CSA licence covering every service you sell	A.5.31

		hunting, cybersecurity solutions, monitoring, managing security controls, compliance assessment against policy, and advice and training.		
ACT-15	s.50	Apply in writing on the prescribed form, with supporting documents and the fee. The Authority acknowledges within 14 days.	Application file	A.5.31
ACT-16	s.51	Expect a decision within 30 days of application; refusals come with reasons within 28 days. Use the licence only for its granted purpose.	Licence and its terms and conditions	A.5.31
ACT-17	s.52	Do not transfer the licence. Transfer is an offence.	Licence held by the legal entity that delivers the service	A.5.31
ACT-18	s.53	Licences last two years. Apply for renewal at least one month before expiry.	Renewal date in the compliance calendar	A.5.31
ACT-19	s.47(2)	Licensees submit reports on their operations, including incidents, within the period the Authority sets.	Submitted operational reports	A.5.5
PROFESSIONALS				
ACT-20	s.57	Follow the Authority's accreditation mechanism for cybersecurity professionals and practitioners.	Accreditation records for staff	Clause 7.2
BUYERS OF SERVICES				
ACT-21	s.49, First Schedule	Check that every cybersecurity provider you hire holds a current CSA licence for that service.	Supplier licence checks on file	A.5.19, A.5.20
EVERY INSTITUTION				
ACT-22	s.59	Track the standards and directives the Authority issues and apply those that cover you.	Regulatory watch log	A.5.31

Penalties: failing to report an incident (s.47(6)), failing to report CII ownership changes (s.36(4)), CII audit failures (s.39(2)) and providing services without a licence (s.49(2)) attract the administrative penalties in the Act's Second Schedule. Transferring a licence is a criminal offence (s.52(2)).

This pack summarises the Cybersecurity Act, 2020 (Act 1038) to help you plan. It is not legal advice. Read the **official Act** and the Cyber Security Authority's current directives for exact requirements. 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.