ONIX DECISION-SUPPORT TOOL

The CISD 2026 Infrastructure Evidence Checklist

What to ask - and what evidence to request - before approving a data-centre, cloud or resilience provider

Work through one defined workload at a time. Tick one status in every review area, record the supporting evidence, and name the internal function accepting each answer. Retain gaps as actions rather than assumptions.

IMPORTANT: This checklist is a general decision-support tool. It is not legal advice, a compliance assessment or a substitute for guidance from the Bank of Ghana. Selecting any particular infrastructure provider, including Onix, does not automatically make an organisation compliant.

1. Workload definition and data classification

Ask What business service and dependencies are in scope? Who owns it? What data classes, criticality, RTO and RPO apply?

Request Approved workload profile; asset and data inventory; business impact analysis; classification and recovery objectives.

Warning signs Undefined scope; no business owner; every dataset treated alike; recovery objectives chosen by the provider.

Accepting owner Business and data owners; Information Security or Risk validates classification.

STATUS [ ] Complete [ ] Action needed [ ] N/A

2. Data location and data-flow mapping

Ask Where are primary data, replicas, backups, logs and keys stored or processed? From where can support staff or subcontractors access them?

Request Current architecture and data-flow maps; location register; support-access map; cross-border safeguards and BoG approval where applicable.

Warning signs A vague region; undisclosed backup or telemetry locations; data moves when the provider changes architecture.

Accepting owner Data Protection or Privacy, CISO, Legal and Compliance.

STATUS [ ] Complete [ ] Action needed [ ] N/A

3. Shared responsibility and control ownership

Ask Who owns each control across facility, network, platform, operating system, application, IAM, keys, logging, backups, incidents and recovery?

Request Signed RACI or shared-responsibility matrix; control mapping; operating playbooks and named control owners.

Warning signs The provider handles security; gaps between layers; customer duties not reflected in the target design.

Accepting owner Solution architect and CISO, with each control owner accepting their obligations.

STATUS [ ] Complete [ ] Action needed [ ] N/A

4. Physical facility resilience

Ask How are site risks, independent power paths, backup capacity, dual feeds, cooling, fire protection, access control and continuous monitoring addressed?

Request Site-risk assessment; electrical and mechanical diagrams; maintenance and test records; access-control evidence; certification scope where relied upon.

Warning signs Single points of failure; expired or out-of-scope certificates; no recent maintenance or failover evidence.

Accepting owner Infrastructure or Facilities, BCM and Information Security.

STATUS [ ] Complete [ ] Action needed [ ] N/A

5. Connectivity and route diversity

Ask Are entry paths, meet-me rooms, carriers and last-mile routes genuinely diverse? Is capacity sufficient during failure and has failover been tested?

Request Route maps and carrier letters; topology; capacity records; recent failover results with issues and remediation.

Warning signs Two links in the same duct; one upstream provider; route details unavailable; failover assumed rather than tested.

Accepting owner Network architect and technical service owner.

STATUS [ ] Complete [ ] Action needed [ ] N/A

6. Security operations and incident communication

Ask What is monitored continuously? Can logs feed the RFI SIEM? Who escalates, preserves evidence and notifies the RFI within the applicable CISD timeframe?

Request SOC operating model; logging design; escalation matrix; incident template; notification clause; exercise and post-incident reports.

Warning signs No log export; vague commercially reasonable notice; provider controls all forensic evidence; contacts are untested.

Accepting owner CISO or SOC; Legal accepts notification and evidence-access terms.

STATUS [ ] Complete [ ] Action needed [ ] N/A

7. Business continuity, backup restoration and DR

Ask Which failure scenarios are covered? Are backups independent and recoverable? Has end-to-end restoration or failover met the approved RTO and RPO?

Request BCP and DR plans; backup inventory and settings; latest restore and failover reports; actual timings; open findings and remediation.

Warning signs Backups never restored; facility failover presented as application recovery; DR relies on the same site, provider or control plane.

Accepting owner BCM, application and technical owners, with Risk accepting residual exposure.

STATUS [ ] Complete [ ] Action needed [ ] N/A

8. Contractual service levels

Ask What service is committed? How are availability, exclusions, maintenance, incident notice, recovery and remedies measured and reported?

Request Signed SLA and service description; metric definitions; sample performance report; remedies, escalation and termination triggers.

Warning signs Marketing availability is not contractual; broad exclusions; provider-only measurements; credits are the only response to chronic failure.

Accepting owner Service owner, Procurement or Vendor Management, and Legal.

STATUS [ ] Complete [ ] Action needed [ ] N/A

9. Audit and information rights

Ask Can the RFI, its auditors and BoG access relevant records, systems, people and facilities? Can controls be tested after an incident?

Request Audit and regulator-access clauses; current independent reports with scope and exceptions; test summaries; remediation evidence; audit procedure.

Warning signs Stale or out-of-scope reports; no rights beyond a certificate; regulator access is conditional; critical findings remain open.

Accepting owner Internal Audit, Compliance, Legal and CISO.

STATUS [ ] Complete [ ] Action needed [ ] N/A

10. Subcontractor oversight

Ask Who supports the service at every tier, where do they operate and what can they access? Is notice or approval required before changes?

Request Current subcontractor register; dependency and location map; flow-down clauses; assurance reports; primary-provider liability.

Warning signs Undisclosed fourth parties; unilateral changes; weaker downstream terms; no audit, objection or exit right.

Accepting owner Third-Party Risk or Procurement, with Legal and CISO.

STATUS [ ] Complete [ ] Action needed [ ] N/A

11. Migration, termination and exit planning

Ask Can data and configurations be exported completely and securely? What are the time, cost, support, rollback, fallback and deletion arrangements?

Request Tested exit runbook; supported formats and sample export; drill results; transition-support clause; deletion attestation covering replicas and backups.

Warning signs Proprietary format; undefined egress cost; no continuity period; backups cannot be deleted; exit has never been tested.

Accepting owner Architecture and service owner, Procurement, Legal and BCM.

STATUS [ ] Complete [ ] Action needed [ ] N/A

12. Ongoing assurance and change control

Ask What evidence will be refreshed, how often, and after which changes or incidents? Who monitors performance, risks, capacity and remediation?

Request Assurance calendar; change-notification clause; quarterly service pack; risk register; action log; next audit, DR and exit-test dates.

Warning signs Approval treated as permanent; material changes need no notice; repeated exceptions; no owner or deadline for findings.

Accepting owner Vendor Management and service owner, overseen by Risk, Compliance and Internal Audit.

STATUS [ ] Complete [ ] Action needed [ ] N/A

Final approval record

Complete this record only after the evidence above has been reviewed. Attach the evidence pack, record conditions explicitly, and set the next test date before sign-off.

Workload reviewed	_____
Business owner	_____
Technical owner	_____
Risk or compliance owner	_____
Provider or architecture considered	_____
Readiness checks	[ ] Evidence pack attached [ ] Open actions logged [ ] Next test date set
Decision	[ ] Approve [ ] Approve with actions [ ] Do not approve
Outstanding evidence	_____ _____ _____
Actions and deadlines	_____ _____ _____
Next review or testing date	_____

Sign-off

Approver	Function	Date
_____	_____	_____

This checklist is a general decision-support tool. It is not legal advice, a compliance assessment or a substitute for guidance from the Bank of Ghana. Selecting any particular infrastructure provider, including Onix, does not automatically make an organisation compliant.

Primary sources used: BoG CISD 2026; BoG Outsourcing Directive 2024. Confirm the provisions and approvals applicable to the specific RFI and workload.