ASTUTE Business Consult
..System. Standard. Strategy

Information Security Governance Checklist

Review responsibilities and turn security gaps into action

Your business holds information people trust you to protect. Use this checklist to examine who makes security decisions, what evidence supports those decisions and which issues need attention.

Prepared by Astute Business Consult • Version 1.0 • November 2026

Business _____

Completed by and role _____

Review date _____

Review scope _____

State the departments, locations, records and systems included. Include paper records and external services where relevant.

How to use this checklist

1. Complete the review with the people who manage your records, systems and suppliers. In a small business, the owner might cover several roles.

2. Check documents and actual practice before selecting one response for each item. Record a document name, date or other evidence reference.

3. Use Yes only when the arrangement is in place and supported by evidence. Use Partial when it is incomplete, No when it is absent, and Unsure when you cannot verify it. Explain every Not applicable response.

4. Transfer gaps to the action plan. Give each action an owner, a priority, a due date and a way to confirm completion.

5. Agree a follow-up date. Treat the completed checklist as internal business information. Record evidence locations rather than passwords or personal records.

This is an initial governance review. It does not establish ISO 27001 conformity, certification readiness or legal compliance.

Review 1 of 4

Select one response per item. Add evidence references and note any gap.

Y = Yes P = Partial N = No U = Unsure NA = Not applicable

Leadership and accountability

A named decision-maker helps staff know who can approve action.

01 A named owner or senior manager is accountable for information security.

Evidence to check: Role description or written appointment.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

02 Staff and service providers know their security responsibilities and reporting contacts.

Evidence to check: Responsibility list and supplier agreement.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

03 Significant risks and spending decisions reach someone with authority to act.

Evidence to check: Escalation process and decision record.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

04 Leaders review security issues and follow up on agreed actions.

Evidence to check: Review notes and action tracker.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

Information and access

Include information stored in email, shared drives, applications and paper files.

05 We have a current list of important information, its locations and its owners.

Evidence to check: Information inventory and storage locations.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

06 We understand where information moves between teams and external services.

Evidence to check: Data flow record or transaction walkthrough.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

07 Access is approved according to work needs and reviewed when roles change.

Evidence to check: Approvals and a recent access review.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

08 Departing staff and suppliers have access removed promptly.

Evidence to check: Departure checklist and account removal records.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

Review 2 of 4

Select one response per item. Add evidence references and note any gap.

Y = Yes P = Partial N = No U = Unsure NA = Not applicable

Risk decisions and resources

Make unresolved risks visible to the people who can address them.

09 We assess likely harm from information being exposed, changed or unavailable.

Evidence to check: Risk register with business impacts.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

10 Each significant risk has an owner and an agreed response.

Evidence to check: Risk treatment plan and named owners.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

11 Accepted risks have a recorded reason, authorised approval and review date.

Evidence to check: Risk acceptance record.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

12 Agreed security work has the time, budget and skills it needs.

Evidence to check: Resource plan, approvals or training records.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

Suppliers and system changes

Keep responsibilities clear during upgrades, migrations and contract changes.

13 We assess suppliers before giving them important information or system access.

Evidence to check: Supplier review and service scope.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

14 Contracts define security duties, incident reporting and information return or disposal.

Evidence to check: Relevant contract terms.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

15 Older systems awaiting replacement have an owner and interim safeguards.

Evidence to check: Migration plan and interim protection review.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

16 Major changes receive security checks before launch and retirement.

Evidence to check: Change approval and retirement checklist.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

Review 3 of 4

Select one response per item. Add evidence references and note any gap.

Y = Yes P = Partial N = No U = Unsure NA = Not applicable

Policies and staff awareness

Check that instructions are practical and understood.

17 Current policies explain how staff should handle, share and protect information.

Evidence to check: Approved policies and staff guidance.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

18 Staff receive relevant training when joining and when responsibilities change.

Evidence to check: Training records and onboarding material.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

19 Staff know how to report a suspicious message, lost device or information mistake.

Evidence to check: Reporting instructions and staff walkthrough.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

20 Sensitive paper records and devices have suitable physical protection and disposal arrangements.

Evidence to check: Storage checks and disposal records.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

Incident response and recovery

Prepare the decisions and contacts needed when something goes wrong.

21 We have a response plan with named contacts and clear escalation steps.

Evidence to check: Incident plan and current contact list.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

22 We have a process to assess notification duties and record incident decisions.

Evidence to check: Notification procedure and incident log.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

23 Important information is backed up appropriately and recovery has been tested.

Evidence to check: Backup schedule and restoration test result.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

24 Exercises or incidents lead to reviewed lessons and corrective actions.

Evidence to check: Exercise notes and completed action records.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

ASTUTE Business Consult
...System. Standard. Strategy

Review 4 of 4

Select one response per item. Add evidence references and note any gap.

Y = Yes P = Partial N = No U = Unsure NA = Not applicable

Privacy and information lifecycle

Confirm the requirements relevant to your activities with qualified support where needed.

25 We record why personal information is collected and the lawful basis for using it.

Evidence to check: Processing record and privacy notice.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

26 Retention periods are defined and unnecessary records are securely removed.

Evidence to check: Retention schedule and disposal evidence.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

27 We have a process for privacy requests and changes involving higher-risk processing.

Evidence to check: Request log and assessment procedure.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

28 We review applicable Nigerian, sector and cross-border obligations as operations change.

Evidence to check: Obligations register and compliance review.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

Assurance and continual improvement

Use evidence to decide whether the arrangements work.

29 Security reports explain material risks, overdue actions and decisions needed.

Evidence to check: Recent management report.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

30 Checks or internal audits examine actual practice and record findings.

Evidence to check: Audit or review report.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

31 Corrective actions are tested before they are marked complete.

Evidence to check: Closure evidence and verification notes.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

32 Where we rely on a certificate, we check its scope, issuer and current status.

Evidence to check: Certificate scope and issuer verification.

☐ Y ☐ P ☐ N ☐ U ☐ NA Evidence or gap: _____

Turn findings into an action plan

Count your responses to check that all 32 items have been reviewed. Use the findings to prioritise work. A high Yes count does not cancel out a serious unresolved gap.

Yes	Partial	No	Unsure	Not applicable
_____	_____	_____	_____	_____

Choose a priority for each gap

Urgent: A suspected incident, exposed information or ongoing unauthorised access needs immediate escalation through your response process. Assess any reporting duties promptly.

High: A significant weakness needs prompt management attention and a dated plan.

Routine: Schedule lower-risk improvements and verify completion.

Unsure: Assign someone to establish the facts before deciding the final priority.

Priorities are planning labels, not a formal risk rating. Agree deadlines based on likely harm and applicable obligations.

Action 1

Checklist item and gap _____

Priority and immediate safeguard _____

Action and evidence needed for closure _____

Owner and due date _____

Verified by and completion date _____

Action 2

Checklist item and gap _____

Priority and immediate safeguard _____

Action and evidence needed for closure _____

Owner and due date _____

Verified by and completion date _____

Copy this page for additional actions.

Next review date _____

Review approved by _____

Understand the terms and next steps

Governance. The direction, accountability and oversight behind security decisions.

ISMS. An information security management system: the organised policies, processes and safeguards used to manage information security risks.

Evidence. A record or observation showing what happens in practice, such as an access review, test result or approved decision.

Risk owner. The person with responsibility and authority to manage a particular risk.

Legacy system. An older system still in use, including one awaiting migration or replacement.

Certification scope. The activities and boundaries covered by a certified management system.

Discuss your findings with Astute Business Consult

If this review identifies gaps your team needs help addressing, contact Astute Business Consult to discuss your findings and management system implementation needs.

Visit astutebusinessconsult.com to enquire about a diagnostic discussion. Bring your completed checklist and your three highest-priority actions. Share summaries rather than sensitive records.

Reference material

This practical checklist draws on the resources below. It is not an exhaustive clause-by-clause audit. Check current legal and contractual requirements when planning your actions.

ISO/IEC 27001 overview

https://www.iso.org/standard/27001

UK National Cyber Security Centre guidance on governance

https://www.ncsc.gov.uk/collection/risk-management/cyber-security-governance

Nigeria Data Protection Act 2023

https://www.nadpa-rapdp.org/sites/default/files/2023-07/Nigeria_Data_Protection_Act_2023_0.pdf

NDPC General Application and Implementation Directive 2025

https://ndpc.gov.ng/wp-content/uploads/2025/07/NDP-ACT-GAID-2025-MARCH-20TH.pdf

Prepared November 2026 • Review this checklist when your systems, suppliers or obligations change.