SecureZaidi
CYBERSECURITY & COMPLIANCE

COMPLIANCE GUIDE 02 / 04

ISO 27001 Implementation Guide for East African Organisations

A practical, step-by-step guide to implementing ISO 27001:2022 — from gap analysis to certification audit — with East African business context throughout.

Produced by	SecureZaidi Limited
Website	securezaidi.com
Email	info@securezaidi.com
Phone	+254 700 000 000
Edition	2026 Edition — For East African Organisations

This guide is produced for educational and informational purposes and does not constitute legal advice. For a tailored compliance assessment, contact SecureZaidi.

Contents

1. What is ISO 27001?

ISO/IEC 27001 is the internationally recognised standard for Information Security Management Systems (ISMS). Published by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), it provides a framework for establishing, implementing, maintaining, and continually improving an organisation's approach to managing information security risks.

Achieving ISO 27001 certification means an independent, accredited certification body has verified — through a formal audit — that your organisation has implemented systematic, comprehensive, and effective controls to protect the confidentiality, integrity, and availability of information. The certificate is valid for three years, subject to annual surveillance audits.

Unlike compliance frameworks that prescribe specific technical controls, ISO 27001 takes a risk-based approach: you identify the information security risks relevant to your organisation and implement appropriate controls to reduce those risks to an acceptable level. This makes it applicable to any organisation of any size or sector.

2. The Business Case for Certification

ISO 27001 certification delivers both internal and external value. Organisations typically pursue it for one or more of the following reasons:

- Customer and procurement requirements: Many enterprise clients — particularly in banking, telecoms, and government — now require their suppliers to hold ISO 27001 as a minimum prerequisite for tendering.
- Regulatory alignment: ISO 27001 provides strong structural alignment with the Kenya DPA, GDPR, PCI DSS, and other regulations — reducing duplication of compliance effort.
- Cyber insurance: Insurers increasingly offer better premiums and coverage terms to ISO 27001 certified organisations.
- Competitive differentiation: Certification signals to the market that your organisation takes security seriously — a powerful differentiator in a region where trust is a key purchasing factor.
- Risk reduction: The structured risk management process identifies and treats real vulnerabilities before they are exploited, reducing the likelihood and cost of security incidents.
- Operational discipline: The documentation and process requirements that certification demands often improve internal operations, accountability, and audit readiness well beyond information security.

3. What Changed in the 2022 Revision

ISO 27001:2022 replaced the 2013 version with significant changes to Annex A (the control catalogue). Organisations certified to the 2013 standard had until October 2025 to transition. Key changes include:

Control count

The 114 controls across 14 domains of the 2013 standard were restructured into 93 controls across 4 themes: Organisational (37), People (8), Physical (14), and Technological (34).

New controls (examples)

- Threat intelligence (5.7) — organisations must now gather, analyse, and act on cyber threat intelligence.
- Cloud services security (5.23) — explicit requirements for securing cloud computing environments.
- ICT readiness for business continuity (5.30) — strengthened link between IT and BCP.
- Web filtering (8.23) — managing access to external websites.
- Data masking (8.11) and Data leakage prevention (8.12) — new controls for data security.
- Secure coding (8.28) — requirements for application development security.

Action required	If your organisation is implementing ISO 27001 now, build to the 2022 standard from the start. New certifications issued after October 2023 must be to ISO 27001:2022.

4. Phase 1 — Gap Analysis

A gap analysis is the starting point for any ISO 27001 implementation. It compares your organisation's current security practices against the full requirements of the standard — identifying what is already in place, what is partially addressed, and what is missing entirely.

What a gap analysis covers:

- Review of existing policies, procedures, and documentation against ISO 27001 clause requirements.
- Assessment of current technical controls against all 93 Annex A controls.
- Interviews with key personnel across IT, operations, HR, legal, and management.
- Assessment of existing risk management practices.
- Review of third-party and supplier security arrangements.

Output:

The gap analysis produces a prioritised remediation roadmap, an estimate of implementation effort and timeline, and a view of certification readiness. For most East African organisations, a gap analysis typically takes 1–3 weeks depending on size and complexity.

5. Phase 2 — Defining Your ISMS Scope

The ISMS scope defines the boundaries of your information security management system — which parts of the organisation, which locations, which systems, and which processes are covered by the certification. Getting the scope right is one of the most important early decisions.

Scope considerations:

- Too narrow: a scope that excludes significant business functions or systems may satisfy the standard technically but provide little actual security assurance or commercial value.
- Too broad: trying to certify everything at once increases cost, time, and complexity — especially for a first certification.
- For most SMEs, scoping to the entire organisation is workable. Larger organisations may scope to a specific business unit, product line, or geographic location initially and expand later.

Scope statement	Your scope statement must describe the organisation, its context (internal and external factors that affect information security), interested parties (customers, regulators, shareholders), and the boundaries of the ISMS. This becomes a formal ISMS document.

6. Phase 3 — Risk Assessment

ISO 27001 is fundamentally a risk-based standard. The risk assessment process identifies the information security risks your organisation faces and determines how to treat each one. There is no prescribed methodology — you choose an approach appropriate to your organisation.

Typical risk assessment steps:

- 1. Asset identification — document all information assets: data, systems, applications, people, processes, and physical assets within scope.
- 2. Threat identification — identify threats relevant to each asset (e.g. ransomware, insider theft, fire, hardware failure, supplier breach).
- 3. Vulnerability identification — identify weaknesses that could be exploited by each threat.
- 4. Risk scoring — assign a likelihood and impact score to each risk (typically using a 5x5 or 3x3 matrix) to produce a risk level (Critical, High, Medium, Low).
- 5. Risk treatment — for each risk, decide: Reduce (implement controls), Transfer (insurance), Avoid (stop the activity), or Accept (document and monitor).

- 6. Risk treatment plan — document the specific controls to be implemented for each risk to be reduced.

Living document	The risk assessment is not a one-time exercise. ISO 27001 requires it to be reviewed at planned intervals and when significant changes occur — new systems, new services, new threats, or new regulatory requirements.

7. Phase 4 — Statement of Applicability (SoA)

The Statement of Applicability (SoA) is one of the most important documents in your ISMS. It lists every one of the 93 Annex A controls and documents for each one: whether it is applicable, whether it is currently implemented, and the justification for inclusion or exclusion.

Controls can be excluded if they are genuinely not relevant to your scope — for example, a fully cloud-based organisation with no physical media may exclude physical media disposal controls. However, exclusions must be justified and documented, and auditors will scrutinise them closely.

The SoA provides a comprehensive, auditable record of your control selection decisions and is a key document reviewed during the Stage 1 certification audit.

8. Phase 5 — Implementing Controls

ISO 27001:2022 organises its 93 Annex A controls across four themes. Below is a summary of key control areas in each theme:

Theme	Key control areas
Organisational (37)	Information security policies, roles & responsibilities, threat intelligence, supplier security, asset management, access control, incident management, business continuity, compliance.
People (8)	Screening, terms of employment, security awareness training, disciplinary process, remote working, confidentiality agreements.
Physical (14)	Physical security perimeters, access controls, equipment security, clear desk policy, secure disposal of media and equipment.
Technological (34)	Endpoint protection, network security, encryption, secure development, vulnerability management, logging & monitoring, cloud security, web filtering, DLP, backup, MFA.

9. Phase 6 — Mandatory Documentation

ISO 27001 has explicit documentation requirements. The following documents are mandatory — auditors will expect to review them:

- ISMS scope statement
- Information security policy
- Information security risk assessment methodology
- Risk assessment results and risk register
- Risk treatment plan
- Statement of Applicability (SoA)
- Information security objectives
- Evidence of competence of ISMS personnel
- Operational planning and control documents
- Internal audit programme and results
- Management review records
- Evidence of monitoring, measurement, analysis, and evaluation
- Nonconformity and corrective action records

Documentation quality	Documents do not need to be long — they need to be accurate, followed in practice, and demonstrably reviewed. A 2-page policy that is actually used is more valuable than a 20-page policy that nobody has read.

10. Phase 7 — Internal Audit

ISO 27001 requires at least one internal audit per year to assess whether the ISMS conforms to the standard's requirements and your own documented procedures. Internal auditors must be objective and impartial — meaning they should not audit their own work.

The audit programme should cover all ISMS clauses over the certification cycle. Findings should be documented as nonconformities or observations, and a corrective action plan should be produced and tracked to closure. Internal audit evidence is reviewed by the certification auditor during Stage 1.

11. Phase 8 — Management Review

Senior management must review the ISMS at planned intervals to ensure it remains suitable, adequate, and effective. This is not simply a status update meeting — it must review specific inputs and produce

documented outputs.

Required inputs include:

- Status of actions from previous reviews
- Changes in internal and external context
- Feedback on information security performance including incidents and audit results
- Opportunities for continual improvement
- Feedback from interested parties
- Results of risk assessments and treatment plan status

12. Phase 9 — Certification Audit

The certification audit is conducted by an accredited certification body (CB) and consists of two stages:

Stage 1 — Documentation review (typically 1–2 days)

The auditor reviews your ISMS documentation — scope, policies, risk assessment, SoA, internal audit results, and management review records — to determine whether your organisation is ready for the Stage 2 audit. Stage 1 is usually conducted remotely.

Stage 2 — On-site audit (typically 2–5 days depending on scope)

The auditor visits your premises (or conducts remote sessions) to verify that the ISMS is being operated in practice — interviewing staff, reviewing evidence, testing controls, and examining records. Certification is awarded if no major nonconformities are found.

Choosing a certification body	Use an IAF-accredited certification body (e.g. BSI, Bureau Veritas, SGS, TÜV). Certificates from non-accredited bodies are not widely recognised and will not satisfy enterprise procurement requirements.

13. Maintaining Your Certificate

ISO 27001 certification is valid for three years, subject to annual surveillance audits in years 1 and 2, and a full recertification audit in year 3. The surveillance audits are typically shorter than the initial certification and focus on whether the ISMS continues to operate effectively and improvements are being made.

Key ongoing activities: continuous monitoring of controls, regular risk assessment reviews, ongoing staff training, management reviews, internal audits, and prompt treatment of identified nonconformities.

14. Realistic Timeline and Budget

Organisation size	Typical timeline	Typical total cost range
Small (under 50 staff)	6–9 months	USD 15,000–35,000
Medium (50–250 staff)	9–14 months	USD 30,000–70,000
Large (250+ staff)	12–24 months	USD 60,000–200,000+

** Costs include consultancy support, staff time, tooling, and certification body fees. Organisations with existing mature security practices will be at the lower end of the range.*

How SecureZaidi Can Help

SecureZaidi is a Kenya-based cybersecurity and GRC consultancy specialising in helping East African organisations achieve and maintain compliance, reduce cyber risk, and build lasting security cultures. Our consultants bring deep, practical expertise in the Kenyan regulatory environment and the realities of doing business in the region.

Kenya DPA Compliance	ODPC registration, DPIA support, DPO-as-a-Service, policy development, and staff training.
ISO 27001 Certification	Gap analysis, ISMS implementation, internal audit support, and certification readiness preparation.
Security Awareness Training	Customised staff workshops, phishing simulation campaigns, and 12-month culture programmes.
GRC Advisory	Risk register development, threat modelling, board-level reporting, and policy frameworks.
vCISO Services	Fractional CISO leadership — strategy, oversight, and executive reporting without a full-time hire.

Penetration Testing	Authorised simulated attacks on networks, web applications, and cloud environments.

Ready to take the next step? Contact us today for a no-obligation consultation.

Email	info@securezaidi.com
Phone	+254 700 000 000
Website	securezaidi.com