912

TECH

The 912 IT Audit Checklist

47 Points. Five Pillars. One Workbook.

Built from 2,000+ client engagements across 10 African countries.
Use this checklist to identify gaps in your hardware, software, security, cloud, and data governance — before they cost you.

BEFORE YOU START

How to Use This Checklist

This checklist is organised into five pillars. For each item, mark one of three statuses:

Status	Meaning
[Done]	Control is in place and documented.
[Partial]	Control exists but is incomplete or undocumented.
[Missing]	Control is absent or unknown.

Tally your results at the end of each pillar. Any pillar scoring below 60% warrants immediate remediation.

This document is the same framework 912 Tech uses in every new client onboarding audit. It is not comprehensive for all regulatory environments — for ODPC, CBK, or ISO 27001 compliance, contact us for a full assessment.

SCORING GUIDE

Score	Risk Level	Recommended Action
80 – 100%	Low	Strong foundation. Address remaining gaps within 90 days.
60 – 79%	Moderate	Prioritise Missing items in Pillars 2 and 3 first.
40 – 59%	High	Engage IT support immediately for Pillar 2 and 3 gaps.
Below 40%	Critical	Stop and call your IT manager or 912 Tech now.

PILLAR 1 OF 5

Physical Security & Infrastructure

*Mark each item: **[Done]** = in place & documented | **[Partial]** = incomplete or undocumented | **[Missing]** = absent or unknown*

#	Control Item	Done	Partial	Missing
1	All IP cameras are inventoried with make, model, firmware version, and last-patched date.	[ ]	[ ]	[ ]
2	CCTV footage is stored with minimum 30-day retention and access is logged per KDPA requirements.	[ ]	[ ]	[ ]
3	IP cameras and NVRs are on a dedicated VLAN, isolated from production network traffic.	[ ]	[ ]	[ ]
4	All camera default credentials have been changed and password policy is enforced.	[ ]	[ ]	[ ]
5	Physical server room / comms cabinet has restricted access (key, biometric, or PIN) with access log.	[ ]	[ ]	[ ]
6	Structured cabling is labelled, documented, and Cat6A or above for new installations.	[ ]	[ ]	[ ]
7	UPS installed for all critical network equipment with monthly test records.	[ ]	[ ]	[ ]
8	Electric perimeter fence (if installed) connected to remote monitoring and VMS integration.	[ ]	[ ]	[ ]
9	Access control system (biometric/card) integrated with HR for immediate leavers de-provisioning.	[ ]	[ ]	[ ]

Pillar 1 Score: _____ / 9 Percentage: _____%

PILLAR 2 OF 5

Cloud & Core IT

*Mark each item: **[Done]** = in place & documented | **[Partial]** = incomplete or undocumented | **[Missing]** = absent or unknown*

#	Control Item	Done	Partial	Missing
10	All cloud accounts (AWS, Azure, Google Cloud) have MFA enforced for every user — no exceptions.	[ ]	[ ]	[ ]
11	Formal offboarding process: cloud access revoked within 24 hours of employee departure.	[ ]	[ ]	[ ]
12	All production servers covered by a monitoring tool with uptime alerting (Zabbix, Datadog, etc.).	[ ]	[ ]	[ ]
13	Network firewall firmware patched within 30 days of a security release.	[ ]	[ ]	[ ]
14	SD-WAN or failover internet link configured for critical sites (single ISP = single point of failure).	[ ]	[ ]	[ ]
15	VPN or Zero Trust Network Access (ZTNA) required for all remote access — no direct RDP to servers.	[ ]	[ ]	[ ]
16	Backup restoration tested in the last 90 days with a documented restore time.	[ ]	[ ]	[ ]
17	Email filtering (anti-spam + anti-phishing) is active and logs are reviewed monthly.	[ ]	[ ]	[ ]
18	Domain DNS records include SPF, DKIM, and DMARC — verified via MXToolbox or equivalent.	[ ]	[ ]	[ ]
19	IT asset management system exists with a record for every device on the network.	[ ]	[ ]	[ ]

Pillar 2 Score: _____ / 10 Percentage: _____%

PILLAR 3 OF 5

Cybersecurity

*Mark each item: **[Done]** = in place & documented | **[Partial]** = incomplete or undocumented | **[Missing]** = absent or unknown*

#	Control Item	Done	Partial	Missing
20	Endpoint Detection and Response (EDR) deployed on 100% of managed endpoints — not legacy antivirus.	[ ]	[ ]	[ ]
21	Security Incident Response Plan (SIRP) exists, tested annually, and staff know their roles.	[ ]	[ ]	[ ]
22	All privileged accounts (Domain Admin, root, superuser) documented and reviewed quarterly.	[ ]	[ ]	[ ]
23	Password policy enforces minimum 12 characters, complexity, and 90-day rotation for privileged accounts.	[ ]	[ ]	[ ]
24	Active Directory / identity provider audited for stale accounts (departed employees) in last 6 months.	[ ]	[ ]	[ ]
25	Security awareness training conducted for all staff in the last 12 months.	[ ]	[ ]	[ ]
26	Vulnerability scanning run quarterly on all internet-facing systems.	[ ]	[ ]	[ ]
27	WAF or DDoS protection active on all public-facing web applications.	[ ]	[ ]	[ ]
28	Penetration test completed in the last 24 months by an independent third party.	[ ]	[ ]	[ ]
29	Logs from firewalls, servers, and endpoints centralised in a SIEM or log management platform.	[ ]	[ ]	[ ]

Pillar 3 Score: _____ / 10 Percentage: _____%

PILLAR 4 OF 5

Applications & Software

*Mark each item: **[Done]** = in place & documented | **[Partial]** = incomplete or undocumented | **[Missing]** = absent or unknown*

#	Control Item	Done	Partial	Missing
30	Software licence register: every SaaS subscription with vendor, cost, renewal date, user count.	[ ]	[ ]	[ ]
31	All software on vendor-supported versions — no end-of-life applications in production.	[ ]	[ ]	[ ]
32	ERP / core business system has documented backup and restore procedure tested in last 90 days.	[ ]	[ ]	[ ]
33	Third-party API integrations (M-Pesa, KRA TIMS, etc.) documented; credentials in secrets manager.	[ ]	[ ]	[ ]
34	Application deployment follows test to staging to production pipeline — no direct production pushes.	[ ]	[ ]	[ ]
35	Mobile applications handling company data enforce device-level MDM policy.	[ ]	[ ]	[ ]
36	SaaS spend reviewed quarterly to identify unused licences or duplicate tools.	[ ]	[ ]	[ ]
37	Custom software has documented ownership, source code in version control, known handover procedure.	[ ]	[ ]	[ ]
38	KRA TIMS integration certified and VAT reconciliation tested against eTIMS monthly.	[ ]	[ ]	[ ]

Pillar 4 Score: _____ / 9 Percentage: _____%

PILLAR 5 OF 5

Data & Governance

*Mark each item: **[Done]** = in place & documented | **[Partial]** = incomplete or undocumented | **[Missing]** = absent or unknown*

#	Control Item	Done	Partial	Missing
39	Data inventory (data map) exists: all personal data held, where stored, and who has access.	[ ]	[ ]	[ ]
40	ODPC-compliant Privacy Notice published on company website, updated within last 12 months.	[ ]	[ ]	[ ]
41	Data retention and deletion schedules documented and enforced — not kept indefinitely.	[ ]	[ ]	[ ]
42	Employees handling personal data have received ODPC/GDPR awareness training in last 12 months.	[ ]	[ ]	[ ]
43	Data breach response: detection, containment, notification within 72 hours (ODPC requirement).	[ ]	[ ]	[ ]
44	Sensitive data at rest encrypted (AES-256 or equivalent) — not stored in unencrypted flat files.	[ ]	[ ]	[ ]
45	Power BI dashboards do not expose row-level personal data to unauthorised users (RLS configured).	[ ]	[ ]	[ ]
46	Cloud storage (SharePoint, Drive, S3) audited — no 'anyone with the link' on sensitive files.	[ ]	[ ]	[ ]
47	Business Continuity Plan (BCP) exists, covers IT systems, and tested in last 12 months.	[ ]	[ ]	[ ]

Pillar 5 Score: _____ / 9 Percentage: _____%

SUMMARY

Your Audit Score Sheet

Transfer your pillar scores from each section below.

Pillar	Items	Score	%	Status
1 — Physical Security & Infrastructure	9	__ / 9	__%	
2 — Cloud & Core IT	10	__ / 10	__%	
3 — Cybersecurity	10	__ / 10	__%	
4 — Applications & Software	9	__ / 9	__%	
5 — Data & Governance	9	__ / 9	__%	
TOTAL	**47**	**__ / 47**	**__%**	

What to do with your score

Share this completed checklist with your IT manager or board. The pillars with the lowest scores are your highest-risk areas.

If you score below 60% on any pillar, we recommend an immediate remediation conversation. Book a free 30-minute Discovery Call at **nineonetwo.co.ke/contact** — we will tell you exactly what we would fix first and why.

912

TECH

One Contract. Every Need.

912 Tech delivers managed IT services across Kenya and Africa — physical security, cloud infrastructure, custom software, and data intelligence under a single SLA.

CONTACT

+254 111 047 120

hello@nineonetwo.co.ke

nineonetwo.co.ke

The Chancery, 8th Floor, Valley Road, Nairobi, Kenya

For ODPC, CBK, or ISO 27001 compliance assessments, engage a qualified auditor.

This checklist is provided for informational purposes.