KEVAJOPA TECHNOLOGIES LIMITED

Make Smarter, Faster, Secure.

ICT SOLUTIONS · SOFTWARE · NETWORKS & INFRASTRUCTURE · SECURITY SYSTEMS · TRAINING

PROFESSIONAL CERTIFICATE PROGRAMME · ITA-2026-019

IT Auditing and Controls Assurance

An eight-week practical programme in planning, testing and reporting an information systems audit — built around real control failures, not framework recitation.

DURATION	CONTACT HOURS	LEVEL	DELIVERY
8 weeks (or 4-week intensive)	**72 hours**	**Intermediate**	**Face-to-face,** Dar es Salaam

Version 1.0 · September 2026 · Kevajopa Technologies Limited, P.O. Box 53028, Dar es Salaam, Tanzania

info@kevajopa.co.tz · +255 782 444 470 · www.kevajopa.co.tz

About Kevajopa Technologies Limited

Kevajopa Technologies Limited is a Tanzanian ICT company registered in Dar es Salaam in February 2024 (Registration No. 172177301) and working across five practice areas: ICT solutions, software development, networks and infrastructure, security systems, and training. We are an authorised Hikvision dealer and training partner, and an active supplier on the National e-Procurement System of Tanzania (NeST).

Our training practice exists because of what we see in the field. We install the systems, we build the applications, and we supply the equipment — which means we spend a great deal of time inside organisations looking at how their controls actually behave rather than how the policy says they behave. That experience is what this programme is built from.

Kevajopa currently runs seventeen professional ICT programmes. This one sits alongside our IT Audit and Digital Forensics programme (ITAF-2026-011) and our Cyber Security Professional Certificate, and is described in relation to both on page 4 so that you choose the right one.

The Problem This Programme Addresses

Most organisations in Tanzania now hold their financial records, their customer data and their operational history in systems that nobody in the organisation is formally responsible for assuring. Internal audit functions built for cash, stores and procurement are being asked to sign off on access rights, change logs and backup regimes. External requirements have arrived at the same time: the Personal Data Protection Act 2022 created obligations that are audited rather than assumed, regulated institutions face supervisory expectations around IT risk, and public entities are increasingly examined on the systems behind the numbers rather than only the numbers.

The practical result is a shortage of people who can walk into a server room, a finance office and an IT manager's meeting in the same week and produce a defensible opinion. It is not a shortage of people who can name frameworks.

> **THE DISTINCTION THIS PROGRAMME IS BUILT ON**
>
> Knowing that COBIT exists is not an audit skill. Being able to take a control objective, turn it into a test, execute that test against a real population, and write a finding that survives a hostile exit meeting — that is an audit skill. This programme spends its time almost entirely on the second thing.

Who This Programme Is For

The programme is designed for professionals who are already responsible for assurance, control or systems, and who need the specific discipline of auditing information systems.

- Internal auditors and audit assistants who are being given IT scope for the first time
- Accountants, finance officers and compliance officers who must rely on system-generated evidence
- IT officers, system administrators and network staff who are audited, and who would work far better with the audit function if they understood what it is looking for
- Risk and governance staff in banks, microfinance institutions, SACCOS, insurers and public entities
- Graduates in accounting, finance, information systems or computer science preparing for an audit career or for CISA-style examinations
- Consultants and ICT service providers who are asked by clients for control reviews and currently have no method for them

Entry Requirements

- A degree, diploma or professional qualification in accounting, finance, audit, information systems, computer science or a related field — or two years of relevant working experience in place of it
- Working comfort with a computer, a browser and a spreadsheet. You must be able to sort, filter and use basic formulas in Excel
- No programming experience is required. Week 5 introduces scripted analysis, but everything is demonstrated from zero and all assessed work can be completed in a spreadsheet
- Adequate written English — a substantial part of the assessment is writing findings and a report

Choosing Between Our Three Related Programmes

Three Kevajopa programmes touch this territory. They are different jobs and they are deliberately not merged.

PROGRAMME	CENTRAL QUESTION	YOU LEAVE ABLE TO	BEST FOR
IT Auditing and Controls Assurance (this programme)	Is the control working, and can I prove it?	Plan, test and report a full IT audit engagement	Auditors, accountants, risk and compliance staff
IT Audit and Digital Forensics (ITAF-2026-011)	What happened, and what can be shown as evidence?	Preserve, examine and present digital evidence after an incident	Investigators, fraud and forensic units
Cyber Security Professional Certificate	How is the system attacked and defended?	Build, harden and monitor defensive controls	IT and security operations staff

If you are unsure, the short version: audit tells you whether the control is there and working, forensics tells you what happened after it failed, and cyber security is the work of making it work in the first place.

What You Will Be Able To Do

On completing the programme you will be able to:

1. Build a risk-based IT audit plan and scope a single engagement, with objectives, criteria, and a defensible statement of what is out of scope and why.
2. Write an audit programme that turns a control objective into specific, executable tests with stated evidence requirements and sample sizes.
3. Test IT general controls across access management, change management, IT operations, and physical and environmental security.
4. Establish the completeness and integrity of a population before testing it — the single most common failure in IT audit work.
5. Test application controls and run analytics over a full data population rather than a sample, using spreadsheet techniques and a basic scripted approach.
6. Assess infrastructure, cloud and third-party arrangements, including reading a third-party assurance report and finding what it excludes.
7. Prepare working papers that a second auditor can follow to the same conclusion without asking you a question.
8. Write a finding with its condition, criteria, cause, effect and recommendation, rated for risk and separated from the person who happened to be at the keyboard.
9. Handle an exit meeting, disagreement and management response, and maintain a follow-up register that closes issues on evidence rather than on assurance.
10. Locate your work correctly against COBIT 2019, ISO/IEC 27001, the ISACA ITAF standards, and the Tanzanian legal and regulatory environment including the Personal Data Protection Act 2022.

How the Programme Is Taught

Every Kevajopa programme is taught the same way, and it is unusual enough to explain properly.

Each week contains one planted failure. Something in the week — a report, an export, a log, a register, a scan result — is accurate, complete on its own terms, and entirely misleading. It is never announced. Participants work with it, reach a confident conclusion, and are then shown what the evidence could not have told them.

> **THE ARGUMENT THE EIGHT WEEKS ARE MAKING**
>
> Week 3's access review reconciles perfectly against a list drawn from the same source. Week 4's change log shows every change approved, because it only knows about changes made through the tool. Week 5's duplicate test returns zero, because the field it tested is unique by construction. Week 6's vulnerability scan is clean on the subnet it was given.
>
> By Week 7 the sentence writes itself, and participants usually say it before the tutor does: every report you were handed was accurate; the population it described was not the population that exists.

This is not a teaching device invented for the classroom. It is the recurring reason real audits miss things, and an auditor who has been caught by it four times in eight weeks tends not to be caught by it in the field.

Session Format

- Three sessions a week, three hours each — nine contact hours a week, the standard Kevajopa pattern
- Roughly one third instruction, two thirds work: testing, sampling, documenting, drafting

- Everything is produced against a running case entity used all eight weeks, so the work compounds instead of resetting each session
- Maximum of twelve participants, so that working papers can be reviewed individually

Week-by-Week Syllabus

Eight weeks, twenty-four sessions, seventy-two contact hours. Each week is three sessions of three hours.

WEEK 1 · 9 HOURS

The Audit Function and Its Standards

What an IT audit actually is, who it answers to, and where its authority comes from. The week that stops participants confusing assurance with consulting, and consulting with security testing.

- **1.1** Assurance, consulting and security testing — three different jobs with three different independence requirements. The three lines model and where internal audit sits. Independence and objectivity in an organisation where you know everybody.
- **1.2** The standards landscape and how a framework becomes audit criteria: ISACA ITAF, the IIA standards, COBIT 2019, ISO/IEC 27001:2022, NIST CSF. Choosing criteria you can hold an entity to rather than criteria that sound impressive.
- **1.3** The Tanzanian environment: the CAG and public sector IT audit, PPRA and procurement records, supervisory expectations for regulated financial institutions, TCRA obligations, and the Personal Data Protection Act 2022 with the Commission it created.

> **THE PLANTED FAILURE**
>
> The case entity's access control policy is current, comprehensive, board-approved and signed by everyone who should have signed it. It has never once been performed. Criteria without evidence of operation is not a control, and a signed policy is the easiest thing in an audit to mistake for one.

WEEK 2 · 9 HOURS

Risk Assessment, Scoping and the Audit Plan

Deciding what to audit, and then deciding what one engagement will and will not cover. Most weak audits were weak before any testing started.

- **2.1** The audit universe and the risk-based annual plan: identifying auditable entities, rating them, and defending the ranking to a committee that has its own view.
- **2.2** Scoping one engagement — objectives, criteria, period under review, systems in and out, and materiality in an IT context where the loss is often not a number. Drafting the engagement letter.
- **2.3** Designing the audit programme: from objective to test to evidence requirement. Resourcing and timing, the entrance meeting, and managing an auditee who has decided in advance what the report will say.

> **THE PLANTED FAILURE**
>
> The risk register is complete, ranked, dated and signed. Every risk on it is a risk somebody thought of. The largest operational loss of the last two years does not appear on it in any form, and nobody has noticed because the register has never been tested against events.

WEEK 3 · 9 HOURS

IT General Controls I — Access Management

The control area that produces more findings than any other, and the week where testing technique is taught properly.

- **3.1** The identity lifecycle: joiners, movers and leavers. Privileged accounts, service accounts, shared accounts, and the local accounts that no directory knows about. Why the mover is more dangerous than the leaver.
- **3.2** Authentication and authorisation, segregation of duties in an ERP or core banking context, and the user access review — how it is meant to work and the four ways it is usually performed without being performed.
- **3.3** Testing technique: enquiry, observation, inspection and re-performance, and what each is worth as evidence. Sampling — how a sample size is arrived at and what a clean sample does and does not permit you to say.

> **THE PLANTED FAILURE**
>
> The leavers list from HR reconciles exactly against the directory export. It reconciles because both are drawn from the same HR system. The two contractors who were engaged directly by the project office and never entered into HR appear on neither list, and both still have active accounts.

WEEK 4 · 9 HOURS

IT General Controls II — Change and Operations

The controls that decide whether the system you tested in January is the system running in June.

- **4.1** Change management: request, approval, testing, and segregation between the person who writes a change and the person who releases it. Emergency change, and the retrospective approval that is the whole population's weak point.
- **4.2** IT operations: job scheduling and batch failure handling, backup regimes, and restore testing — the difference between a backup that exists and a backup that has been proven. Incident and problem management, and capacity.
- **4.3** Physical and environmental controls: data room access, power and cooling, and using access control and CCTV records as audit evidence — including their retention limits and what makes them admissible internally.

> **THE PLANTED FAILURE**
>
> One hundred per cent of changes in the change management tool were approved before release. The tool records changes that were made through the tool. The database correction applied at the console at 23:40 on a month-end night is not in the population, and the population is where the audit went wrong — not the testing.

WEEK 5 · 9 HOURS

Application Controls and Audit Data Analytics

Moving from the environment around the system to the system's own controls, and from sampling to testing everything.

- **5.1** Input, processing, output and interface controls. Reconciliations, control totals, exception reports, and the recurring finding that an exception report is produced daily and read by nobody.
- **5.2** Analytics over a full population: duplicates, sequence gaps, round-sum values, out-of-hours postings, ageing, and same-supplier different-reference patterns. What each test is actually evidence of.

- **5.3** Working reproducibly — keeping the query with the working paper so a second auditor can re-run it. A short, from-zero introduction to scripted analysis for those who want it; the assessed work can be done entirely in a spreadsheet.

> **THE PLANTED FAILURE**
>
> The duplicate payment test over the full year returns zero duplicates. The reference number is system-generated and unique by construction, so testing it for duplicates was always going to return zero. The genuine duplicates share supplier, amount and date, and differ only in the one field that was tested.

WEEK 6 · 9 HOURS

Infrastructure, Cloud and Cyber Security in Audit Scope

Auditing the technical estate without becoming a penetration tester, and auditing what you no longer own. Includes the graded mid-programme practical test.

- **6.1** Network, server and endpoint controls in audit terms. Patch and vulnerability management, hardening standards, logging and monitoring — and what it means for an auditor to conclude on a log that only the audited party can produce.
- **6.2** Cloud and outsourcing: shared responsibility, what the SLA actually commits to, right-to-audit clauses, and reading a third-party assurance report — in particular finding the carve-outs, the exceptions and the period it does not cover.
- **6.3** Mid-programme practical test (graded, 10%): a scoped control area, tested and documented in one session.

> **THE PLANTED FAILURE**
>
> The vulnerability scan report is clean. The scan authenticated to, and covered, the subnet the IT manager supplied. Two servers were moved during a migration eighteen months ago into a range that appears on no current diagram and in no scan scope, and they answer to nobody.

WEEK 7 · 9 HOURS

Evidence, Findings and the Audit Report

The week that decides whether eight weeks of work changes anything. Most audit work that is technically correct fails here.

- **7.1** Working papers: what has to be in them for a second auditor to reach your conclusion unaided. Evidence quality, sufficiency, and retention. Cross-referencing that survives review.
- **7.2** The finding: condition, criteria, cause, effect and recommendation. Root cause against symptom — and the discipline of separating the control failure from the individual who happened to be at the keyboard. Risk rating that means the same thing to every reader.
- **7.3** Writing the report, agreeing management responses, and running an exit meeting including one where the auditee disagrees. The follow-up register, and closing an issue on evidence rather than on an assurance that it has been dealt with.

> **THE PLANTED FAILURE**
>
> A finding drafted in Session 7.2 is factually correct in every particular and identifies the wrong cause. The officer named in it had no access to the information the finding says she should have acted on. The class marks it correct, and then reads her job description.

WEEK 8 · 9 HOURS

Governance, Compliance and Capstone

The layer above the controls, the legal obligations around them, and the assessed engagement that closes the programme.

- **8.1** Auditing governance with COBIT 2019: governance against management objectives, the IT steering committee, project and investment oversight, and how to audit a decision rather than a system.
- **8.2** Compliance and resilience: obligations under the Personal Data Protection Act 2022 and how they are evidenced, business continuity and disaster recovery testing, and quality assurance of the audit function itself.
- **8.3** Capstone presentation, exit-meeting defence and written examination.

> **THE PLANTED FAILURE**
>
> Week 8 plants nothing new. The capstone entity contains three of the seven failures from earlier weeks, unlabelled and rearranged. Participants who have understood the programme find them without being told to look.

The Case Entity, Materials and Tools

The programme runs on a single fictional entity — a mid-sized Tanzanian organisation with a finance system, a directory, a change tool, a helpdesk, a data room and an outsourced hosting arrangement. It is used from Week 1 to Week 8, so a scoping decision made in Week 2 constrains what can be tested in Week 5, exactly as it does in practice.

- Complete document set: policies, registers, org charts, contracts, service reports and prior-year audit files, all internally consistent and containing the planted failures
- Real data populations — payment, ledger, access, change and log extracts sized to make full-population analytics meaningful and sampling necessary
- A live directory, ticketing and access-control environment on Kevajopa's own server for the technical sessions, so evidence is gathered from a running system rather than a screenshot
- Kevajopa working paper, audit programme, finding and report templates, which participants keep and may use in their own organisations
- Per-week guides, lab worksheets and slide sets, issued through the Kevajopa training portal
- Software: Microsoft Excel or LibreOffice Calc throughout; Python and pandas demonstrated in Week 5 and provided pre-configured for anyone who wants it

Assessment and Certification

Assessment is continuous and almost entirely practical. There is no assessment that consists of naming a framework.

COMPONENT	WEIGHT	WHAT IS MARKED
Continuous practical work	20%	Weekly testing and working papers, marked for whether a second auditor could follow them to the same conclusion
Planning and programme portfolio	15%	The risk assessment, scope, engagement letter and audit programme produced in Week 2 and refined through the programme
Mid-programme practical test	10%	One scoped control area tested and documented under time constraint in Session 6.3
Capstone engagement	35%	A full engagement on the case entity: plan, test, findings, report, and an oral exit-meeting defence in which the tutor plays a disagreeing auditee
Written examination	20%	Standards, criteria, method and judgement, taken in Session 8.3

Certification

- A Kevajopa Technologies Limited Professional Certificate in IT Auditing and Controls Assurance is awarded on an overall mark of 60% or above, with a hard floor of 50% on the capstone.
- Minimum 80% attendance is required. Attendance is recorded per session.
- Participants below the threshold receive a statement of attendance and may re-sit the capstone with a later intake at no additional tuition charge.
- The certificate is a Kevajopa award. It is not a CISA, CIA or ISO certification and we do not represent it as one — but it maps closely onto the CISA domains and is deliberately structured to be useful preparation for candidates working towards that examination.

Delivery Options and Schedule

The same syllabus, the same 72 contact hours, the same assessment and the same certificate. Choose the pattern that fits your work.

	OPTION A — PART-TIME	OPTION B — INTENSIVE
Duration	8 weeks	4 weeks
Pattern	3 sessions a week, 3 hours each	6 sessions a week, 3 hours each
Typical days	Tuesday, Thursday, Saturday	Monday to Saturday
Hours	Weekday sessions after 16:00; Saturday morning	09:00–12:00 and 13:00–16:00
Suits	Participants in full-time employment	Graduates, and staff released for training

	OPTION A — PART-TIME	OPTION B — INTENSIVE
Total	72 contact hours	72 contact hours

Exact session days are confirmed with each intake, since a cohort drawn mostly from one employer will usually want a pattern built around their own working week. Corporate cohorts are scheduled entirely to the client's convenience and can be delivered on the client's premises.

> **INTAKE DATES**
>
> We do not advertise a fixed calendar. An intake is scheduled as soon as four participants have confirmed, and confirmed participants are given at least ten working days' notice of the start date. This keeps class sizes small and means nobody waits three months for a term to begin.

Fees

All figures are in Tanzanian Shillings. Kevajopa Technologies Limited is not VAT-registered; no VAT is charged and none should be added to any payment.

	AMOUNT (TZS)	NOTES
Registration fee	30,000	One-off, non-refundable, payable with the registration form
Tuition — individual	700,000	Either delivery option
Total, individual	730,000	
Tuition — group rate	630,000 each	Three or more participants registering together
Corporate cohort	5,200,000	Up to eight participants, deliverable at the client's premises
Additional corporate seat	600,000 each	Beyond the eighth participant

What the Fee Includes

- All 72 contact hours and all tuition
- The complete document set, data populations, worksheets and slide material
- Kevajopa working paper, audit programme, finding and report templates, retained by the participant
- Portal access for the duration of the programme and for six months afterwards
- All assessment, marking and the certificate
- Refreshments at Kevajopa's Dar es Salaam training room

Payment Options

1. Payment in full before the first session.
2. Fifty per cent deposit before the first session, balance by the end of Week 4.
3. Forty, thirty, thirty — before Week 1, before Week 4 and before Week 7 — available on request.

- A place is confirmed by the registration fee together with a deposit of at least 50% of tuition.
- Certificates are issued only when the account is settled in full.
- Public entities deduct 2% withholding tax at source in accordance with Tanzanian law; the withholding certificate should be issued to Kevajopa Technologies Limited, TIN 172-177-301.
- Withdrawal before the first session: the tuition deposit is refunded in full, less the registration fee. After the first session, tuition is not refundable, but the place may be transferred to a later intake once.

What This Programme Does Not Cover

Stated plainly so that nobody registers expecting the wrong thing.

- It is not penetration testing or ethical hacking. Technical security testing is covered as something an auditor commissions, scopes and reviews — not as something the auditor performs.
- It is not digital forensics. Evidence preservation, imaging, chain of custody and examination are the subject of ITAF-2026-011.
- It is not financial statement auditing. We assume you either have that discipline already or do not need it.
- It does not confer CISA, CIA, CISSP or ISO certification, and does not include the examination fee for any of them.
- It does not cover audit software licensing — ACL, IDEA, TeamMate and similar. The techniques are taught in tools you already own; the concepts transfer directly if your employer licenses a dedicated platform.
- It does not cover auditing under IFRS or public sector accounting standards.

Registration and Next Steps

1. Request the registration form for ITA-2026-019 by email or WhatsApp, or collect it from our office.
2. Return the completed form with a copy of your national identification and your highest qualification.
3. Pay the registration fee and your chosen deposit. Bank and mobile money details are issued with the form.
4. You will receive written confirmation, the intake start date once the cohort is confirmed, portal login details and the Week 1 pre-reading.

Employers registering three or more participants, or a full corporate cohort, should contact us directly — the syllabus can be weighted towards your sector, and the case entity can be adapted to resemble your own environment without using your real data.

KEVAJOPA TECHNOLOGIES LIMITED

P.O. Box 53028, Dar es Salaam, Tanzania

info@kevajopa.co.tz · +255 782 444 470 · www.kevajopa.co.tz

Managing Director: James Alex Masoy · jamasoy@kevajopa.co.tz

Registered in Dar es Salaam under the Companies Act 2002 · Reg. No. 172177301 · TIN 172-177-301 · Not VAT-registered · Authorised Hikvision Dealer and Training Partner