DATA PROTECTION AND CYBERSECURITY

CORPORATE TRAINING CURRICULUM 2026

Short-Term Programmes • 10-Day Programmes • Master Classes

Data Protection • Cybersecurity • Digital Forensics & Incident Response • OSINT • Governance, Risk & Ethics

Accredited by NITA, the ICT Authority and the Office of the Data Protection Commissioner

southendtech.co.ke • info@southendtech.co.ke • +254 721864169 or +254728223333

November 2026

Contents

1. About This Curriculum
2. Programme Framework
3. Short-Term Programmes (3–5 Days)
4. 10-Day Practitioner Programmes
5. Master Class Programmes
6. Assessment, Certification and Quality Assurance
7. Annexes and How to Book

Course finder

If you are…	Start with	Then progress to
Staff handling personal data (ICT, HR, marketing, finance, customer service)	ST-01	TD-01
A data protection regulator or authority	ST-02	TD-01, MC-02
An NGO, UN agency or humanitarian organisation	ST-03	TD-01
ICT, security or SOC staff	ST-04, ST-08	TD-02, MC-06
An incident response, legal or risk officer	ST-05	TD-02
An investigator, auditor or law-enforcement officer	ST-06, ST-07	TD-03, MC-05
A journalist, fact-checker or human-rights defender	ST-07	TD-03, MC-04
A senior DPO, architect or AI governance lead	TD-01	MC-03
A board member or senior executive	MC-01	—

1. About This Curriculum

South-End Tech Limited offers one integrated training curriculum in data protection and cybersecurity, delivered in three tiers: Short-Term Programmes (3–5 days), 10-Day Practitioner Programmes and Master Classes (2–3 days). Its 17 courses cover five domains: data protection and privacy; data security and cybersecurity; digital forensics and incident response (DFIR); open-source intelligence (OSINT); and governance, risk and ethics.

1.1 About South-End Tech Limited

South-End Tech Limited is a consulting firm specialising in Data Protection Services, Cybersecurity Solutions, Data Governance and Management, and Digital Solutions.

Vision	To build trust in data and cyberspace.
Mission	To ensure responsible data use and safe cyberspace for all through global support.
Core values	Teamwork • Passion • Respect • Innovation
Accreditation	National Industrial Training Authority (NITA); Information and Communication Technology (ICT) Authority; Office of the Data Protection Commissioner (ODPC)

1.2 Why this training matters

Every organisation now stores, accesses and shares large volumes of personal and confidential data electronically, with staff, clients, vendors and partners. The same technology brings new threats: ransomware, business email compromise, insider misuse, data leaks and manipulated media. Regulators, meanwhile, are moving from awareness to active enforcement.

Training helps an organisation prevent a breach and, when one occurs, limit the damage and its liability to regulators, data subjects and third parties. This curriculum builds that capacity from front-line staff to the board, and equips regulators to supervise and enforce effectively.

1.3 What your organisation gains

The programmes aim to:

1. Build awareness of the legal, regulatory and policy frameworks for data protection and cybersecurity.
2. Develop a culture of data ethics, privacy by design and security by default.
3. Give organisations a practical roadmap to compliance and cyber resilience.
4. Build hands-on technical capacity to secure systems, respond to incidents, investigate and preserve digital evidence, and gather open-source intelligence lawfully.

Expected outputs are stronger staff, supervisor and management capacity; privacy embedded in daily operations; working data governance and incident-response frameworks; and defensible investigation and evidence-handling practice.

1.4 Who we train

Sector	Typical participants	Recommended entry point
Public sector regulators	Data protection authorities and commissioners' offices, ICT and cybersecurity authorities, communications regulators, sector regulators (financial, health, telecoms)	ST-02, then TD-01 and MC-02
Other public sector bodies	Ministries, departments, agencies, county and local governments, law enforcement, judiciary and prosecution staff	ST-01, ST-06 or ST-07, then TD-03
Private sector	Banks, SACCOs, fintechs, insurers, telecoms, health providers, retailers, SMEs; DPOs, ICT, HR, legal, risk, audit and marketing teams	ST-01, ST-04, TD-01 or TD-02
Non-profit organisations	NGOs, CBOs, foundations, faith-based organisations, research institutions	ST-01, ST-03
Humanitarian entities	UN agencies, international NGOs, refugee and relief programmes handling beneficiary and biometric data	ST-03, then TD-01
Media and civil society	Investigative journalists, fact-checkers, human-rights defenders	ST-07, TD-03, MC-04
Boards and executives	Board members, CEOs, CFOs, CIOs, CISOs, heads of legal and risk	MC-01

1.5 Built on proven programmes

This curriculum consolidates five South-End Tech programmes: the Data Protection Legal and Technical Training Manual, the Industrial Cybersecurity Facilitation Plan, the Ethical Hacking Training Programme, the OSINT Curriculum and Facilitation Plan, and the Digital Forensics and Incident Response Services Portfolio.

2. Programme Framework

The curriculum has 17 courses across three tiers. Short-term courses build awareness and core skills; 10-day programmes build practitioner competence; master classes serve senior leaders and specialists.



Figure 1: The three programme tiers.

2.1 Programme tiers

Tier	Duration	Level	Primary purpose	Courses	Credential
Short-Term Programmes	3–5 days	Foundation to intermediate	Awareness, compliance basics and entry-level technical skills	ST-01 to ST-08	Certificate of Completion
10-Day Programmes	10 days (2 weeks)	Intermediate to practitioner	Job-ready competence, assessed labs and a capstone	TD-01 to TD-03	Certificate of Competence (Practitioner)
Master Class Programmes	2–3 days	Advanced and executive	Strategy, leadership, advanced tradecraft and emerging issues	MC-01 to MC-06	Master Class Certificate

2.2 Course catalogue

Code	Course	Days	Domain
ST-01	Data Protection and Privacy Compliance Essentials	3	Data protection
ST-02	Data Protection Supervision, Investigation and Enforcement for Regulators	5	Data protection (regulators)
ST-03	Data Protection in Humanitarian and Non-Profit Operations	3	Data protection

Code	Course	Days	Domain
ST-04	Cybersecurity and Data Security Foundations	5	Cybersecurity
ST-05	Incident Response and Personal Data Breach Management	3	DFIR / data protection
ST-06	Digital Forensics Foundations	5	Digital forensics
ST-07	Open-Source Intelligence (OSINT) Foundations	5	OSINT
ST-08	Ethical Hacking and Penetration Testing Foundations	3	Cybersecurity
TD-01	Certified Data Protection Practitioner (DPO) Programme	10	Data protection and security
TD-02	Cybersecurity Operations and Incident Response Programme	10	Cybersecurity and DFIR
TD-03	Digital Forensics and OSINT Investigations Programme	10	Forensics and OSINT
MC-01	Board and Executive Master Class: Data Governance, Cyber Risk and Crisis Leadership	2	Governance
MC-02	Regulators' Master Class: Advanced Supervision, Cross-Border Transfers and Emerging Technology	3	Data protection (regulators)
MC-03	Privacy Engineering and AI Governance Master Class	2	Data protection and security
MC-04	Advanced OSINT and Counter-Disinformation Master Class	3	OSINT
MC-05	Advanced DFIR and Expert Witness Master Class	3	Digital forensics
MC-06	Adversary Emulation: Active Directory Attack and Defence Master Class	3	Cybersecurity

2.3 A Standard Training Day

Time	Session
8:30 – 9:00 AM	Registration, recap and daily objectives
9:00 – 10:30 AM	Session 1: concepts and frameworks
10:30 – 11:00 AM	Tea break
11:00 AM – 1:00 PM	Session 2: deep dive, demonstrations and case studies
1:00 – 2:00 PM	Lunch break
2:00 – 3:30 PM	Session 3: practical lab, simulation or group work

Time	Session
3:30 – 4:30 PM	Session 4: exercise debrief, quiz and reflection

2.4 How we teach

Delivery is learner-centred and practical. Participants are encouraged to bring and share their own organisational experience.

- **Knowledge sessions:** short lectures, guided discussion, and question-and-answer.
- **Applied learning:** case studies, role-play, group work and best-practice reviews.
- **Technical practice:** hands-on labs, demonstrations, capture-the-flag (CTF) games and sourcing challenges.
- **Simulation:** tabletop breach exercises, mock regulatory investigations and moot court testimony.
- **Multimedia:** videos, documentaries and podcasts for discussion (for example, Darknet Diaries and BBC Africa Eye).

2.5 Delivery options

- **Open (public) courses** at South-End Tech's training venue or partner venues.
- **In-house courses** customised to one organisation's sector, systems and policies.
- **Virtual instructor-led** delivery with cloud-hosted labs.
- **Blended delivery** combining self-paced pre-work, live sessions and online labs.

2.6 Prerequisites

Tier	Prerequisites
Short-term, non-technical (ST-01, ST-02, ST-03, ST-05)	None beyond basic computer literacy
Short-term, technical (ST-04, ST-06, ST-07)	Comfort with computers, browsers and common productivity tools; no prior Linux needed
ST-08 Ethical Hacking	Cybersecurity essentials, networking fundamentals, Linux and Windows basics (or ST-04)
10-Day Programmes	A related short-term course or equivalent work experience
Master Classes	Senior role or 3+ years of relevant experience; MC-05 and MC-06 require TD-02 or TD-03 level skills

2.7 Code of conduct for technical training

All offensive security, forensics and OSINT techniques are taught and practised only in authorised lab environments or against publicly available information. Participants sign an ethics and lawful-use undertaking before technical courses. Data minimisation and OPSEC are reinforced in every session.

3. Short-Term Programmes (3–5 Days)

Eight short courses build awareness and core skills in one working week or less. Each can run as an open course or be tailored in-house to one organisation.

ST-01 Data Protection and Privacy Compliance Essentials

COURSE CODE	DURATION	LEVEL	CREDENTIAL
ST-01	3 days	Short-Term	Completion

Who should attend: Non-supervisory staff and mid-level managers who handle client, employee or sensitive personal data: ICT, HR, marketing, communications, finance, customer service and records teams.

Learning objectives

By the end, participants will be able to:

1. Identify the legal and regulatory framework for data protection that applies to their organisation.
2. Handle personal data lawfully online and offline, and recognise special categories of data.
3. Explain data subject rights and how to respond to requests.
4. Recognise a personal data breach and the organisation's liability for it.
5. Contribute to a data protection gap assessment and implement internal policies.

Course outline

Day	Topics	Practical / activity
1	Legal and regulatory frameworks; objectives of the Data Protection Act; key terms (personal data, data subject, controller, processor); what is and is not personal data; special categories and sensitive personal data	Data classification exercise using sample records
2	Principles of data processing; lawful bases; consent; data subject rights; duties of controllers and processors; registration with the regulator; data sharing and third parties	Role play: handling a data subject access request
3	Personal data breaches and liability; administrative fines and enforcement; technical and organisational safeguards; gap and risk assessment; policies, procedures and a culture of compliance	Case study of a regulator's enforcement decision; post-assessment

ST-02 Data Protection Supervision, Investigation and Enforcement for Regulators

COURSE CODE	DURATION	LEVEL	CREDENTIAL
ST-02	5 days	Short-Term	Completion

Who should attend: Staff of data protection authorities and public bodies responsible for regulating privacy: compliance officers, investigators, complaints handlers, legal officers and registration staff.

Learning objectives

By the end, participants will be able to:

1. Apply the national data protection law and its regulations consistently to real cases.
2. Run a registration, complaints-handling and investigation process from intake to decision.
3. Assess breach notifications and the technical adequacy of an organisation's safeguards.
4. Draft enforcement notices, penalty decisions and guidance that withstand appeal.
5. Handle digital evidence and technical evidence lawfully during investigations.

Course outline

Day	Topics	Practical / activity
1	Mandate and powers of the regulator; constitutional right to privacy; national, regional (Malabo Convention, EAC) and international (GDPR, Convention 108+) benchmarks; regulator independence and ethics	Mapping exercise: regulatory powers vs. obligations of controllers
2	Registration of controllers and processors; compliance audits and inspections; DPIA review; codes of practice and sector guidance; risk-based supervision planning	Mock compliance audit of a sample organisation
3	Complaints handling; investigation planning; interviews; requests for information; evidence gathering; basics of digital evidence and chain of custody	Simulated complaint: from intake to investigation plan
4	Breach notification assessment; technical safeguards review (encryption, access control, logging, DLP); reading incident and forensic reports; cross-border transfer assessments	Tabletop: assessing a breach notification from a bank
5	Enforcement notices; administrative fines and proportionality; drafting reasoned decisions; appeals and judicial review; public communication and awareness campaigns	Moot: drafting and defending a penalty decision; post-assessment

ST-03 Data Protection in Humanitarian and Non-Profit Operations

COURSE CODE	DURATION	LEVEL	CREDENTIAL
ST-03	3 days	Short-Term	Completion

Who should attend: Programme, M&E, protection, cash-transfer, ICT and data management staff of NGOs, UN agencies, humanitarian and relief organisations.

Learning objectives

By the end, participants will be able to:

1. Apply data protection principles to beneficiary, donor and staff data in fragile and emergency settings.
2. Identify lawful bases suited to humanitarian work, including vital interest and public interest.
3. Conduct a DPIA for biometrics, digital cash and mobile data collection.
4. Manage data sharing with donors, governments and partners responsibly.

Course outline

Day	Topics	Practical / activity
1	Humanitarian data ecosystem; national laws and international guidance (ICRC Handbook on Data Protection in Humanitarian Action, IASC Operational Guidance on Data Responsibility); "do no harm" and vulnerable groups; consent in crisis settings	Mapping the data flow of a refugee registration programme
2	Biometrics, digital identity and cash-transfer programmes; mobile data collection tools; data minimisation and retention; data sharing agreements with donors and governments; cross-border transfers	DPIA workshop for a biometric cash-transfer project
3	Field data security: devices, encryption, secure messaging; breach response in low-connectivity settings; staff OPSEC; community feedback mechanisms and data subject rights	Tabletop: lost field tablet with beneficiary records; post-assessment

ST-04 Cybersecurity and Data Security Foundations

COURSE CODE	DURATION	LEVEL	CREDENTIAL
ST-04	5 days	Short-Term	Completion

Who should attend: ICT officers, system administrators, data protection and compliance staff, and professionals moving into security roles.

Learning objectives

By the end, participants will be able to:

1. Explain the "why" behind cybersecurity, the CIA triad and risk management principles.
2. Understand networks, cryptography, identity, cloud and zero trust.
3. Recognise attack types, threat actors and the kill chain.
4. Select and configure core security controls that protect personal data.

Course outline

Day	Topics	Practical / activity
1	Need for security; CIA triad; cybersecurity risk management; identity, authentication, authorisation and auditing (IAAA); security compliance and frameworks (ISO/IEC 27001, NIST CSF, CIS Controls)	Risk register exercise for a sample organisation
2	Networking fundamentals: OSI and TCP/IP models; network security design; Wireshark; enterprise applications; cryptography and what it protects (at rest, in transit)	Wireshark packet analysis lab; encryption lab
3	Zero trust architecture; securing the cloud; data security controls: classification, encryption, access control, backup, data loss prevention (DLP)	Configure a DLP policy and cloud access controls
4	Understanding cyber attacks: threat actors; malware; attack vectors; attack kill chain; MITRE ATT&CK; indicators of compromise; physical and social engineering attacks	Map a real attack (e.g. SolarWinds, Colonial Pipeline) to ATT&CK
5	Defensive controls: firewalls, WAF, IDS/IPS, antivirus and EDR, email protection; vulnerability management and patching; Nessus scanning basics	Vulnerability scan and remediation plan; post-assessment

ST-05 Incident Response and Personal Data Breach Management

COURSE CODE	DURATION	LEVEL	CREDENTIAL
ST-05	3 days	Short-Term	Completion

Who should attend: Incident response teams, ICT and security staff, DPOs, legal, communications and risk officers.

Learning objectives

By the end, participants will be able to:

1. Prevent, recognise and assess personal data breaches.
2. Follow the incident response lifecycle and use playbooks.
3. Notify the regulator and affected data subjects on time and correctly.
4. Preserve evidence for legal, regulatory and insurance purposes.

Course outline

Day	Topics	Practical / activity
1	Types and causes of data breaches; NIST incident response lifecycle; the golden hour; incident response team roles and escalation; playbooks and runbooks; DLP alert monitoring	Build an incident response playbook for ransomware
2	Triage, containment and eradication; log and email analysis; evidence preservation and chain of custody; assessing impact on affected individuals; breach notification to the regulator (typically within 72 hours) and to data subjects	Log and phishing email analysis lab; draft a breach notification
3	Media and law enforcement engagement; recovery strategy; lessons learned; writing incident reports; SLAs, KPIs and KRIs; handling data subject rights requests after a breach	Full tabletop breach simulation; post-assessment

ST-06 Digital Forensics Foundations

COURSE CODE	DURATION	LEVEL	CREDENTIAL
ST-06	5 days	Short-Term	Completion

Who should attend: Investigators, law enforcement, auditors, fraud examiners, ICT staff, legal practitioners and regulators' investigators.

Learning objectives

By the end, participants will be able to:

1. Follow a forensically sound process from identification to reporting.
2. Acquire and verify evidence with hashing and chain of custody.
3. Examine computer, mobile, email and cloud evidence at a foundation level.
4. Write a clear forensic report that meets evidentiary standards.

Course outline

Day	Topics	Practical / activity
1	Digital forensics principles; the DFIR lifecycle (prepare, identify, preserve, contain, investigate, eradicate and recover, report and testify); admissibility of electronic evidence; cybercrime and evidence laws; chain of custody	Chain-of-custody documentation exercise
2	Computer forensics: forensic imaging and write-blocking; hash verification; file systems; deleted file recovery and data carving; Windows artefacts (registry, event logs, activity timelines)	Imaging and artefact analysis lab (Autopsy / FTK Imager)
3	Memory and volatile data capture; malware and ransomware triage; root-cause and scope determination	Memory analysis lab (Volatility)
4	Mobile forensics (Android and iOS extraction; WhatsApp, SMS, call logs, mobile money records; location history); cloud and email forensics (header analysis, spoofing, business email compromise)	Email header and BEC investigation lab
5	Network forensics (log analysis, IOC identification, breach timeline reconstruction); multimedia forensics (image tampering, CCTV authenticity); forensic report writing	Mini-case: examine an evidence set and write a report; post-assessment

ST-07 Open-Source Intelligence (OSINT) Foundations

COURSE CODE	DURATION	LEVEL	CREDENTIAL
ST-07	5 days	Short-Term	Completion

Who should attend: Security, intelligence and law enforcement analysts; regulators' investigators; journalists and fact-checkers; corporate risk, fraud and due diligence teams; human rights researchers.

Learning objectives

By the end, participants will be able to:

1. Explain intelligence, the OSINT cycle and its lawful uses.
2. Design and follow a repeatable, documented OSINT process.
3. Work securely and anonymously, applying OPSEC and threat modelling.
4. Collect, verify and document open-source information to an evidentiary standard, within privacy law.

Course outline

Day	Topics	Practical / activity
1	Intelligence: definition, types (HUMINT, SIGINT, GEOINT, OSINT), intelligence cycle, cyber intelligence lifecycle; OSINT definition, cycle, types and sources; goals of OSINT; legal, ethical and privacy framework for OSINT	Class activity: design an OSINT process for a scenario
2	OSINT frameworks (OSINT Framework, IntelTechniques, start.me pages, PTES recon, ARF); threat profile and threat model; OPSEC; anonymity across device, person, service and linkage; avatars (sock puppets) and spotting bots	Phishing quiz; document an avatar design rationale
3	Levels of the internet: surface, deep and dark web; advanced search operators (dorking); public records and registries; dark web intelligence with legal and safety limits	Sourcing games: Game 1
4	Investigative platform: virtualisation, Linux 101, Ubuntu, Trace Labs OSINT VM; documentation: screenshots, web archiving, hashing, timelines, link analysis	Build a secure OSINT VM; OverTheWire Bandit starter levels
5	Gathering emails, phone numbers, usernames, locations and connections; SOCMINT (Facebook, X, Instagram, LinkedIn, Telegram); geolocation and chronolocation; reverse image search; metadata analysis	Verification exercise: confirm or debunk a viral image; post-assessment

ST-08 Ethical Hacking and Penetration Testing Foundations

COURSE CODE	DURATION	LEVEL	CREDENTIAL
ST-08	3 days	Short-Term	Completion

Who should attend: ICT and security staff, system administrators, auditors, and regulators' technical staff who assess organisational security.
Prerequisites: Cybersecurity essentials, networking, Linux and Windows fundamentals (or ST-04).

Learning objectives

By the end, participants will be able to:

1. Explain the key concepts, phases and legal boundaries of ethical hacking.
2. Understand and test for the OWASP Top 10 web application vulnerabilities in a lab.
3. Understand the Active Directory attack kill chain and its defences.
4. Scope, run and report an authorised penetration test.

Course outline

Day	Topics	Practical / activity
1	Ethical hacking fundamentals; phases of ethical hacking; rules of engagement, scoping and legal authorisation; OSINT and OPSEC for reconnaissance; introduction to social engineering	Passive reconnaissance lab on a practice target
2	Website penetration testing: importance and need; OWASP Top 10; common open-source tools (Burp Suite, OWASP ZAP, Nmap, Nikto); remediation	Web application testing lab (DVWA / OWASP Juice Shop)
3	Network and Active Directory: enumeration and reconnaissance; local privilege escalation; host persistence; domain reconnaissance; domain privilege escalation; domain persistence; detection and hardening; writing a pentest report	AD lab (TryHackMe / Hack The Box); pentest report; post-assessment

4. 10-Day Practitioner Programmes

Three two-week practitioner programmes build job-ready competence, each ending in an assessed capstone. Week 1 builds the foundations; Week 2 applies them in labs, simulations and a capstone project.

TD-01 Certified Data Protection Practitioner (DPO) Programme

COURSE CODE	DURATION	LEVEL	CREDENTIAL
TD-01	**10 days**	**Practitioner**	**Competence**

Who should attend: Data Protection Officers and their deputies, compliance, legal, risk and audit officers, ICT managers, regulators' staff, and privacy leads in NGOs and humanitarian agencies.

Outcome: Participants can design, run and audit a data protection compliance programme, including its technical safeguards.

Course outline

Day	Theme	Topics	Practical / activity
1	Foundations of privacy law	Right to privacy; history of data protection; national laws and regulations; regional and international frameworks (Malabo Convention, GDPR, Convention 108+); role of the regulator	Pre-assessment; jurisdiction mapping exercise
2	Core concepts and principles	Personal and sensitive data; controllers and processors; principles of processing; lawful bases; consent; children's data; special categories	Lawful basis decision exercise
3	Rights and obligations	Data subject rights and request handling; transparency and privacy notices; registration with the regulator; records of processing activities (ROPA); duties of the DPO	Draft a privacy notice and ROPA entry
4	Governance and accountability	Data governance framework and roles; policies, procedures, standards and guidelines; privacy by design and default; data retention and disposal; vendor and processor management	Build a data governance model for a case organisation
5	Risk and DPIA	Privacy risk assessment; data protection gap assessment; DPIA methodology; legitimate interest assessments; transfer impact assessments; cross-border data transfers	DPIA workshop on a real-world project

Day	Theme	Topics	Practical / activity
6	Data security for privacy	CIA triad; access control and identity; encryption and pseudonymisation; cloud security; backups; DLP administration (policies, patching, monitoring alerts)	DLP configuration and access review lab
7	Breach management	Recognising and assessing breaches; incident response team flow; escalation; notification to the regulator and data subjects; impact on individuals; evidence preservation	Breach notification drafting lab
8	Sector applications	Data protection in banking and fintech, health, telecoms, public sector, education, HR, marketing and CCTV; humanitarian and biometric data; AI and automated decision-making	Sector case study clinics
9	Audit and enforcement	Internal compliance audits; monitoring and KPIs; regulator investigations and enforcement; fines and case law; handling media and law enforcement after a breach	Mock regulatory audit and tabletop breach simulation
10	Capstone	Presentation of a compliance roadmap for a case organisation; written examination; course review	Capstone assessment; post-assessment; certification

TD-02 Cybersecurity Operations and Incident Response Programme

COURSE CODE	DURATION	LEVEL	CREDENTIAL
TD-02	10 days	Practitioner	Competence

Who should attend: ICT and security officers, SOC analysts, system and network administrators, and technical staff of regulators and critical infrastructure operators.
Outcome: Participants can design security controls, monitor and detect threats, test defences ethically and lead a response to a cyber incident. The programme follows four milestones: foundations, understanding attacks, designing controls, and responding to incidents.

Course outline

Day	Theme	Topics	Practical / activity
1	Foundations of information security	Need for security; CIA triad; risk management; IAAA; security compliance and frameworks (ISO/IEC 27001, NIST CSF, CIS Controls)	Pre-assessment; risk register
2	Networks, cryptography and cloud	OSI and TCP/IP models; network security design; Wireshark; enterprise applications; cryptography; zero trust; securing the cloud	Packet analysis and cloud hardening labs
3	Understanding cyber attacks	Threat actors and tactics; malware; attack vectors; attack kill chain; MITRE ATT&CK; TTPs; IOCs; physical attacks; deep dive into the dark web	Case study: SolarWinds and Colonial Pipeline mapped to ATT&CK
4	Ethical hacking and web security	Phases of ethical hacking; rules of engagement; OSINT and social engineering; OWASP Top 10; Nessus and Metasploit in a lab	Web application testing lab
5	Active Directory attack and defence	AD enumeration and reconnaissance; local and domain privilege escalation; host and domain persistence; hardening and detection	AD attack-and-defend lab
6	Designing security controls	Firewalls and WAF; IDS/IPS; antivirus and EDR; email protection; DLP; vulnerability management; zero-day vulnerabilities; patching; system audit	Control design for a mock enterprise; shell scripting basics
7	Security monitoring	Maintenance, monitoring and analysis of audit logs; SIEM purpose and use cases; threat intelligence; threat hunting	SIEM lab (e.g. Wazuh / Splunk / ELK)
8	Incident response	Incident response playbooks; NIST lifecycle; the golden hour; log and email analysis; SOC tasks; SLAs, KPIs and KRIs	Playbook build; phishing investigation lab

Day	Theme	Topics	Practical / activity
9	Forensics and recovery	Incident investigation; forensic triage and evidence preservation; recovery strategy; writing incident reports; breach notification obligations	Full-day ransomware simulation
10	Capstone	Red team / blue team exercise; incident report and executive briefing; written examination	Capstone assessment; post-assessment; certification

TD-03 Digital Forensics and OSINT Investigations Programme

COURSE CODE	DURATION	LEVEL	CREDENTIAL
TD-03	10 days	Practitioner	Competence

Who should attend: Investigators in law enforcement, regulators, anti-corruption and financial intelligence bodies; corporate fraud and risk teams; journalists; human rights and humanitarian investigators.
Outcome: Participants can run a lawful investigation that combines open-source research and digital forensics, and produce court-ready findings.

Course outline

Day	Theme	Topics	Practical / activity
1	Intelligence and legal framework	Intelligence types and cycle; OSINT cycle, sources and goals; constitutional privacy; data protection, cybercrime and evidence laws; ethics, data minimisation and lawful basis	Pre-assessment; design an OSINT process for a scenario
2	OPSEC and investigative technique	Threat profile and model; anonymity layers; secure communication; encrypted containers; avatar management and spotting bots; social engineering; cross-referencing (lessons of the Boston Marathon case)	Avatar rationale; phishing quiz
3	Internet levels and platforms	Surface, deep and dark web; search engine exploitation and dorking; public registries; dark web intelligence (historical marketplaces: Silk Road, AlphaBay, Empire); secure platform (virtualisation, Linux, Trace Labs VM)	Sourcing game; OverTheWire Bandit
4	Collection and SOCMINT	Emails, phone numbers, usernames, locations, connections; selector-based pivoting; Facebook, X, Instagram, LinkedIn and Telegram analysis; lawful scraping	Aware Online OSINT challenge
5	Verification	Geolocation and chronolocation; satellite and thermal imagery (Sentinel Hub, NASA FIRMS); reverse image search; video analysis; deepfake detection; metadata analysis	Verify or debunk conflict footage; confidence-rated report
6	Forensic process and acquisition	DFIR lifecycle; admissibility of electronic evidence; chain of custody; forensic imaging; hashing; write-blockers	Imaging and hashing lab

Day	Theme	Topics	Practical / activity
7	Computer and memory forensics	File systems; deleted file recovery and carving; Windows artefacts; timelines; RAM capture; malware and ransomware analysis	Autopsy and Volatility labs
8	Mobile, cloud and email forensics	Android and iOS extraction; WhatsApp, SMS, call logs and mobile money records; GPS history; email headers, spoofing and BEC; cloud accounts; social media account forensics	BEC investigation lab
9	Network and multimedia forensics; reporting	Network log analysis; IOC and attacker reconstruction; breach timelines; CCTV, audio and image authentication; documentation, link analysis and visualisation; expert report writing	Build a case timeline and link chart
10	Capstone	Full mini-investigation from tasking to archived report, fusing OSINT and forensic findings; moot court testimony	Capstone assessment; post-assessment; certification

5. Master Class Programmes

Six master classes of 2–3 days serve senior leaders, regulators and advanced specialists. They are led by senior practitioners and guest experts, run in small cohorts (maximum 20), and rely on peer exchange, live simulations and current cases rather than lectures.

MC-01 Board and Executive Master Class: Data Governance, Cyber Risk and Crisis Leadership

COURSE CODE	DURATION	LEVEL	CREDENTIAL
MC-01	2 days	Master Class	Master Class

Who should attend: Board members, CEOs, directors, CFOs, CIOs, CISOs, heads of legal, risk and communications, and heads of NGOs and humanitarian country offices.
Outcome: Identify the legal, regulatory and institutional framework; distinguish every stakeholder's role in the data governance framework; build a data ethics culture; and lead the organisation through a cyber or data crisis.

Course outline

Session	Topics
Day 1 AM	Organisational structuring for data privacy compliance through a data governance framework; board duties and personal accountability; compliance as a business continuity need
Day 1 PM	Tools for measuring data privacy and cyber risk; cyber risk quantification and reporting to the board; cost-effective compliance programmes; cyber insurance
Day 2 AM	Corporate data ethics and enterprise risk management (ERM); AI, data monetisation and reputational risk; third-party and supply chain risk
Day 2 PM	Crisis leadership simulation: a live ransomware and data breach scenario; dealing with regulators, law enforcement and the media; post-crisis review

MC-02 Regulators' Master Class: Advanced Supervision, Cross-Border Transfers and Emerging Technology

COURSE CODE	DURATION	LEVEL	CREDENTIAL
MC-02	3 days	Master Class	Master Class

Who should attend: Commissioners, directors and senior officers of data protection authorities, cybersecurity agencies and sector regulators.
Outcome: Stronger regulatory strategy, cooperation and technical capacity for complex, cross-border and technology-driven cases.

Course outline

Session	Topics
Day 1	Regulatory strategy and risk-based supervision; measuring regulatory impact; building investigative and technical capacity inside the authority; independence and accountability
Day 2	Cross-border data transfers and adequacy; regional harmonisation (AU Malabo Convention, EAC, ECOWAS, SADC model law); cooperation and mutual assistance between authorities; big tech and multinational investigations
Day 3	Emerging technology: AI and automated decision-making, biometrics and digital ID, surveillance technology, fintech and digital lending, data in elections; technical deep dive for regulators (reading forensic reports, testing security claims); drafting guidance on new technology

MC-03 Privacy Engineering and AI Governance Master Class

COURSE CODE	DURATION	LEVEL	CREDENTIAL
MC-03	2 days	Master Class	Master Class

Who should attend: Senior DPOs, CISOs, solution architects, data scientists, product leaders and AI governance leads.

Course outline

Session	Topics
Day 1	Privacy by design in system architecture; privacy-enhancing technologies (pseudonymisation, anonymisation, differential privacy, secure enclaves); data mapping automation; consent and preference management; secure software development
Day 2	AI governance frameworks (ISO/IEC 42001, NIST AI RMF, EU AI Act as benchmark); algorithmic impact assessments; bias and fairness; generative AI and data leakage; AI incident response; building an AI use policy

MC-04 Advanced OSINT and Counter-Disinformation Master Class

COURSE CODE	DURATION	LEVEL	CREDENTIAL
MC-04	3 days	Master Class	Master Class

Who should attend: Experienced OSINT analysts, intelligence and law enforcement leads, newsroom verification editors, election bodies, and human rights investigators.
Prerequisites: ST-07 or TD-03.

Course outline

Session	Topics
Day 1	Advanced OPSEC and attribution risk; managing aged avatars at scale; automation and scripting for collection; advanced link analysis (Maltego); managing an OSINT team and case file
Day 2	Advanced geolocation and chronolocation; satellite and thermal imagery; conflict and atrocity verification (Anatomy of a Killing; Sudan, Mozambique and Kunbu-Kumfutu case studies); BBC Africa Eye "Blood Parliament" and Bellingcat methods
Day 3	Coordinated inauthentic behaviour and bot network detection; deepfakes and synthetic media; counter-disinformation workflows; legal limits on publication; Trace Labs Search Party-style CTF

MC-05 Advanced DFIR and Expert Witness Master Class

COURSE CODE	DURATION	LEVEL	CREDENTIAL
MC-05	3 days	Master Class	Master Class

Who should attend: Forensic examiners, incident responders, investigators and legal practitioners.
Prerequisites: ST-06, TD-02 or TD-03.

Course outline

Session	Topics
Day 1	Advanced memory forensics; ransomware investigation and root-cause analysis; threat hunting and compromise assessments; cloud incident response (Microsoft 365, Google Workspace, AWS)
Day 2	Advanced mobile forensics; mobile money and fintech fraud investigation; multimedia authentication (CCTV, audio, image forgery); forensic readiness and evidence handling maturity
Day 3	E-discovery; drafting expert witness reports; courtroom testimony and cross-examination (moot court); running a DFIR retainer and readiness programme

MC-06 Adversary Emulation: Active Directory Attack and Defence Master Class

COURSE CODE	DURATION	LEVEL	CREDENTIAL
MC-06	3 days	Master Class	Master Class

Who should attend: Penetration testers, red and blue team members, SOC leads and senior system administrators.
Prerequisites: ST-08 or TD-02.

Course outline

Session	Topics
Day 1	Threat-informed defence with MITRE ATT&CK; planning an authorised adversary emulation; AD enumeration and reconnaissance; local privilege escalation
Day 2	Host persistence; domain reconnaissance; domain privilege escalation; domain persistence; purple teaming and detection engineering for each stage
Day 3	AD hardening (tiered administration, LAPS, credential protection); full lab-based attack-and-defend exercise; executive-ready reporting

6. Assessment, Certification and Quality Assurance

Every course is evaluated on the Kirkpatrick model, with a pre-assessment before training and a post-assessment at the end. Certificates reflect both technical skill and consistent lawful, ethical conduct.

6.1 Evaluation model (Kirkpatrick)

Level	Measures	Method	When
1. Reaction	Participant satisfaction and relevance	End-of-course evaluation form	Last day
2. Learning	Gain in knowledge and skills	Pre- and post-assessment; quizzes; lab scores	First and last day
3. Behaviour	Use of learning at work	Follow-up survey of participant and supervisor; action plan review	3 months after
4. Results	Impact on the organisation	Compliance indicators, incident metrics, audit findings	6–12 months after (in-house clients)

6.2 Assessment weighting by tier

Component	Short-term	10-day	Master class
Attendance and participation	30%	10%	30%
Quizzes and lab completion	40%	30%	—
Practical exercises and case work	30%	20%	40%
Capstone project	—	30%	—
Written examination	—	10%	—
Strategic action plan or peer presentation	—	—	30%

The pass mark is 60% for short-term and master class courses, and 70% for 10-day programmes. Minimum attendance is 80%.

6.3 Capstones and practical assessments

- **Data protection:** a compliance roadmap, DPIA or mock regulatory decision for a case organisation.
- **Cybersecurity:** a red team / blue team exercise with an incident report and executive briefing.
- **Forensics and OSINT:** a full mini-investigation from tasking to archived report, assessed on method, verification, documentation, OPSEC, and legal and ethical compliance.

6.4 Certification

Credential	Awarded for
Certificate of Attendance	Attending at least 80% of sessions without passing the assessment
Certificate of Completion	Passing a short-term course
Certificate of Competence (Practitioner)	Passing a 10-day programme and its capstone
Master Class Certificate	Completing a master class and its action plan

Courses can also prepare participants for international certifications, such as IAPP (CIPP, CIPM, CIPT), ISACA, EC-Council, CompTIA Security+ and GIAC. Those exams are taken separately.

6.5 Our facilitators

Facilitators are proficient in data protection, cybersecurity, forensics or OSINT, as relevant; conversant with this curriculum; able to consult on the subject matter; and prepared with all materials and labs in place. They are resourceful and able to understand trainees from different perspectives.

6.6 Quality assurance

- The curriculum is reviewed every year, and case studies and legal content are updated at least every six months.
- Labs are isolated, tested before each cohort, and reset after.
- Participant feedback is reviewed after every course, with corrective actions logged.
- For Kenyan employers, evaluation follows National Industrial Training Authority (NITA) guidelines to support training levy reimbursement claims.

7. Annexes and How to Book

Annex A: Legal and Regulatory Frameworks

Each course is anchored on the participants' own jurisdiction, with Kenya as the default and regional laws added for mixed cohorts. Facilitators confirm the current status of each law before delivery, because amendments and court challenges are frequent.

Jurisdiction	Key laws	Regulator
Kenya	Constitution (Article 31); Data Protection Act, 2019 and 2021 Regulations; Computer Misuse and Cybercrimes Act, 2018 (amended October 2025, some provisions subject to court orders); Evidence Act (Cap. 80)	Office of the Data Protection Commissioner (ODPC); NC4
Rwanda	Law No. 058/2021 on the protection of personal data and privacy; cybercrime law	National Cyber Security Authority (NCSA)
Uganda	Data Protection and Privacy Act, 2019; Computer Misuse Act	Personal Data Protection Office (PDPO)
Tanzania	Personal Data Protection Act, 2022; Cybercrimes Act, 2015	Personal Data Protection Commission (PDPC)
Nigeria	Nigeria Data Protection Act, 2023	Nigeria Data Protection Commission (NDPC)
South Africa	Protection of Personal Information Act, 2013 (POPIA)	Information Regulator
Regional	AU Malabo Convention on Cyber Security and Personal Data Protection	African Union member states
International benchmarks	EU GDPR; Council of Europe Convention 108+; ISO/IEC 27001, 27701 and 42001; NIST CSF and NIST SP 800-61	—
Humanitarian	ICRC Handbook on Data Protection in Humanitarian Action; IASC Operational Guidance on Data Responsibility	—

Annex B: Laboratory Environment and Tools

Tools change often, so this is a starting map rather than a fixed list. All labs run in isolated virtual environments.

Area	Tools and platforms
Lab platform	VirtualBox / VMware, Ubuntu, Kali Linux, Trace Labs OSINT VM, cloud-hosted lab ranges

Area	Tools and platforms
Network and monitoring	Wireshark, Nmap, Wazuh, Splunk / ELK SIEM, Security Onion
Vulnerability and pentest	Nessus, OpenVAS, Metasploit, Burp Suite, OWASP ZAP, Nikto, DVWA, OWASP Juice Shop
Forensics	FTK Imager, Autopsy, Volatility, open-source mobile extraction tools, hashing utilities
OSINT	OSINT Framework, IntelTechniques, start.me pages, search operators, reverse image search, Sentinel Hub, NASA FIRMS, EXIF viewers, Maltego, Obsidian, web archiving tools
Data protection	DPIA and ROPA templates, gap assessment toolkit, breach notification templates, DLP console demo
Practice platforms	TryHackMe, Hack The Box, OverTheWire Bandit, Trace Labs Search Party CTF, Aware Online OSINT challenges

Annex C: Case Study Bank

Case	Domain	Teaches
SolarWinds supply chain attack	Cybersecurity	Supply chain risk; kill chain; detection gaps
Colonial Pipeline ransomware	Cybersecurity / IR	Ransomware response; business continuity; crisis leadership
Regulator enforcement decisions (e.g. ODPC determinations)	Data protection	Lawful basis, consent and fines in practice
Trace Labs missing persons CTFs	OSINT	Structured, lawful crowdsourced investigation
Bellingcat methods; Bellingcat and Daily Nation on ammunition crates near Khartoum (2024)	OSINT	Open-source verification to a publishable standard
BBC Africa Eye, “Blood Parliament” (June 2024)	OSINT	Video synchronisation, geolocation, responsible attribution
Boston Marathon crowdsourced misidentification (2013)	OSINT ethics	Harm from unverified naming
Albert Ojwang custody case (2025)	Forensics	Evidence integrity and early, independent preservation
Silk Road, AlphaBay and Empire takedowns	OSINT / cybercrime	Selector-to-identity pivoting; OPSEC failures

Case	Domain	Teaches
Anatomy of a Killing; Sudan, Mozambique and Kunbu-Kumfutu verification	OSINT	Geolocation and chronolocation in atrocity reporting
Humanitarian biometric data programmes	Data protection	DPIA, consent and data sharing in crisis settings

How to Book

Every course can run as an open course, in-house for your organisation, virtually or in a blended format. For in-house delivery we tailor case studies, examples and labs to your sector, systems and policies. To book a course, request a tailored proposal or ask about training levy reimbursement, contact us:

Company	**South-End Tech Limited**
Email	**info@southendtech.co.ke; ceo@southendtech.co.ke; cybersecurity@southendtech.co.ke**
Phone	**+254 717 335 467; +254 721 864 169**
Website	**southendtech.co.ke**

To build trust in data and cyberspace.