SecureZaidi
CYBERSECURITY & COMPLIANCE

COMPLIANCE GUIDE 03 / 04

Building a Security-First Culture: A 12-Month Programme Guide

How to design, deploy, and measure a security awareness programme that genuinely changes employee behaviour — built for African business environments.

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

Contents

1. Why Security Culture Matters

Technology alone cannot protect an organisation. The most sophisticated firewall, the most up-to-date endpoint protection, the most rigorously managed access controls — all can be bypassed by a single employee who clicks a phishing link, shares a password, or sends a sensitive document to the wrong recipient.

According to global breach data, more than 80% of confirmed data breaches involve a human element — phishing, use of stolen credentials, misdelivery, or social engineering. In East Africa, where mobile money fraud, Business Email Compromise, and SIM-swap attacks are prevalent, the human factor is even more pronounced.

A security awareness programme addresses this by changing the attitudes, knowledge, and behaviours of your workforce — making security a natural part of how people think and work, rather than an obstacle they try to navigate around.

The goal	A successful programme does not just tick a training box. It produces measurable, lasting changes in employee behaviour that meaningfully reduce the organisation's risk.

2. Programme Design Principles

Effective security awareness programmes are grounded in adult learning theory and behaviour science. Key principles:

- Relevance: training must connect to employees' actual roles and real threats they face — not generic, globally produced content that references organisations and scenarios alien to Kenyan employees.
- Repetition and reinforcement: behaviour change requires repeated exposure. A single annual training session is not sufficient. Plan monthly touchpoints across the year.
- Short and engaging: attention spans are short. Aim for 10–15 minute training modules, supplemented by short emails, posters, and awareness messages rather than hour-long sessions.
- Tone: avoid blame and shame. Create a psychologically safe environment where employees feel able to report mistakes and suspicious activity without fear of punishment.
- Leadership modelling: if the CEO is seen ignoring security policies, no training programme will overcome that signal. Secure visible commitment from senior leadership.
- Local context: use Kenya-specific examples — M-Pesa fraud, fake KRA letters, WhatsApp scams, SIM swaps — rather than international case studies that feel distant.
- Measurable outcomes: define what success looks like before you start. Reduced click rates on phishing simulations, increased incident reports, and improved quiz scores are measurable leading indicators.

3. Getting Stakeholder Buy-In

A 12-month programme requires time, budget, and management attention. Before you begin, secure genuine commitment from senior leadership. The business case should address:

- Cost of a breach: a single successful phishing attack can result in financial fraud, ransomware, regulatory fines, and reputational damage far exceeding the cost of awareness training.
- Regulatory requirement: Kenya DPA and ISO 27001 both require staff awareness training. This is not optional.
- Insurance implications: cyber insurers are increasingly requiring evidence of regular security training as a condition of coverage.
- Board accountability: under Kenya DPA, directors and senior officers can be held personally liable for organisational non-compliance.

Recommended executive briefing structure:

Lead with business risk in financial terms. Quantify the cost of a realistic breach scenario for your organisation. Then present the programme as a cost-effective risk mitigation investment — not an IT compliance exercise.

4. Months 1–2: Assessment and Foundation

Baseline assessment

Before training begins, establish a baseline. Send a security knowledge survey to all staff to assess current awareness levels. Topics to assess: phishing recognition, password practices, incident reporting, data handling, and device security. This gives you a starting point against which to measure progress.

Policy review

Review your current information security policies. Ensure they are up to date, accessible, and written in plain language that employees can actually understand and apply.

Programme communications

Launch the programme with a message from the CEO or MD explaining why security matters to the organisation and what employees can expect over the coming year. Name a point of contact for security questions. Set a positive, supportive tone from the start.

5. Months 3–4: Core Security Awareness Training

Deploy the core training modules to all staff. Each module should be no longer than 15 minutes and should include a short knowledge check at the end.

Module	Key topics covered
Phishing and Social Engineering	Email red flags, smishing, vishing, WhatsApp scams, M-Pesa fraud, how to report suspicious messages.
Password Security and MFA	Strong password creation, password manager usage, why MFA matters, setting up MFA on work accounts.
Data Handling and Classification	What is personal data, Kenya DPA obligations, data classification, secure sharing, cloud storage rules.
Device and Physical Security	Screen locking, clear desk, lost device procedure, public Wi-Fi risks, printer security.
Incident Reporting	What counts as an incident, how and where to report, why reporting quickly matters, no-blame culture.

6. Months 5–6: Phishing Simulation Campaigns

Phishing simulations are controlled tests that send fake phishing emails to your staff to measure how many click the link, submit credentials, or report the email. They are one of the most valuable tools in a security awareness programme.

Simulation methodology:

- Run at least two simulations per year. The first (Months 5–6) establishes a post-training baseline. The second (Months 9–10) measures improvement.
- Use Kenyan-context templates: fake KRA refund notifications, M-Pesa account alerts, Safaricom data bundle offers, and HR announcement emails are all highly effective simulations for East African workplaces.
- Start with medium-difficulty simulations. Extremely obvious or extremely sophisticated simulations are less useful for measuring and improving behaviour.
- Provide immediate teachable moments: when a staff member clicks, redirect them instantly to a short (3-minute) reminder page rather than simply logging the failure.

Expected benchmark results:

Industry benchmarks suggest organisations new to phishing simulation programmes should expect an initial click rate of 25–40%. A well-run programme should drive this below 10% within 12 months.

7. Months 7–8: Departmental Deep Dives

Different departments face different security risks. Months 7 and 8 are used for targeted, role-specific training sessions:

- Finance and Accounts: BEC fraud, payment verification procedures, wire transfer controls, supplier impersonation attacks.
- HR: handling personal data of staff, reference check fraud, social engineering targeting HR for employee data.
- IT and Systems Administrators: privileged access management, secure configuration, patch management, vendor access controls.
- Management and Senior Leadership: CEO fraud, targeted spear phishing, board-level security briefing and responsibilities under Kenya DPA.
- Customer-facing staff: handling customer personal data, KYC obligations, what to do if a customer reports fraud.

8. Months 9–10: Security Champions Programme

A Security Champions programme identifies and empowers enthusiastic individuals across the organisation to act as security advocates within their teams — extending the reach of your programme without requiring additional headcount in the security function.

Champion responsibilities:

- Be the first point of contact for security questions in their department.
- Share security tips and reminders with their team on a monthly basis.
- Report observed security weaknesses or policy violations to the IT/security team.
- Participate in quarterly champions briefings to stay current with emerging threats.

What champions need:

A small time commitment (2–3 hours/month), management support, a recognised role, access to up-to-date awareness materials, and — where budget allows — a small incentive or recognition for their contribution.

9. Months 11–12: Measurement, Reporting, and Year 2 Planning

The final two months focus on measuring the programme's impact, reporting results to leadership, and planning Year 2.

Measurement activities:

- Repeat the baseline knowledge survey from Month 1 and compare scores.
- Run the second phishing simulation and compare click rates to Month 5–6 results.
- Analyse incident reports: has the volume of reported suspicious emails increased? (This is a positive indicator — more reporting means higher awareness.)
- Review security incidents from the year: are there trends attributable to human behaviour?

Executive report:

Produce a concise (4–6 page) report for senior leadership covering: programme activities completed, before/after metrics, incidents attributable to human factors, programme ROI, and recommendations for Year 2. Attach this to the annual management review if you are pursuing ISO 27001.

10. Key Performance Indicators

KPI	Target (end of Year 1)
Training completion rate	≥ 95% of all staff complete all modules
Post-training quiz pass rate	≥ 85% average score across all modules
Phishing simulation click rate	< 10% (from an expected starting rate of 25–40%)
Phishing simulation report rate	≥ 30% of staff actively report simulation emails
Security incident reports (human)	Increase of ≥ 50% from Year 0 (more reporting = more awareness)
Policy acknowledgement	100% of staff have signed/acknowledged the information security policy

11. Communication Tips for East African Organisations

- Use WhatsApp for awareness nudges: most Kenyan staff are more likely to read a short WhatsApp message from a security awareness group than an email.
- Use real local examples: reference actual M-Pesa fraud cases, ODPC enforcement actions, and local cybercrime news stories to make threats feel real and relevant.
- Conduct sessions in Swahili where appropriate: for front-line and operational staff where English is not the primary working language, delivering sessions bilingually significantly improves comprehension and engagement.
- Use staff meeting integration: a 10-minute security update at the start of a regular all-hands or departmental meeting is often more effective than a standalone training event that staff treat as a box-ticking exercise.
- Recognise and reward good behaviour: celebrate staff who report phishing simulations or genuine threats. Public recognition (with permission) creates positive social norms around security behaviour.

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