



Advancing Regional Cybersecurity (ARC) KENYA

Recommendations for cybersecurity incident response in Kenya

4 May 2026

Authors: Elizabeth Eigner, Patricia Eke, Colonel (Dr) James Kimuyu, PhD, Markus Münzer

Contents

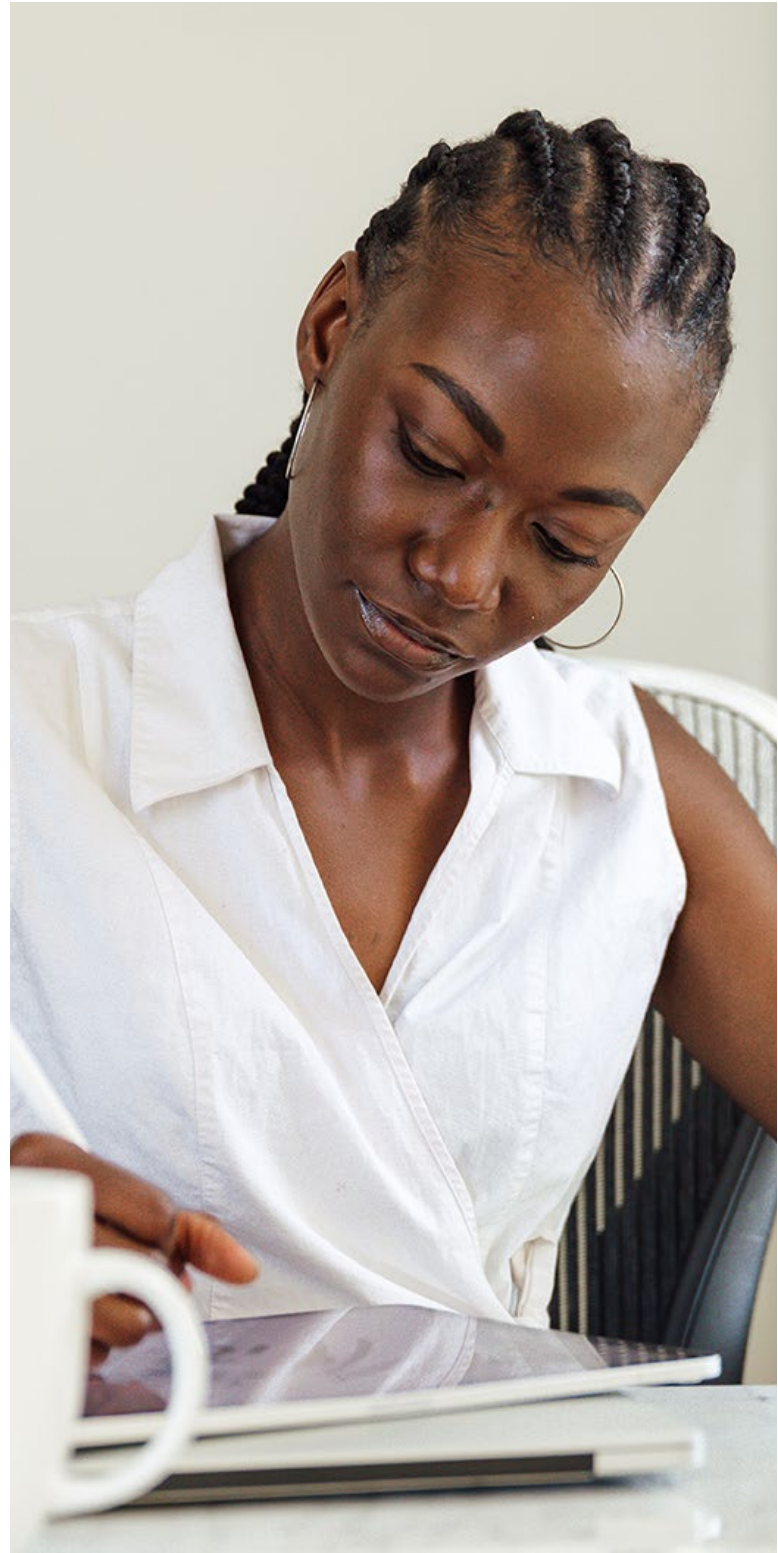
Acknowledgements	1
Introduction by Microsoft	2
Letter from NC4	3
Executive summary	4
Actionable recommendations	5
1. Governance & national coordination	5
2. Incident response framework & playbooks	8
3. Technical & operational coordination	10
4. Trust & information sharing	13
5. Bolster policies on ransomware	15
Conclusion	17

Acknowledgements

We extend our sincere appreciation to all participants whose dedication, expertise, and collaborative spirit were instrumental in the success of the ARC Kenya Roundtable and Tabletop Exercise. Your commitment to open dialogue, shared learning, and collective problem-solving has greatly contributed to advancing Kenya's national cyber resilience, and we thank you for your invaluable efforts in shaping a more secure and resilient digital future. With special thanks to our participants drawn for the Government of Kenya Ministries, Departments and Agencies, the Private sector and Industry; and academia.

Without you, this work would not be possible.

We would also like to extend our thanks to the organisers, including NC4 staff including David Kimemia, Microsoft colleagues Malcolm Kijirah and Akua Gyeke, and Markus Münzer of RiskSight, for their invaluable efforts and support throughout the exercise.



Introduction by Microsoft

Digital transformation is rapidly advancing across Africa. This progress makes robust cybersecurity essential to protect systems and data, and also to maintain public trust and support economic and national security. The Advancing Regional Cybersecurity (ARC): Kenya Roundtable and Tabletop Exercise reflect a shared recognition of this reality. Convened by Microsoft, in partnership with the [National Computer and Cybercrime Coordination Committee](#) (NC4) and [RiskSight](#), the exercise brought together government, regulators, the private sector, academia, and civil society to test decision-making, coordination, and preparedness in the face of complex, large-scale cyber incidents.

The ARC Initiative was announced during Geneva Cyber Week, as a reflection of the multistakeholder commitments of the [Accra Call](#), signed in Ghana at the inaugural GC3B in 2023. ARC was developed to fulfil those promises by providing model public-private partnership initiatives, ensuring that the commitments articulated in advancing cybersecurity in Africa. It is a public-private partnership model designed to strengthen countries' ability to address cybersecurity incidents through practical collaboration with government, critical infrastructure owners and operators, civil society and academia. Kenya's NC4 was a natural and compelling first partner for this initiative. Kenya has demonstrated a clear strategic vision for digital innovation and has positioned itself as a regional leader in technological investment and cyber governance. As a mobile-first country, it has established itself as a digital powerhouse with innovations like M-Pesa redefining how people interact with technology. From pioneering mobile money to digitising public services and building a vibrant tech ecosystem, Kenya has positioned itself as a regional leader and a global source of digital solutions. NC4 has protected Kenya's digital growth with efforts to build trust and resilience, launching national cyber initiatives and actively engaging in digital policy discussions at regional and global levels.

This ARC toolkit is intended to support that next phase of progress. It captures practical lessons from the exercise, identify priority actions for the coming months and years, and provides a structured reference for strengthening national cyber resilience.

Microsoft is grateful to NC4 for its leadership, to all participants for their candid engagement, and to our partners for their collaboration in delivering this initiative. We hope this toolkit serves as a practical resource for continued dialogue, planning, and action—supporting Kenya's vision of a secure, resilient, and inclusive digital future.

Amy Hogan-Burney
Corporate Vice President (CVP),
[Customer Security & Trust](#)
Microsoft

Letter from NC4

The National Computer and Cybercrimes Coordination Committee (NC4) is pleased to recommend the Advancing Regional Cybersecurity (ARC): Kenya Toolkit to all stakeholders engaged in strengthening Kenya's National cybersecurity posture.

NC4 is honoured to have served as the Government of Kenya's lead partner in the ARC Kenya Roundtable and Tabletop Exercise, convened in collaboration with Microsoft and RiskSight. The exercise brought together senior representatives from across Government Ministries, Departments and Agencies, the private sector, academia, and civil society — a testament to the cross-sector commitment that effective national cyber resilience demands. The quality of engagement from all participating institutions was commendable, and the candour with which participants examined Kenya's strengths and vulnerabilities made for a genuinely productive dialogue.

This Toolkit, comprising the Actionable Recommendations, the full Roundtable and Tabletop Exercise Report, and the accompanying Annex — represent a significant contribution to Kenya's cyber governance landscape. The recommendations are grounded in real operational discussions and reflection of the lived experiences of practitioners who bear daily responsibility for the nation's cyber security.

NC4 endorses the Toolkit's findings and commends its three central priorities: establishing a clearly defined national incident response framework; strengthening coordination across organisational, sectoral, and National Security Operations Centre tiers; and clarifying the reporting obligations and response responsibilities of both government and Critical Information Infrastructure operators.

Kenya has earned its standing as a regional digital leader. Sustaining that position requires that our governance frameworks keep pace with the sophistication of the threats we face. NC4 is

committed to working with all partners — public and private — to translate the recommendations in this Toolkit into concrete policy, institutional arrangements, and operational capability.

We welcome the initiative of Microsoft and RiskSight in developing the ARC model, and we look forward to continued collaboration as Kenya advances its national cyber resilience agenda.

We congratulate the organising team on completing this important body of work and commend this Toolkit to all who share our commitment to a secure, resilient, and inclusive digital future for Kenya and the broader region.

Yours sincerely,

Col (Dr) James J Kimuyu, PhD

Director
National Computer and
Cybercrimes Coordination
Committee (NC4)

Executive summary

The [ARC: Kenya \(ARC Kenya\) Roundtable and Tabletop Exercise](#) organised by NC4, Microsoft, and RiskSight, brought together key stakeholders from government, industry, academia, and civil society to discuss and test Kenya's national cyber preparedness through a realistic scenario-based exercise. This document—Recommendations for Cybersecurity Incident Response in Kenya, the Roundtable and Tabletop Exercise Report, and the accompanying [Annex](#) form the ARC Kenya Toolkit, providing a comprehensive and integrated set of policy, operational, and practical guidance. The roundtable provided a platform for participants to examine key challenges, share expertise, and identify practical actions for strengthening cyber resilience. Through structured discussions, the roundtable focused on improving incident response, fostering cross-sector coordination, and building a clear roadmap for cyber capacity building for the next 12 months.

At the same time, the tabletop exercise focused on strategic decision-making during complex cyber incidents, with participants working through 29 injects simulating large-scale attacks including distributed denial of Services (DDoS), ransomware, and AI-enabled threats. The discussions underscored the need for a clearly defined national operating model, strengthened Security Operations Centre (SOC) coordination across organisational, sectoral, and national levels, and clarified incident reporting obligations and government actions.

The central thesis of these findings is that Kenya, as a regional digital leader, is making significant progress in digital transformation but must prioritise strengthening its national cybersecurity posture to keep pace with evolving threats. The findings underscore that while Kenya demonstrates strong commitment, expertise, and leadership in cyber governance, effective national resilience depends on more clearly defined incident response frameworks, enhanced information sharing, and robust cross-sector coordination.

The Roundtable and Tabletop Exercise highlighted that the current approach to incident response remains government-led and fragmented, emphasising the need for an operational, international standard-aligned Incident Response Framework that defines clear roles, responsibilities, and minimum requirements for detection, reporting, coordination, and recovery. It reiterates the importance of a structured SOC coordination model spanning organisational, sectoral, and national levels, with improved communication channels and centralised reporting.

Overall, this document serves as one of three resources in a toolkit, aiming to guide Kenya and similar stakeholders in building a secure, resilient, and inclusive digital future through practical collaboration and continuous capacity building. Kenya's journey towards cyber resilience is marked by strong leadership, robust stakeholder engagement, and a clear vision for digital innovation. The ARC Kenya initiative has highlighted both achievements and areas for improvement, offering actionable recommendations to guide future progress. By embracing collaborative frameworks, prioritising operational readiness, and fostering continuous dialogue, Kenya is well positioned to strengthen its cybersecurity posture and safeguard its digital future.

Actionable recommendations

Based on the Roundtable and Tabletop Exercise, the following action plan is recommended to be applied to improve Cyber Incident Response in Kenya.

1. Governance & national coordination

Objective

Establish clear leadership, roles, and decision-making for cyber incidents.

Background

Kenya's cybersecurity landscape was acknowledged as fragmented in the roundtable and exercise, with entities having an overlapping role in cybersecurity.

An incident might see multiple parallel tracks (technical containment by the National SOC (NSOC), criminal investigation by DCI, etc.) that all need careful coordination by NC4 to avoid gaps or conflicts.

NC4's leadership role is largely one of orchestration, and without pre-defined emergency protocols, its effectiveness hinges on the voluntary cooperation of peer agencies. Exercise participants recognized a need to formalize who does what and when under NC4's leadership to enable more decisive action.

Key Activities

Assign a single national lead for cyber incident coordination

Policymakers could consider strengthening NC4's role as the national lead for cyber incident coordination. This would ensure clarity of mandate, streamline authority across agencies, and

provide a robust foundation for national incident management and escalation processes.

However, to enhance NC4 capability, the Kenyan government should consider transforming it into a more autonomous agency or authority dedicated to cybersecurity, similar to how other nations have dedicated cyber agencies. For instance, the U.S. elevated CISA into a standalone agency in 2018 to give it a clearer mission and direct funding, enabling it to hire specialized talent and deploy field teams. Singapore's Cybersecurity Agency (CSA) was set up as a dedicated body from the outset, signalling high-level commitment to cybersecurity.

Clarify mandates across government, regulators, law enforcement, defense, and critical infrastructure operators

Establishing NC4 as the lead and coordinator for national cyber incidents would go far in providing mandate clarity. Exercise participants agreed Kenya's path to improved cyber incident response lies in eliminating uncertainty in its multi-agency model. By enacting targeted legal reforms (like the 2024 CII Regulations), Kenya has begun to clarify "who is in charge" of what. The next steps involve detailed planning (incident response frameworks, MoUs, playbooks) and capacity-building to ensure each actor can fulfil its mandate.

This approach will help ensure that responsibilities are well delineated, reducing overlaps and confusion, and fostering more efficient collaboration between government, regulators, law enforcement, defence, and critical infrastructure operators. By establishing explicit roles and coordination mechanisms within the strategy, Kenya can build a more unified and effective national cyber defence posture. These roles can be defined as:

- **KE-CIRT:** As per the CMCA, 2018 (CII Regulations, 2024) the CIRT will continue to function as a Sector SOC responsible for the ICT

and Telecommunication sectors. Together with other sector SOCs, it shall provide input into the NSOC which will coordinate incident response at the national level.

- **Sector Regulators (Energy, Finance, ICT, Transport, Health):** Sector regulators play a pivotal role in Kenya's cyber incident response model by setting sector-specific cyber requirements, licensing and supervising operators, enforcing baseline controls through audits and reporting obligations, and maintaining sector Cyber Security Operations Centres (CSOCs). They ensure that operators are prepared to respond to incidents and, during major events, support NC4 by enforcing directives, mobilising sector operators, and clearing regulatory blockers such as authorising emergency changes. However, it should be clarified that sector regulators do not lead the national incident response effort or negotiate incident priorities. Their function is to act as force multipliers, providing operational support to NC4, rather than taking command of national coordination or decision-making during cyber incidents.
- **Law Enforcement:** Law enforcement agencies should work in parallel with other responders, rather than taking control during the immediate aftermath of cyber incidents. Kenya's new National Cyber Strategy should clarify that they are expected to follow NC4's guidance, particularly regarding the timing of seizures and ensuring that evidence collection does not hinder recovery operations.

The International Telecommunication Union (ITU). [Guide to Developing a National Cybersecurity Strategy](#) offers a well-established foundation for defining clear roles and responsibilities among agencies and stakeholders. By following these internationally recognised best practices, Kenya can ensure that its incident response framework is structured, comprehensive, and aligned with global standards, thereby reducing confusion and enhancing coordination during cyber incidents.

Define a national public-private operating model

Kenya's current public-private cybersecurity operating model is coordination-led rather than command-driven. NC4 provides cross government strategic coordination and escalation but does not exercise continuous operational control over private networks. Law enforcement and national security actors operate in parallel, preserving a civilian, trust-based reporting environment. The model emphasises shared responsibility, regulatory integration, and voluntary cooperation rather than centralised national cyber command.

While Kenya's coordination-led model fosters shared responsibility, exercise participants agreed that there is need for continuous public awareness and sensitisation to provide clarity on the escalation mechanism during high-impact scenarios. This highlights the need for clearer, streamlined coordination and escalation pathways during major incidents to ensure rapid, unified action and avoid gaps in the national response.

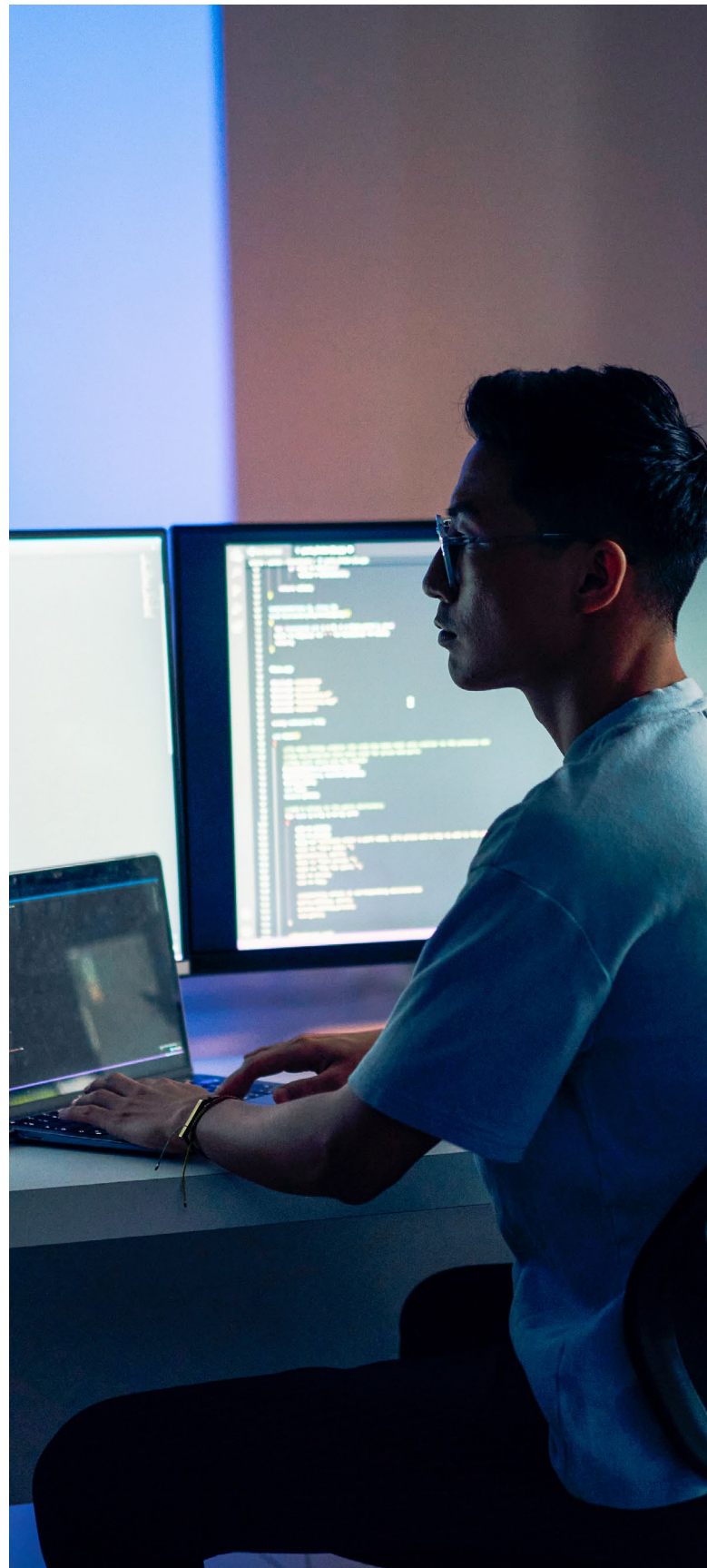
Kenya's draft National Cyber Strategy 2026 – 2031, currently in development, could be leveraged to clarify mandates and roles by explicitly defining responsibilities for each agency involved in incident response. The International Telecommunication Union (ITU), in its National Cybersecurity Strategy guidance, emphasizes that public-private partnerships (PPPs) are a critical component of effective cyber incident response within a nation's cybersecurity strategy. From these recommendations, Kenya could focus specifically on:

- **Formalizing Public-Private Partnerships (PPPs):** without formal frameworks, ad hoc PPP responses often lead to ambiguity regarding responsibilities, inconsistent communication, and delays in decision-making, as parties are uncertain about escalation routes and authority.
- **Embedding PPP frameworks in national cybersecurity strategies as a matter of policy:** could serve as coordinators and facilitators of incident response – providing overall leadership, legal support, resources, and threat intelligence – while the private sector

brings in technical expertise, operates critical infrastructure, and implements cybersecurity measures in practice. Clearly delineating public vs. private responsibilities ensures each party knows its role in the incident response process.

- **Building Trust in Information-sharing initiatives:** Successful PPP information sharing systems require a clear mutual value proposition and a foundation of trust. Both sectors must see concrete benefits: for example, industry gains timely aggregated threat intelligence and even government support for recovery during major incidents, while government gains access to industry's specialized incident response skills and on-the-ground technical know-how. To implement this, ITU's guidance stresses establishing trusted communication channels and legal frameworks that protect sensitive information shared by companies. Without trust and confidentiality measures, businesses may hesitate to share incident data, undermining the partnership's effectiveness.
(see Section 4 Below for more details)

Tabletop exercises and other public-private partnerships, such as ARC, also play a crucial role in clarifying pathways for collaboration between government and private sector operators. By simulating incident scenarios and fostering joint engagement, these mechanisms offer practical opportunities to identify points of contact, escalation routes, and decision-making roles with greater specificity—enabling both sides to test and refine coordination protocols, ensuring that responsibilities and communication channels are well understood ahead of real-world incidents.



2. Incident response framework & playbooks

Objective

Standardise how cyber incidents are managed across sectors

Background

Kenya's National Cybersecurity Strategy clearly covers detection and response, but the lifecycle is implicit, fragmented across agencies, and not codified as a single national model. Participants identified this as a hurdle in multiple incident-response scenarios in the exercise.

Key Activities

Adopt a national Incident Response Framework aligned with NIST CSF 2.0's Detect–Respond–Recover functions

Kenya could consider leveraging [NIST Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile \(NIST SP 800-61 Rev 3\)](#) to build its incident response model. NIST SP 800-61 Rev 3 outlines a standard, cyclical process comprising [Preparation, Detection & Analysis, Containment, Eradication & Recovery, and Post-Incident Activity](#) (Lessons Learned). Kenya can leverage the NIST incident response model both legally and tactically by enacting targeted regulations and policies that formally mandate its use across all relevant agencies and sectors. Legally, this involves updating national cybersecurity laws and sector-specific regulations to require adherence to the NIST lifecycle, ensuring that roles, reporting thresholds, and escalation pathways are clearly defined. Tactically, Kenya should translate these requirements into actionable frameworks and playbooks (see recommendations below), provide training for responders, and set up integrated coordination mechanisms—such as a single national incident reporting channel and

tiered SOC structure—to operationalise the model in practice. This dual approach would ensure both compliance and effective implementation, fostering a unified national response to cyber threats.

Develop national playbooks for priority incidents

A NIST CSF 2.0 -aligned framework would also place greater emphasis on preparation, which exercise participants noted remains one of the least developed elements in Kenya's current incident response posture. NIST's CSF 2.0 treats preparation—defined roles, tested playbooks, trained teams, and regular exercises—as the primary determinant of response effectiveness. Kenya could strengthen alignment by publishing a national cyber incident response playbook structured around NIST phases, establishing clear incident severity classifications and escalation triggers, and institutionalizing regular cross-sector tabletop exercises involving NC4, KE-CIRT, sector regulators, and critical infrastructure operators. These measures would operationalize the intent of the National Cybersecurity Strategy's call to streamline incident response and move coordination from ad hoc to rehearsed.

During discussions, the group identified certain playbooks as the highest priority for development. These were recognised as the most critical scenarios requiring immediate and coordinated national response, ensuring the incident response framework addresses the most pressing cyber threats facing Kenya. These included:

- DDoS
- Ransomware
- Phishing
- Data breaches including PII
- Cloud service incidents

To create these playbooks, Kenya could leverage [SANS playbooks and guidance](#) by using them as practical templates to guide incident response actions across sectors. These playbooks offer step-by-step procedures for handling specific types of cyber incidents, complementing the national

NIST-aligned framework by providing clear, actionable guidance for responders.

Equally important is embedding post-incident learning and continuous improvement into Kenya's framework. NIST 2.0 treats lessons learned and feedback loops as mandatory, not optional, ensuring that incidents drive improvements in controls, policies, and operational readiness. Kenya's current approach to post-incident review is inconsistent and rarely leveraged to produce systemic change. A NIST 2.0 -aligned model would require NC4-led after-action reviews for nationally significant incidents, with findings feeding into the NSOC advisories, sector regulator guidance, and future strategy updates, including the publication of sanitized lessons learned to build trust and shared awareness across the ecosystem.

Closer alignment with NIST 2.0 would support a shift in Kenya's incident response posture from a predominantly crime-centric model toward a resilience-first approach. NIST prioritises rapid containment, service restoration, and risk reduction, with criminal investigation proceeding in parallel but not at the expense of recovery. Kenya's framework has historically leaned toward criminalisation, which can deter early reporting by private operators. Explicitly separating technical incident reporting from criminal complaints, providing clarity and assurance around early disclosure, and reinforcing sector regulators as the first line of engagement would improve reporting, speed response, and strengthen national cyber resilience without weakening law enforcement outcomes.

Require incident response and business continuity plans from critical infrastructure operators

Roundtable discussions highlighted gaps in how critical infrastructure operators handle incident response. Participants argued that Kenya should require incident response (IR) and business continuity (BC) plans from Critical Information Infrastructure (CII) operators. This could be accomplished by using regulation and licensing conditions, rather than new institutions—specifically by amending or issuing guidance under the existing Computer Misuse and Cybercrimes 2024,

which already gives government authority to set cybersecurity obligations for designated CII, including audits, reporting, and risk management requirements. Regulators (ICT, finance, energy, transport, health) would be empowered to mandate that licensed CII operators maintain documented, tested IR and BC plans as a condition of operation, aligned to recognized standards e.g., [NIST SP 800-61](#) for incident response and [ISO 22301](#) for business continuity), without hard-coding the standards themselves into law.

In practice, if applied, CII operators would be required to (1) maintain a written incident response plan covering detection, escalation, containment, recovery, and coordination that is in line with the National Incident Response Plan; (2) maintain a business continuity and disaster recovery plan identifying critical services, recovery time objectives, and backup arrangements; (3) test both plans regularly through tabletop or simulation exercises; and (4) submit high-level attestations or summaries to their sector regulator, with full plans reviewed during audits rather than publicly disclosed. During incidents, operators would be required to activate their IR plans immediately and notify their sector regulator and the NSOC.

This approach builds on Kenya's existing regulatory model, strengthens preparedness without over-criminalisation, and mirrors international practice where governments require plans, testing, and assurance, while leaving operational ownership with infrastructure operators.



3. Technical & operational coordination

Objective

Enable early detection and coordinated operational response.

Background

Kenya's main national detection capability sits with the NSOC. The NSOC is the national focal point for monitoring, detecting, preventing, responding, investigating and attribution of cyber threats, computer and cybercrimes in Kenya.

Under the Computer Misuse and Cybercrimes Regulations (2024), Kenya has moved toward sector-based CSOCs. These CSOCs provide real-time event monitoring, log aggregation, alerting, and threat analysis within specific sectors.

Key Activities

Define national incident reporting thresholds and timelines

Kenya could define national cyber incident reporting thresholds using the impact-based approach articulated in both NIST SP 800-61 Rev. 3 and the EU's [Network and Information Security Directive 2](#) (NIS2), [Cyber Incident Reporting for Critical Infrastructure Act](#) (CIRCIA), rather than technical indicators alone. Under NIST SP 800-61, an incident becomes significant based on its functional impact (disruption of mission or services), informational impact (loss of confidentiality, integrity, or availability), and recoverability impact (time and effort required to restore operations), not on the specific malware or attack vector involved. Under the EU's NIS2 Directive, essential and important entities must report significant cyber incidents to the relevant national authority or CSIRT under a structured, time-bound process. This includes an early warning within 24 hours of becoming aware of an incident, a more detailed notification within 72

hours, and a final report within one month outlining impact, root cause, and mitigation measures.

Drawing on the analysis of this [report](#) from The Fletcher School of Law and Diplomacy on "[International Cybersecurity Regulatory Harmonization: Opportunities for Reciprocity & Mutual Recognition Among G7 and Quad Countries](#)", cyber incident reporting requirements should be triggered only by incidents that have caused, or present a credible risk of causing, material harm. Thresholds should be defined using objective, impact-based criteria— such as significant disruption to essential or critical services, substantial financial or operational impacts, large-scale compromise of sensitive data, or broader effects on other entities or the public— rather than the mere occurrence of technical security events.

Ensuring alignment of Kenya's incident reporting thresholds and timelines with NIST and the NIS2 Directive is crucial for achieving seamless interoperability, particularly when responding to cross-border cyber threats or collaborating with international partners. Alignment enables consistent communication, facilitates information sharing, and ensures that Kenyan organisations can participate effectively in global incident response efforts. Moreover, it supports best practice adoption and regulatory compliance, reducing fragmentation and strengthening overall cyber resilience.

Kenya already has several strong legal and policy levers it could leverage to implement national cyber-incident thresholds without new primary legislation. First, the CMCA gives NC4 an explicit mandate to coordinate national detection, response, and reporting of cyber incidents and to set cybersecurity codes of practice and standards for Critical Information Infrastructure (CII) owners, which provides a statutory basis for defining what constitutes a nationally reportable incident. Second, the Computer Misuse and Cybercrimes Regulations (2024) already empower NC4 and sector regulators to issue binding directives, require incident reporting, mandate Cybersecurity Operations Centres, and oversee compliance by CII operators.

Kenya could embed these thresholds in the National Cybersecurity Strategy implementation plans

and sector-specific regulatory instruments (e.g., banking, telecoms, energy), ensuring consistent application across sectors while preserving flexibility and avoiding over-criminalization of early technical reporting.

Establish a single national incident reporting channel

Kenya could establish a single national cyber incident reporting channel, leveraging early, impact-based notification and the CIRCIA “report once, share many” model, with NC4 responsible for escalation and national coordination and initial intake the NSOC. In the European Union, the “report once, share many” principle is similarly embedded in NIS2 and the [Cyber Resilience Act](#) (CRA). The Cyber Resilience Act establishes a Single Reporting Platform (SRP) as an EU level mechanism for reporting cybersecurity incidents affecting products with digital elements placed on the EU market.

The SRP is managed at EU level by ENISA and routes incident reports to the designated national CSIRTs responsible for follow up and response. NIS2 requires essential and important entities to notify significant incidents to their national CSIRT, which then distributes the information to other competent authorities.

Finally, under the [EU Digital Omnibus package](#), the European Commission has proposed a Single Entry Point (SEP) that would allow entities to submit a single cybersecurity incident notification to meet reporting obligations under multiple EU legal instruments, including NIS2, [General Data Protection Regulation](#) (GDPR), DORA, [Critical Entities Resilience Directive](#) (CER), and [electronic Identification, Authentication and trust Services Regulation](#) (eIDAS).

Implement a tiered SOC coordination model

Exercise participants strongly felt that a tiered SOC organisational model would improve Kenya’s incident response capabilities. Kenya already has a national technical SOC and coordination function, which operates 24/7, receives incident reports, issues alerts, and coordinates technical response nationally and internationally. This aligns with the “national fusion” layer in a tiered SOC model

and is explicitly mandated under the 2024 Critical Information Infrastructure Regulations.

However, Kenya does not yet operate a fully codified, impact-based tiered SOC escalation model across sectors. While NC4 has authority to coordinate nationally, escalation thresholds, standardized SOC minimum capabilities, and routine sector to national information flows are being streamlined across all sectors.

Strengthen sectoral SOC beyond telecoms and banking

Kenya already has a functioning sectoral SOC model in banking. The Central Bank of Kenya has established the Banking Sector Cybersecurity Operations Centre (BS-SOC), which receives reports from regulated financial institutions, conducts sector-wide monitoring, and coordinates incident response within the banking and payments ecosystem. This is a textbook example of a Tier-2 sector SOC operating between individual institutions and the national level. Kenya also has partial sectoral SOC capability in telecoms, led by the Communications Authority through KE-CIRT and its telecom-focused Cyber Security Operations Centre functions. This gives the communications sector stronger detection and coordination than most other sectors, but it is not yet mirrored consistently elsewhere.

However, most other critical sectors in Kenya do not yet have mature sector SOC. Energy, transport, health, water, and government digital services are designated as Critical Information Infrastructure under the 2024 Regulations, but there has been uneven SOC maturity, often limited to organization-level monitoring without a sector-wide aggregation and coordination layer. The regulations allow for sector SOC, but they do not automatically create them.

Kenya could strengthen sectoral SOC by formalizing sector SOC requirements beyond telecoms and banking, using the existing Critical Information Infrastructure (CII) framework. Kenya’s 2024 CII Regulations already allow NC4 and sector regulators to require monitoring and incident response capabilities; the first step is issuing sector-specific guidance that clearly states which

sectors must have a sector-level SOC function, even if delivered through shared or managed models.

The next step is to select two or three major high-impact sectors that already have established operators and regulators, making them ideal pilots for sector SOC coordination with minimal groundwork.

Rather than mandating full, bespoke SOC, Kenya should consider defining minimum sector SOC functions, not infrastructure. This includes aggregating incident reports from operators, correlating events across the sector, issuing technical advisories, and escalating to THE NSOC when patterns suggest broader risk. This lowers cost and avoids unrealistic compliance burdens, especially for smaller operators. Kenya can then leverage shared or managed SOC models for sectors with limited capacity, such as health or water. Regulators can approve trusted SOC service providers that serve multiple operators, ensuring consistent visibility while avoiding fragmentation. This approach is consistent with international practice and fits Kenya's mixed public-private infrastructure system.

Finally, Kenya could test-drive the model through cross-sector tabletop exercises, starting with one new sector at a time. These exercises should test reporting flows, SOC-to-SOC coordination, and NC4 escalation decisions, turning policy into operational capacity before expanding nationwide.



4. Trust & information sharing

Objective

Improve trust, intelligence and information sharing and collective security.

Background

Kenya does not currently have a single, nationally mandated information-sharing and classification framework for cyber incidents equivalent to the [Traffic Light Protocol \(TLP\)](#) or another standardized scheme. There is no binding policy instrument that requires all government bodies, sector regulators, SOCs, or operators to use a common marking system to indicate how cyber incident information may be shared or restricted. Instead, information sharing is handled through institution-specific practices, bilateral arrangements, and informal norms, which vary by sector and by institution. Exercise participants identified this as a serious sticking point in information-sharing during incidents.

NC4 handles cyber information primarily through a national security, law-enforcement, and inter-agency coordination lens, as defined under the CMCA. When cyber incidents reach NC4, information handling tends to default to government security sensitivity, criminal investigation considerations, or intelligence handling norms. These are not designed for rapid operational cyber information sharing, and they do not distinguish cleanly between technical indicators that should be widely shared, and sensitive attribution or investigative material that should not. As a result, escalation to NC4 often narrows information flow rather than enabling broader defensive sharing.

Some sectors have stronger internal sharing practices, but they are not harmonised nationally. There is no common language across sectors to

indicate “this can be shared with peers,” “this stays within government,” or “this is public-facing.”

Key Activities

Introduce a national information sharing framework

Kenya could introduce a national cyber information-sharing and classification framework by adopting a lightweight, internationally recognised marking system. The most widely used model is the [Traffic Light Protocol \(TLP\) v2.0](#), maintained by FIRST. TLP provides four simple labels—TLP:RED, AMBER, GREEN, CLEAR—that define how widely cyber information may be shared, without turning it into classified or law-enforcement material.

To ensure consistency, Kenya could pair TLP markings with standardised incident information categories such as service disruption, loss of confidentiality, impact on critical services, and public safety relevance. This would ensure that information shared across sectors is both properly handled and immediately actionable, even when technical details are limited.

Kenya could adopt frameworks such as TLP as the default marking for all cyber incident information, threat intelligence, advisories, and coordination messages shared between the NSOC, sector SOCs, Organisational SOCs and NC4 coordination channels. This could be done through an NC4 policy directive and sector-regulator guidance, rather than legislation, making TLP mandatory for incident reports, alerts, and cross-sector coordination during cyber events.

Provide confidentiality and legal protections for “good faith” reporting

Kenya requires cyber incident reporting and generally treats reported information as confidential through government handling norms under the CMCA and the 2024 Critical Information Infrastructure Regulations, but it lacks clear, explicit legal protections for “good-faith” reporting: there is no statutory safe harbour that prevents incident reports from being reused for regulatory penalties, civil liability, or enforcement actions, and no clear limits on secondary use of shared technical

information once incidents escalate beyond technical coordination. As a result, confidentiality is largely implicit and practice-based rather than rule-based, creating uncertainty that can discourage early, technical disclosure.

Roundtable participants concluded that Kenya should adopt a safe-harbour model where organisations that report cyber incidents in good faith are protected from that report being treated as an admission of fault or automatically triggering penalties. The protection is limited to the act of reporting and the information shared for cybersecurity risk management.

To implement this, NC4 to provide a platform for anonymous reporting to allow any person/organisation to disclose useful information relating to cyber incidents or crimes anonymously for response and coordination purposes.

Promote cross-sector SOC cooperation and joint training

Kenya could consider institutionalising regular cross-sector cyber exercises that test SOC-to-SOC coordination, not just individual sector readiness. This aligns with CISA Cybersecurity Incident Response and Vulnerability Response Playbooks, which emphasise coordinated response and shared situational awareness across entities, and with NIST SP 800-61 Rev. 3, which treats incident response as a multi-stakeholder risk-management function rather than a siloed technical task.

NC4 could operationalise this through joint SOC training programmes delivered across sectors using a common curriculum, applying a similar approach to CISA's Incident Response Training and Cyber Range exercises, which focus on shared detection, triage, and coordination skills rather than sector-specific tooling, ensuring SOC analysts across energy, health, transport, and government speak the same operational language.

Kenya may consider institutionalising national joint cyber tabletop exercises (TTXs) as the primary mechanism for testing cross-sector SOC coordination. Internationally, national cyber authorities use discussion-based TTXs to pressure-test decision-making, information sharing,

escalation, and coordination without touching live systems. CISA's Tabletop Exercise Packages provide a proven, customisable model covering ransomware and cross-sector disruption, explicitly designed to test information sharing, response, and recovery across multiple stakeholders. Exercises would ideally bring together the NSOC, sector SOC (banking, telecoms, energy, transport, health), regulators, and NC4 to rehearse how incidents move from operator SOC to sector coordination, national technical fusion, and national decision-making.

NC4 could also introduce short-term SOC staff exchanges and secondments between mature SOC (banking, telecoms) and emerging sector SOC.

Finally, NC4 should require structured post-incident and post-exercise reviews involving all affected SOC, coordinated by NC4, with lessons shared nationally—implementing the "Improve" function in NIST CSF 2.0 and ensuring cooperation continuously strengthens rather than resetting after each incident.



5. Bolster policies on ransomware

Objective

Bolster Kenya's readiness and responses to combat the growing ransomware threat.

Background

As a rapidly advancing digital economy, Kenya faces heightened risk from ransomware attacks. The swift expansion of digital services—across government, fintech, and telecommunications—has created a broad attack surface, while institutional capacity and specialist cybersecurity expertise have struggled to keep pace. This combination of accelerated digital adoption and skills shortages makes it more likely that attackers will target Kenya, viewing its growing digital infrastructure as both valuable and potentially vulnerable to disruption and extortion.

Kenya's response to ransomware is anchored in general cybercrime and incident-response structures, rather than a ransomware-specific strategy. Public reporting and advisories focus heavily on technical mitigations and awareness, rather than coordinated national response or victim-support models. Kenya does not have a ransomware playbook (see Playbooks section above), a policy on ransom payments, or a dedicated victim support or coordination mechanism. Ransomware is subsumed under cybercrime generally, which contrasts with international best practice.

Key Activities

Apply the Ransomware Task Force (RTF) Strategic Framework in Kenya

The [Ransomware Task Force](#) (RTF) is a multistakeholder initiative that brings together governments, civil society, and industry—including Microsoft—to address ransomware as a systemic national security and economic threat,

rather than a purely technical or criminal issue. Its 2021 report, [Combating Ransomware: A Comprehensive Framework for Action](#), sets out a strategic framework focused on four mutually reinforcing objectives: deterrence, disruption of the ransomware ecosystem, preparedness and resilience, and effective response and recovery. The framework is used internationally, including by participants in the International [Counter Ransomware Initiative](#) (CRI), of which Kenya is already a member. Applying this framework could allow Kenya to build on its existing institutions while addressing current gaps in its ransomware posture. Within this framework, Kenya could consider prioritising:

- Elevating ransomware within national cyber strategy and coordination structures, consistent with the RTF's deterrence pillar: While Kenya's legal and policy frameworks clearly recognize cybercrime risks, ransomware is currently treated as one threat among many, rather than as a distinct national security and economic risk. The RTF framework emphasizes the importance of clear national signalling that ransomware is a strategic threat requiring sustained, high-level attention. Kenya could address this by explicitly identifying ransomware as a priority threat in national cybersecurity strategy updates and by clarifying national leadership for counter-ransomware coordination. Assigning NC4 a clearly articulated role as the national strategic coordinator for ransomware—working alongside Sector SOCs technical response function—could strengthen coherence and accountability without creating new institutions.
- Moving beyond incident handling toward active disruption of the ransomware ecosystem in line with the RTF's disruption objective: The RTF framework stresses that ransomware cannot be managed through response alone; it requires coordinated efforts to disrupt criminal infrastructure, financial flows, and enabling services. Kenya could advance this by more systematically integrating law enforcement, financial regulators, and international partners into ransomware-specific operations, including cooperation on cryptocurrency-enabled extortion and participation in international

disruption efforts through CRI and related mechanisms. This would shift the national posture from managing harm to actively reducing the profitability and feasibility of ransomware attacks.

- Improving the effectiveness and clarity of response model by adopting a more victim-centric approach, consistent with the RTF's response and recovery pillar: The RTF framework stresses that victims need clear pathways for reporting, technical assistance, law-enforcement engagement, and recovery support during ransomware incidents. In Kenya, responsibilities are currently spread across multiple institutions, which can create confusion during high-impact incidents. Kenya could consider establishing a clearly defined ransomware incident coordination pathway—where NC4 provides strategic coordination leads technical response. This could improve speed, trust, and outcomes. Equally important is ensuring that reporting frameworks encourage early disclosure by providing appropriate confidentiality and good-faith protections, which the RTF identifies as critical to effective national response (see Provide confidentiality and legal protections for “good faith” reporting in 5.4 Trust & Information Sharing above).
- Deepening structured public-private collaboration as a core element of Kenya's counter-ransomware strategy: Kenya already engages the private sector through advisories and information sharing, but this could be strengthened by more operational collaboration, such as trusted threat-intelligence exchanges, joint exercises, and coordinated response planning for ransomware scenarios. Embedding these practices within existing national structures would improve collective resilience while reinforcing Kenya's role as a regional leader in cybersecurity cooperation.

Treat national backup and recovery infrastructure as a strategic resilience investment

Kenya could elevate backup and recovery infrastructure—especially for core public systems—from an IT issue to a national resilience asset. Recent investments such as government data recovery centres reflect recognition of this need, but these efforts remain fragmented and agency-specific rather than part of a coordinated ransomware resilience strategy. A national policy could set baseline expectations for immutable backups, geographic redundancy, and recovery testing for critical public platforms, while encouraging shared services or reference architectures for counties and smaller agencies. This would reduce ransomware leverage by ensuring the state can restore services without paying or negotiating. Framing backup infrastructure as part of Kenya's broader cyber resilience and economic stability agenda—rather than merely technical compliance—would materially reduce the impact of future ransomware incidents.



Conclusion

In closing, we wish to express our sincere gratitude to NC4, the broader Kenyan government, and all the participants whose expertise, commitment, and collaborative spirit have been instrumental in the development of this toolkit. Their collective efforts and engagement have not only shaped its content and direction but also exemplified the dedication required to strengthen Kenya's cyber resilience for the future.

We hope this report will serve as a practical blueprint to support Kenya as it builds on its ongoing efforts to enhance cybersecurity capacity

and resilience, particularly at the policy level. By capturing lessons learned and best practices, it is intended to guide the continued development of robust national frameworks and strategic initiatives.

It is our aspiration that this report will not only serve Kenya but will also provide practical guidance to other countries with similar capacities and challenges. By sharing lessons learned, best practices, and strategic frameworks, we hope to contribute to a wider regional and international effort in strengthening cyber resilience and preparedness against evolving threats.



