

INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA

STAKEHOLDER ENGAGEMENT

NETWORK RELIABILITY AND INFORMATION SECURITY

CONTENT

- BACKGROUND
- LEGISLATIVE AND POLICY FRAMEWORK
- RESEARCH RESULTS
- BROADCASTING DIGITAL PIRACY
- CONCLUSION

BACKGROUND

In 2018, the Authority initiated an inquiry into the Authority's role and responsibilities in Cybersecurity, which resulted in a Findings Document

The findings acknowledged the importance of cybersecurity;

However, stakeholders were of the view that ICASA does not have a role to play at that stage, and that its mandate did not clearly extend to comprehensively regulating cybersecurity.

The Authority resolved not to introduce regulations at that time instead encourage the adoption of recognised technical standards in collaboration with relevant institutions.

The focus for the Authority was placed on consumer education and awareness, research and development, and building partnerships with cybersecurity entities and other regulatory bodies.

LEGISLATIVE AND POLICY FRAMEWORK

- The Constitution of the Republic of South Africa;
- The Cybercrime Act;
- The Electronic Communications and Transactions Act 25 of 2002;
- The Protection of Personal Information Act 4 of 2013;
- The National Cybersecurity Policy Framework (2015);
- The Independent Communications Authority of South Africa Act; and
- The ECA

EMPOWERING LEGISLATION

Section 4(3) of the Electronic Communications Act, 2005 (ECA), which empowers the authority to conduct research into matters relating to electronic communications, broadcasting and postal services and to make findings and recommendations that support effective regulation.

Guided also by ECA s 2(n), s 2(q), s 36(1)–(2) the authority is conducting further research to develop an understanding of emerging risks affecting network reliability and information security across the sectors regulated by the authority.

THE PURPOSE OF THE STUDY

- The study sought to develop a comprehensive and evidence-based understanding of cybersecurity readiness among I-ECNS and ECS licensees to inform effective regulatory oversight by the Authority.
    - The study examined the extent to which licensees can detect, mitigate and recover from cyber threats.
    - It also explored whether licensees have end-to-end protection
    - The study considered the extent to which licensees have adopted relevant international cybersecurity standards and frameworks

SCOPE AND APPROACH OF THE STUDY

Research Approach

The Authority adopted a mixed research method to conduct this study

Qualitative Desktop Research	reviewing of a range of materials, including academic, policy, regulatory sources & international frameworks
Online Survey	structured questionnaire designed to collect data from Individual-ECNS and ECS licensees in South Africa
International Study Visits	to gain direct knowledge into successful regulatory and industry-led approaches.

SCOPE AND APPROACH OF THE STUDY

- The target was all 430 Individual-ECNS and ECS licensees in ICASA's database.
- The questionnaire was tested among the research team as a pilot to ensure usability and question clarity testing.
- The responses were de-identified before analyses.

STUDY LIMITATIONS

- Limited access to documents for desktop research;
- Limited responses due to outdated email addresses;
- Low survey response rate due to fear of exposure of cybersecurity vulnerabilities;
- The international benchmark exercise was only possible in three out of the six countries that were identified (Brazil, Kenya, and UK).

LITERATURE REVIEW

- The Authority engaged publicly available documents and the following key global frameworks that offers tools for identifying cyber risks, implementing security controls and assessing the maturity of cybersecurity capabilities:
  - ITU Security Manual
  - NIST cybersecurity framework (CSF)
  - ISO/IEC 27001
  - ENISA – national capabilities assessment framework
  - ACS Essential Eight maturity model
  - DOE C2M2 maturity model
- These frameworks were used to guide the questionnaire to collect data that will enable the Authority to understand how telecommunications operators perceive, organise and manage cybersecurity risks.
- The purpose of the study was not to measure compliance with the frameworks.

DESKTOP RESEARCH

USA

- Federal Communications Commission (FCC)-Cybersecurity and Communications Reliability Division is the Regulatory Authority
- Monitors network outages and vulnerabilities; Coordinate responses during disasters and emergencies
- Combine voluntary and mandatory requirements
- NIST driven approach with strong emphasis on resilience, co ordination and public private collaboration.

Estonia

- The Consumer Protection & Technical Regulatory Authority (CPTRA) is the certification authority and regulator.
- Information System Authority (RIA) leads incident response and operations
- Standards aligned with ISO/IEC 27001 through the development of E-ITS (Estonian Information Security Standard).
- Cybersecurity compliance for connected devices
- Compliance with EU directives and adopts a multi-agency coordination

Ghana

- National Communications Authority (NCA) as the regulatory Authority oversees cybersecurity in telecoms sector.
- The law requires operators to implement technical and organisational security measures in line with international best practice.
- Sector specific CERT under NCA to monitor and analyse incidents
- Combines proactive engagement and reactive incident handling

DESKTOP RESEARCH

Kenya

- Communications Authority (CA) regulatory Authority with KE-CIRT set within the Authority for sector incidence monitoring and response.
- Mandatory incident reporting within 24 hours and cybersecurity audits for critical infrastructure
- The computer misuse and cybercrimes Act criminalise unlawful cyber activities and provides for the enforcement and investigative mechanisms cyber offenses.
- Evolving framework with ongoing legal reforms and takes multi agency coordination
- ITU and ISO aligned

UK

- Ofcom oversees telecom security compliance and enforcement
- NCSC – National technical authority for cybersecurity
- Based on a Tier system(operator size and risk exposure)
- Mandatory incident reporting to Ofcom
- NIST and ISO aligned.

Brazil

- Anatel is the main regulator
- Transitioning from voluntary guidelines to mandatory cybersecurity requirements
- Requirement for certification of Customer Premises Equipment (CPE) devices; security by design principle and mandatory vulnerability management and updates
- Testing and certification via labs, non-compliant products can be recalled or withdrawn from the market.
- Alignment with ITU framework and ISO standard.

KEY FINDINGS FROM DESKTOP RESEARCH

Increased importance of cybersecurity governance.	as digital networks evolve into critical infrastructure they increasingly underpin economic activity, public services and national security.
structured approach is favourable	managing cyber risks, recognising that the resilience of telecommunications networks is fundamental to maintaining trust in digital ecosystems.
Adoption of globally recognized Frameworks	frameworks include: ITU, the NIST, and the European Union Agency for Cybersecurity offer valuable tools for identifying cyber risks, implementing security controls and assessing the maturity of cybersecurity capabilities.
The importance of shared understanding	This can be achieved through instruments such as regional policies such as SADC Model Law on Computer Crime and Cybercrime. The law provides a harmonised legal foundation for cybercrime legislation across the region and informs South Africa's domestic cybersecurity framework.

INTERNATIONAL BENCHMARK: LEGISLATIVE FRAMEWORK

Framework	United Kingdom	Brazil	Kenya
Primary Legislation basis	Telecommunications (Security) Act, 2021 (TSA)	Resolution 767/2024 (R-Ciber amendment); Act 2,436/2024 (CPE); Act 16,417/2024 (Supplier Audits)	Computer Misuse and Cybercrimes Act 2018 (CMCA); Kenya Information and Communications Act 1998 (KICA)
Secondary/ Regulatory Instruments	Electronic Communications (Security Measures) Regulations 2022; Telecoms Security Code of Practice	Cybersecurity Regulation Telecommunications Sector (R-Ciber Resolution 740/2020)	Critical Information Infrastructure & Cybercrime Management Regulations 2024; Communications Subscriber Registration Regulations, 2025.
Pending Legislation	N/A (framework considered mature)	Ongoing expansion of R-Ciber scope	KICA Bill 2024; CMC Amendment Act 2025; Cybersecurity Bill 2026 (draft);

INTERNATIONAL BENCHMARK : INSTITUTIONAL COORDINATION

Aspect	United Kingdom	Brazil	Kenya
CIRT Structure	NCSC as national technical authority; Ofcom for sector regulation.	CTIR Gov as national CSIRT; GT-Ciber for telecoms sector technical oversight.	KE-CIRT (hosted by CA) as sector SOC; NC4 as the government strategic national committee.
Public-Private Collaboration	Structured via Code of Practice obligations; industry compliance-led	CNCiber includes government, academia, civil society, private sector.	Strong CA–Tespok relationship; private sector excluded from NC4
Industry Role	Regulated compliance; independent audits mandated.	Industry audits required; suppliers must hold compliance certificates.	Industry-led cyber efforts through early warning systems for detection, prevention and resolution.
Funding Model	Well-resourced national institutions.	Established national budget; separate regulatory funding.	Limited budget through national treasury approval, NC4 has no dedicated budget; National Cybersecurity Agency proposed.

LESSONS FROM INTERNATIONAL BENCHMARK

All three jurisdictions (Brazil; UK and Kenya)--Persistent challenges around governance clarity, private sector inclusion, and sustainable funding.

Cyber hygiene and user behaviour are cited as the most significant barriers to effective cybersecurity across all three countries. Key strength lies in the early adoption of collaborative mechanisms.

Public-private collaboration is essential in all jurisdictions, though the model and maturity differ significantly. Effective cybersecurity is as much about relationships, and shared ownership as it is about laws and institutions

Financing cybersecurity is a universal challenge — even mature frameworks require sustained investment in people, tools, and processes. Invest in skills and capability

The tension between regulation and innovation is a recurring theme (e.g.drone regulation). SIM registration and subscriber identity management are active regulatory concerns in Kenya and offer lessons for other developing economies.

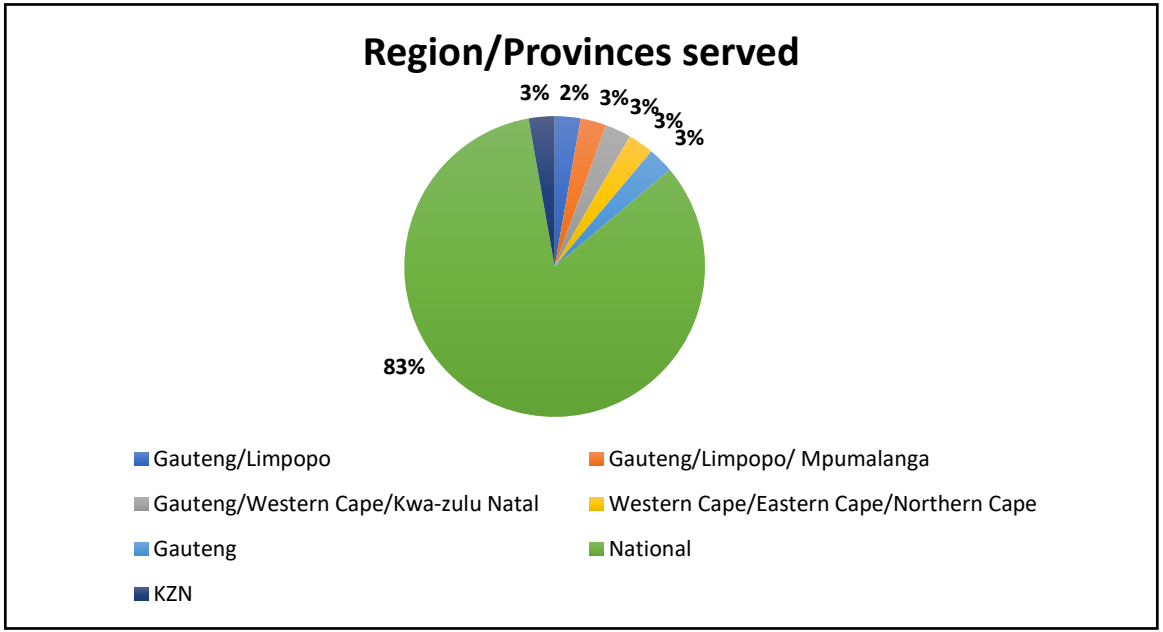
Trust-building, phased consultation, and clear role definition approach is critical than building formal structures alone.

SURVEY OVERVIEW

- The questionnaire was sent to over 430 ECS and ECNS licensees
- 37 licensees responded, Majority operate nationally (83%) - represents significant market coverage
- **Key focus areas:**
    - Organisational Overview
    - Governance (Cybersecurity Standards/Frameworks; Strategy; Board oversight)
    - Prevention & detection(Network security controls)
    - Incident response & Recovery (Incident management)
    - Capacity & preparedness (Organisational capacity & information sharing)
    - Consumer protection & SIM security(data protection & privacy compliance)

ORGANISATIONAL OVERVIEW

- The survey results show that a large proportion of the respondents (83%) offer services nationally.



CYBERSECURITY GOVERNANCE & STRATEGY

- 62% have Formal strategy adoption aligned to ISO/IEC 27001 and NIST CSF;
- 86% have Strong risk management integration; and
- 76% have Continuous cybersecurity strategies maintenance.
- However, only 6 organizations have dedicated CISO with board access.
- While cybersecurity strategy is updated/reviewed, it is predominantly done annually, which may be insufficient for rapidly evolving threats.
- Best practice suggests that organisations that combine internal continuous monitoring with external annual assessments achieve optimal assurance.
- It also suggests that dedicated CISO roles with direct board reporting enhance cybersecurity governance.

PREVENTATIVE MEASURES AND DETECTION MONITORING

- 76% apply broad range of security safeguards (perimeter protection etc)
- 80% resolve high-priority weaknesses within 24–48 hrs, 7% indicate in 7 days, 3% in 14 days, 7% quarterly, and 3% monthly
- 41% perform Independent Security Assessments annually, 33% occasionally, 16% quarterly, and only 5% reported bi-annually
- 68% of the respondents use third-party vendors. Of those (68%) who use third-party reviewers, majority (76%) of them conduct these assessments annually.
- Annual Security Assessments culture exists; however, it may not be sufficient given the evolving threat landscape.
- Preventative assurance mechanisms are not consistently embedded as continuous processes. This limits early detection of systemic vulnerabilities.
- There is a need to cultivate a culture of continuous and frequent security assessments.

INCIDENT RESPONSE AND RECOVERY

- 84% have formal incident response plan
- 84% no significant cyber incident reported in the last 24 months
- 24-48 hours turn around time to respond to incident
- 84% have procedures to notify affected parties
- The findings suggest that although the sector may have a reasonable level of baseline awareness and adoption of cybersecurity measures, this does not yet amount to uniform or sufficiently mature cybersecurity readiness across all operators.
- There is a differentiation of periodic and applications of monitoring and testing across the operators. There is a need to cultivate a culture of continuous and frequent security assessments.

ORGANISATIONAL CAPACITY & FUTURE PREPAREDNESS

- 58% does not participate in national or international information sharing platform
- 42% participate (e.g InfraGard, Information Security Forum, COMRiC, OWASP, ITWeb Security Summit)
- 68% have cybersecurity teams, 32% don't. Without a dedicated team, responsibility for cybersecurity may be dispersed across general IT which can weaken accountability
- 81% provide cybersecurity awareness training, of that 81% only 77% conduct training regularly

ORGANISATIONAL CAPACITY & FUTURE PREPAREDNESS

- It is essential to have a coordinated national/international information sharing platform schedule that every operator will be aware of to ensure consistent participation and information sharing.
- Legal instruments should also clarify the process and requirements such as thresholds of incidents to be reported that operators must be aware of.
- Clarification may also include a centralized incident reporting portal with guidance on how to report and should have feedback loops that are timeous to the operator.
- Periodic (Quarterly) sector briefings should also be encouraged; these will enhance knowledge and capacity for operators on types of incidents and how to handle them whilst also building trusting relationship with the Authority.

CONSUMER PROTECTIONS & SIM REGISTRATION SECURITY

- All the respondents indicated that they do comply with POPIA
- 81% restrict network access to approved users
- 51% apply a layered verification SIM registration process
- 70% of respondents fully protect & de-identify consumer data
- Responses indicated there are different data security measures in place but not uniform they vary from one organisation to the next.
- ICASA should consider introducing baseline technical security standards for licensees handling SIM registration and consumer data.
- Harmonised standards would strengthen consumer data protection and reduce systemic vulnerabilities.

CONCLUSION

- The findings show that, although South Africa's telecommunications sector has taken important steps to improve cybersecurity, the level of maturity across the sector is not uniform.
- The study also identified gaps in implementation, preparedness, internal capability, coordination and information-sharing, which suggest that the sector cannot yet be regarded as uniformly resilient.
- The study points to a need for timely and proportionate intervention by the Authority.
- To improve consistency across licensees and strengthen resilience in the telecommunications environment, Cybersecurity need to be approached carefully and in a manner that is responsive to the realities of the sector.



INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA

BROADCASTING DIGITAL PIRACY NETWORK RELIABILITY AND INFORMATION SECURITY.

BACKGOUND

- Rapid expansion of digital platforms have transformed content distribution and audience engagement.
- While these platforms have created new opportunities for South Africa to reach international markets, they have amplified the challenge of broadcasting content piracy.
- This unauthorised use and digital duplication in turn undermines the financial viability, sustainability, inhibit innovation and negatively affects employment opportunities.
- Illegal distribution is most commonly over the internet, and the pirated content is almost always hosted on servers outside South Africa.

BROADCASTING SECTOR ENGAGEMENT

- The Authority has been engaging with the broadcasting sector on matters relating to broadcasting piracy including its potential impact on network reliability, consumer cybersecurity, fraud and information security.
- To date the Authority has engaged the following stakeholders:
  - Multichoice and Iderto;
  - SABC;
  - eTV;
  - Faith Terrestrial;
  - National Association of Broadcasters;
  - Motion Pictures;
  - National Gambling Board;

CONCERNS ON BROADCASTING DIGITAL PIRACY

- There is currently no statutory legal mechanism under South African law under which a broadcaster (or any other person) can ask for unlawful content (such as content that breaches copyright) that is hosted in South Africa and abroad to be taken down or blocked by the South African ISPs that transmit the pirate platforms' websites in South Africa.
- A South African ISP that is a member of the Internet Service Providers' Association ("ISPA")under the requirements of Electronic Communications and Transactions Act 72 of 2002 ("ECTA") cannot be held liable for transmitting unlawful content.
- Therefore, broadcasters cannot claim damages from South African ISPs that distribute the pirate platforms to South African viewers.

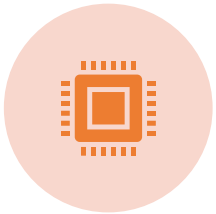
PROPOSED SOLUTION BY THE BROADCASTERS

- During the engagements with the broadcasters, it was proposed that the Authority should implement: **IP/SITE-BLOCKING TO COMBAT PIRACY.**
- **Proposed mechanism — a two-stage process:**
- General Blocking Direction - broadcasters apply to ICASA, providing their detection methodology, categories of content, blocking type (static/dynamic), and anti-over-blocking safeguards.
- Specific Blocking Notices - once approved, broadcasters can issue notices for specific pirated content/IPs/domains, which ISPs must then implement quickly (important for live sport).

WHY THE AUTHORITY



According to Broadcasters; the Authority is ideally placed to put a solution in place because: it regulates both **ISPs** (which are ECS licensees) and **broadcasters.**



It has the **technical know how and capacity** to monitor the systems broadcasters will use to identify what ISPs need to block



The Authority has the power to: **make regulations** on any matter consistent with the objects of the ICASA Act, the ECA and the Broadcasting Act.



The Authority can prescribe standard terms and conditions that apply to licensees (including ECS licensees) and would be able to require ECS licensees that are ISPs to implement blocking directions.

CONCLUSION

The Authority's aim in 2026/27 financial year is to deepen regulatory understanding of emerging risks affecting network reliability and information security across the sectors: Telecommunications, Broadcasting and Postal services.

The Authority will produce a Discussion Document for further engagement with stakeholders on strengthening network reliability and information security and on building consumer trust and confidence in ICT services.



INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA

QUESTIONS SESSION.