COMPETITION AUTHORITY OF KENYA
Creating efficient markets for consumers

BACK-TO-OFFICE REPORT

	Date submitted: **28th July, 2026** _____ **Activity date(s):** *29th June – 3rd July, 2026* _____

Activity details *(name, participants, venue)*

***Name**: The 6th Annual Information Security Management Systems (ISMS) Conference*

***Participants**:*

- *Anthony Irungu, Principal HR & Admin Officer*
- *James Thogo, Principal ICT Officer*
- *Samuel Roba, Senior Investigations Officer, Contracts/Deputy MR*

***Venue:** Sawela Lodge, Naivasha*

Department/Division/Reps:

- *Management Rep. Office*
- *Auditors*

Brief descriptions of the activity *(overview of the activity)*

The 6th Annual Information Security Management Systems (ISMS) Conference was jointly organized by the Kenya Bureau of Standards (KEBS) and the National Computer and Cybercrimes Coordination Committee (NC4) under the theme *"Securing a Digital Future: Fostering Governance and Resilience through ISMS in the Era of AI."* It was held from 29th June to 3rd July, 2026 at Sawela Lodge, Naivasha.

Purpose/objective of the activity

The conference brought together government agencies, regulators, ICT professionals, information security practitioners, and cybersecurity solution providers to strengthen information security governance and cyber resilience in Kenya.

Insights/lessons learned (*brief description of how the lessons learned can be applied at the Authority)*

PRE-CONFERENCE: DAY 1

Status of digital transformation and cybersecurity in Kenya and globally – Leonard Ngeso, NC4

Digital transformation continues to accelerate globally, driven by rapid advances in artificial intelligence (AI), cloud computing, the Internet of Things (IoT), 5G connectivity and data analytics. Governments and businesses are increasingly digitizing public services, financial systems, healthcare, education and supply chains to improve efficiency, innovation and service delivery. However, this increased digital interconnectedness has expanded the cyber threat landscape, with ransomware, phishing, supply chain attacks and AI-enabled cyberattacks becoming more sophisticated and frequent. As a result, cybersecurity has become a strategic priority, with organizations adopting international standards such as ISO/IEC 27001, implementing zero-trust security models and strengthening cyber resilience through risk-based approaches.

In Kenya, digital transformation is a key pillar of national development under the Digital Superhighway and Creative Economy agenda. Significant progress has been made through the expansion of e-government services, digital identity initiatives, mobile money innovations, digital health systems and the rollout of high-speed broadband infrastructure. Kenya's vibrant fintech ecosystem and widespread adoption of mobile technologies have positioned the country as a regional leader in digital innovation. At the same time, increased digitization has heightened exposure to cyber threats targeting government institutions, financial services, critical infrastructure and private enterprises.

To address these challenges, Kenya has strengthened its cybersecurity framework through the Computer Misuse and Cybercrimes Act, the Data Protection Act and the establishment of institutions such as the National Kenya Computer Incident Response Team–Coordination Centre (KE-CIRT/CC) and the National Computer and Cybercrimes Coordination Committee (NC4). Organizations are increasingly implementing Information Security Management Systems (ISMS) based on ISO/IEC 27001 to safeguard information assets, ensure regulatory compliance and enhance business continuity. Continued collaboration among government, industry, academia and international partners remains essential to building a secure, resilient and trusted digital economy.

Information security, cyber security and privacy protection in Kenya – KeBS

Information security, cybersecurity and privacy protection have become fundamental pillars of Kenya's digital economy as government services, financial systems, healthcare, education, and businesses increasingly rely on digital technologies. Information security focuses on protecting the confidentiality, integrity and availability of information, while cybersecurity safeguards networks, systems and digital infrastructure against cyber threats such as malware, ransomware, phishing and unauthorized access. Privacy protection complements these efforts by ensuring that personal data is collected, processed, stored, and shared lawfully and securely. Together, these three disciplines foster public trust, support innovation, and strengthen the resilience of critical information infrastructure.

Kenya has established a robust legal and institutional framework to enhance digital security and privacy. Key legislation includes the Computer Misuse and Cybercrimes Act, 2018, the Data Protection Act, 2019 and regulations issued by the Office of the Data Protection Commissioner (ODPC). Institutions such as the National Kenya Computer Incident Response Team – Coordination Centre (KE-CIRT/CC), the National Computer and Cybercrimes Coordination Committee (NC4) and sector regulators work collaboratively to prevent, detect and respond to cyber incidents. Organizations are also increasingly adopting internationally recognized standards such as ISO/IEC 27001 to implement Information Security Management Systems (ISMS), improve governance, manage cyber risks and ensure compliance with national and international best practices.

Security Operations Center – Palo Alto Networks

A Security Operations Center (SOC) is a centralized capability that continuously monitors, detects, investigates, and responds to cybersecurity threats affecting an organization's information systems, networks, applications and data. It combines skilled cybersecurity personnel, standardized processes, and advanced security technologies such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and threat intelligence platforms to identify and mitigate cyber risks in real time. By providing continuous security monitoring, incident response, threat hunting, and vulnerability management, a SOC enhances an organization's cyber resilience, minimizes the impact of cyberattacks, ensures regulatory compliance, and safeguards the confidentiality, integrity, and availability of critical information assets.

PRE-CONFERENCE: DAY 2

Emerging technologies in ISMS - ISACA

According to ISACA, emerging technologies such as artificial intelligence (AI), machine learning, cloud computing, the Internet of Things (IoT), blockchain, quantum computing and extended detection and response (XDR) are transforming the way organizations manage information security. While these technologies improve operational efficiency, automation, and decision-making, they also introduce new cyber risks, including AI-enabled attacks, cloud misconfigurations, supply chain vulnerabilities and increased exposure of interconnected devices. ISACA emphasized

that organizations should adopt a risk-based approach to integrating these technologies, ensuring that security, governance and compliance are embedded throughout their lifecycle.

ISACA further advocated for modern Information Security Management Systems (ISMS) that are adaptive, resilient and aligned with internationally recognized frameworks such as ISO/IEC 27001 and COBIT. It encouraged organisations to leverage automation, continuous monitoring, threat intelligence and security analytics to enhance cyber resilience while maintaining robust governance and accountability. As emerging technologies continue to evolve, ISACA underscored the importance of continuous risk assessment, workforce upskilling and collaboration among technology, security, and business leaders to ensure innovation is accompanied by effective information security and privacy protection.

Operationalising AI governance with ISMS: Practical controls for trust, accountability and resilience – Dr. Makau, KeBS

Operationalizing AI governance through an Information Security Management System (ISMS) involves embedding AI-specific risk management, accountability and security controls into an organization's governance framework to ensure the trustworthy, ethical and resilient use of artificial intelligence. This includes establishing clear governance structures, defining roles and responsibilities, conducting AI risk and impact assessments, protecting data integrity and privacy, monitoring AI models for bias and performance, maintaining transparency and auditability of AI decisions and implementing continuous monitoring and incident response mechanisms. By aligning AI governance with ISMS and emerging AI governance standards such as ISO/IEC 42001, organizations can strengthen stakeholder trust, ensure regulatory compliance, enhance accountability and build resilient AI systems capable of adapting to evolving technological and cybersecurity risks.

Digital/IS risk quantification for executives – Asset-Based Approach

Digital/Information Security (IS) risk quantification using an asset-based approach enables executives to measure cyber risks in business terms by identifying and valuing an organization's critical information assets, assessing the threats and vulnerabilities affecting those assets and estimating the potential financial and operational impact of security incidents. Rather than relying solely on qualitative risk ratings, this approach quantifies potential losses based on asset value, likelihood of occurrence and business consequences, enabling leadership to prioritize investments, allocate cybersecurity resources effectively, support informed decision-making and demonstrate the value of security initiatives in protecting organizational objectives, regulatory compliance and business resilience.

Cloud Computing – Hpe

Cloud computing is the delivery of computing services such as servers, storage, databases, software and networking over the internet on demand. It enables organizations to scale their IT resources quickly while reducing infrastructure and maintenance costs. Cloud computing supports innovation, business continuity and remote access to applications

and data from virtually anywhere. To ensure secure adoption, HPe recommended that organizations implement strong cybersecurity controls, data protection measures and internationally recognized standards such as ISO/IEC 27001.

DAY 1: MAIN CONFERENCE

Governance and Regulatory Framework: National Cybersecurity Threat Landscape – NC4

From the National Computer and Cybercrimes Coordination Committee (NC4) perspective, Kenya's cybersecurity governance framework is anchored on the Computer Misuse and Cybercrimes Act, 2018, the Data Protection Act, 2019, the National Cybersecurity Strategy (2022–2027) and other sector-specific laws and regulations. These instruments establish a coordinated national approach to preventing, detecting, responding to and recovering from cyber threats while promoting collaboration among government agencies, critical information infrastructure operators, the private sector, academia and international partners. NC4 plays a central role in coordinating national cybersecurity efforts, developing policy, enhancing cyber resilience and fostering information sharing to strengthen Kenya's digital ecosystem.

NC4 recognizes that Kenya's cyber threat landscape continues to evolve as digital transformation accelerates across government and industry. The country faces increasing threats from ransomware, phishing, business email compromise, malware, distributed denial-of-service (DDoS) attacks, insider threats and attacks targeting critical information infrastructure. To address these risks, NC4 advocates for proactive cybersecurity governance, continuous risk assessments, implementation of Information Security Management Systems (ISMS), threat intelligence sharing, capacity building and public-private partnerships. These measures are essential to safeguarding national security, protecting critical services, and building trust and resilience in Kenya's digital economy.

Securing a digital future: Fostering governance and resilience through ISMS in the era of AI – ODPC

From the Office of the Data Protection Commissioner (ODPC) viewpoint, securing a digital future requires organizations to integrate Information Security Management Systems (ISMS) with robust data protection and AI governance frameworks. As artificial intelligence becomes increasingly embedded in public and private sector operations, organizations must ensure that the processing of personal data is lawful, fair, transparent and secure throughout the AI lifecycle. An ISMS based on ISO/IEC 27001 provides a structured approach to managing information security risks, while complementing Kenya's Data Protection Act, 2019 by strengthening confidentiality, integrity, availability, accountability and privacy-by-design principles.

The ODPC emphasized that governance and resilience in the era of AI extend beyond technical security to include responsible data governance, human oversight, transparency and effective risk management. Organizations should conduct data protection impact assessments for high-risk AI systems, implement appropriate technical and organizational measures to safeguard personal data, continuously monitor AI systems for security and privacy risks and

establish clear accountability mechanisms. By embedding privacy, security, and ethical considerations into AI-enabled systems, organizations can enhance public trust, support regulatory compliance and foster responsible digital innovation while safeguarding the rights and freedoms of individual.

DAY 2 & 3: MAIN CONFERENCE

Cybersecurity and digital resilience

From the financial sector players perspective i.e., Equity Bank Ltd, cybersecurity and digital resilience are essential to safeguarding customer trust, ensuring uninterrupted financial services and supporting secure digital innovation.

As financial institutions continue to expand digital banking channels, mobile payments and cloud-based services, Equity emphasized that they must strengthen cyber resilience through robust governance, continuous security monitoring, multi-factor authentication, threat intelligence, incident response capabilities and Information Security Management Systems (ISMS). The bank recommended the adoption of a proactive, risk-based approach to cybersecurity to protect customer data, maintain regulatory compliance, mitigate evolving cyber threats, and ensure the availability, integrity, and confidentiality of critical financial systems and services.

AI, Innovation and Information Security Controls Evolution – Adili

As AI continues to reshape business operations and digital services, organizations must evolve their information security controls to address emerging risks while enabling responsible innovation. From Adili's perspective, effective AI governance requires security controls that are adaptive, risk-based and embedded throughout the AI lifecycle from data collection and model development to deployment, monitoring and decommissioning. Integrating AI governance with ISMS helps organizations strengthen accountability, protect sensitive data, manage AI-related risks, and foster innovation that is secure, ethical, transparent and resilient.

Cyber resilience in a high threat environment – Mahsen Abud, KRA

KRA emphasized the increasing sophistication of cyber threats, which demands that critical public institutions build resilience rather than focus solely on prevention. Mahsen indicated that cyber resilience is achieved through strong governance, continuous risk assessment, secure digital infrastructure, effective incident response, regular testing of business continuity plans and the implementation of internationally recognized information security standards such as ISO/IEC 27001. This integrated approach enables KRA to protect sensitive taxpayer information, sustain essential tax and customs services during cyber incidents and strengthen public trust in Kenya's digital revenue administration.

FUTURE READINESS

Human Security – Secure Behavior, Culture and People Aspects of ISMS – Dr. Marigat

Future readiness in information security depends not only on technology but also on people, culture and secure behavior. A human-centric ISMS fosters a security-conscious culture by promoting continuous awareness, leadership commitment, accountability and responsible digital practices across all levels of an organization. Empowering employees to recognize and respond to cyber risks, encouraging secure behaviours and embedding security into everyday business processes reduces human-related vulnerabilities, strengthens resilience and creates a sustainable foundation for protecting information assets in an increasingly complex digital environment.

Standard-Based Solutions for AI, Cyber Security and Privacy Solutions

As organizations accelerate digital transformation and AI adoption, standards-based solutions provide a consistent framework for managing information security, cybersecurity and privacy risks.

International standards such as ISO/IEC 27001 (Information Security Management Systems), ISO/IEC 27701 (Privacy Information Management), ISO/IEC 42001 (Artificial Intelligence Management Systems) and the ISO/IEC 27000 family enable organizations to establish effective governance, implement risk-based controls, ensure regulatory compliance and build resilient digital systems. Adopting these standards helps organizations strengthen stakeholder trust, promote responsible innovation and safeguard information assets while adapting to the evolving cyber and AI risk landscape.

Recommendations/Action points *(What actions is the Authority required to take, by when, by whom)*
Based on the Information Security Management Systems (ISMS), cybersecurity, AI governance, cloud computing, digital resilience and privacy themes discussed, the following four (4) recommendations suffice:

1. Strengthen ISMS implementation and certification by adopting and maintaining ISO/IEC 27001 to establish a risk-based approach to information security, improve governance, and enhance organizational resilience.
2. Embed AI governance into organizational frameworks by implementing clear policies, conducting AI risk and impact assessments and aligning AI deployment with standards such as ISO/IEC 42001 to ensure transparency, accountability and responsible innovation.
3. Enhance cyber resilience through continuous monitoring and incident response by investing in Security Operations Centers (SOCs), threat intelligence, regular vulnerability assessments and business continuity and disaster recovery capabilities.
4. Promote a security-conscious organizational culture by conducting regular cybersecurity awareness training, strengthening leadership commitment and fostering secure behaviors to reduce human-related cyber risks.

COMPETITION AUTHORITY OF KENYA
Creating efficient markets for consumers

Appendix

a. Copies of Certificate

Prepared by:

Anthony Irungu	
James Thogo	
Samuel Roba	

Approved by:

_____

Signed:

_____