



National Computer and Cybercrimes Coordination Committee (NC4)

GUIDELINES FOR IMPLEMENTING SECURITY OPERATIONS CENTERS (SOC)

2025

FORWARD

As we continue to navigate the complexities of the digital age, the legal landscape surrounding cybersecurity remains a critical pillar in safeguarding our operations. In alignment with the **Computer Misuse and Cybercrimes Act 2018** and the **Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024**, it is crucial that we stay vigilant and proactive in securing our critical information infrastructure.

These regulations establish important guidelines for managing cyber threats, protecting sensitive data, and ensuring the resilience of our critical systems. As part of our commitment to upholding the highest standards of security and compliance, the implementation of Cybersecurity Operations Center (SOC) must be fully aligned with these guideline requirements.

This document provides you with the key steps and guidelines for establishing and managing SOC in line with the **Cybercrime Management Regulations**. It also outlines how we can work together to ensure that our practices reflect the intent of the **Computer Misuse and Cybercrimes Act 2018**, while addressing emerging challenges in the ever-evolving world of cyber threats.

Our collective responsibility is to build and maintain a SOC that not only meets internal security objectives but also aligns with these national regulations to protect our organization and the broader digital ecosystem. I urge you to review these guidelines thoroughly and engage with your teams to ensure compliance, efficiency, and the continuous enhancement of our cybersecurity posture.

Together, we can build a robust framework for combating cybercrime, protecting critical infrastructure, and ensuring a secure environment for all stakeholders.

Thank you for your continued support and cooperation.

Col (Dr) James J Kimuyu, PhD

Director

National Computer and Cybercrimes Co-ordination Committee

1.0 Introduction

The establishment of a robust Cybersecurity Operations Center (SOC) is paramount for organizations seeking to proactively monitor, detect, prevent and defend against the ever-evolving landscape of cyber threats. This document serves as a guide for planning and developing a SOC, aligning with both industry best practices and the legal frameworks established by the Computer Misuse and Cybercrimes Act, 2018 and the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024.

2.0 Categories of SOC

There are different categories of SOC in Kenya

- a. **National Cybersecurity Operations Centre** - National focal point for monitoring, detecting, preventing, responding, investigating and attribution of cyber threats, computer and cybercrimes in Kenya.
- b. **Sector Cybersecurity Operations Centre** - Responsible for monitoring, detecting, preventing, responding and investigating cyber threats, that are specific to specific Sector.
- c. **Critical Information Infrastructure Cybersecurity Operations Centre** - Responsible for monitoring, detecting, preventing, responding and investigating of cyber threats, in a Critical Information Infrastructure.
- d. **Organizational Cybersecurity Operations Centre** - Responsible for monitoring, detecting, preventing, responding and investigating of cyber threats, in an organization.

3.0 Overall Capabilities of a SOC

At minimum, every SOC should have the following capabilities.

- a. Real time event monitoring, analysis, log collection and aggregation
- b. An alert system
- c. Cybersecurity specialists organized to prevent, detect, analyse and respond to threats
- d. Asset inventory
- e. Vulnerability management
- f. Network detection and response

- g. End point detection and response
- h. Intrusion detection
- i. Malware analysis and testing
- j. Threat prevention, monitoring and detection
- k. Incidence response and management
- l. Threat intelligence platform.

4.0 Functions of Cybersecurity Operations Centers

a. The National Cybersecurity Operations Center

The National Cybersecurity Operations Center shall

- (1) Have visibility of threats and incidents that occur in Sector Cybersecurity Operations Centre(s) and Critical Information Infrastructure Cybersecurity Operations Centre(s).
- (2) Have the capability to perform the functions of a Sector Cybersecurity Operations Centre and Critical Information Infrastructure Cybersecurity Operations Centre.
- (3) Co-ordinate response to cybersecurity incidents Nationally and within the Sector Cybersecurity Operations Centre(s) and Critical Information Infrastructure Cybersecurity Operations Centre(s).
- (4) Coordinate capacity building programs, research and development activities on cyber threats and incidents.
- (5) Report to the Committee on all cyber incidents reported by the Sector Cybersecurity Operations Centre(s) and Critical Information Infrastructure Cybersecurity Operations Centre(s).
- (6) Convene cybersecurity meetings, colloquiums, webinars, workshops or other consultative platforms for Cybersecurity Operations Centre(s).
- (7) Undertake research and development for tool engineering.
- (8) Facilitate cooperation of the Committee with Sector Cybersecurity Operations Centre(s) and Critical Information Infrastructure Cybersecurity

Operations Centre(s) and other relevant bodies, locally and internationally in response to threats of computer and cybercrime incidents.

b. The Sector Cybersecurity Operations Centers

The Cybersecurity Sector Operations Center shall

- (1) Collaborate, through information and threat intelligence sharing, within the Sector.
- (2) Coordinate advanced cyber threat analytics particularly on Sector specific threats, incidence response, joint trainings or joint exercises and other cross-sectoral cybersecurity initiatives.
- (3) Have visibility of threats and incidents that occur in the Critical Information Infrastructure Cybersecurity Operations Centre(s) in the Sector.
- (4) Have the requisite capability to perform the functions of a Sector Critical Information Infrastructure Cybersecurity Operations Centre.
- (5) Convene consultative foras through meetings, colloquiums, webinars, workshops or other platforms on sectoral issues of common interest to the sectors.
- (6) Co-ordinate sectoral threat, monitor and respond to incidents in the Critical Information Infrastructure Cybersecurity Operations Centre(s) in their respective Sector including:
 - (a) Collecting, analyzing and responding to threats reported by the Critical Information Infrastructure Cybersecurity Operations Centre(s);
 - (b) Having visibility of threats and incidents that occur in the Critical Information Infrastructure Cybersecurity Operations Centre(s);
 - (c) Co-operating with computer incident response teams through sharing of threat intelligence to inform response to cyber incidents, utilizing technologies and tools;
 - (d) Receiving real-time information on cyber threats and incidents from the Critical Information Infrastructure Cybersecurity Operations Centre(s);
 - (e) Threat and information sharing
 - (f) Incidence response coordination

- (g) Joint exercises and training of the critical information infrastructure cybersecurity operations Centre(s)
 - (h) Supporting supply chain risk management efforts
- (7) Coordinate capacity building programs, research and development activities on cyber threats and incidents in the Sector.
- (8) Report to the National Cybersecurity Operations Centre on all cyber incidents reported by the Critical Information Infrastructure Cybersecurity Operations Centre(s) in the Sector.
- (9) Undertake research and development for tool engineering.
- (10) Facilitate collaboration and cooperation amongst Critical Information Infrastructure Cybersecurity Operations Centre(s) in the Sector.
- (11) Utilize threat surveillance from internal and external sources to enhance its situational awareness and response capabilities.
- (12) Facilitate the implementation of standards operating procedures formulated by the Committee to guide the Operations of the Critical Information Infrastructure Cybersecurity Operations Centre(s).

c. Critical Information Infrastructure (CII) Cybersecurity Operations Center

The Critical Information Infrastructure Cybersecurity Operations Centre shall

- (1) Provide real-time information on cyber threats and incidents to the National Cybersecurity Operations Centre and Sector Cybersecurity Operations Centre.
- (2) Collaborate with the relevant agencies, on cyber threat surveillance and analysis.
- (3) Have the requisite capability to detect, monitor, prohibit, prevent, respond and investigate cyber threats, computer and cybercrimes in the concerned organization.

- (4) Be responsible for incidence detection, analysis and response in the organization.
- (5) Undertake capacity building programs, research and development activities on cyber threats and incidents in the organization.
- (6) report to the respective Sector Cybersecurity Operations Centre on all cyber incidents reported in the organization.
- (7) undertake research and development for tool engineering.
- (8) co-operate with other Critical Information Infrastructure Cybersecurity Operations Centre(s) in the concerned Sector.
- (9) utilize threat surveillance from internal and external sources to enhance its situational awareness and response capabilities.
- (10) implement the codes or standard operating procedures formulated by the Committee to guide the Operations of the Critical Information Infrastructure Cybersecurity Operations Centre(s).

Each owner of a Critical Information Infrastructure shall meet the administrative costs and other expenses of their respective Critical Information Infrastructure Cybersecurity Operations Centre.

d. Organizational Cybersecurity Operations Center

Given that Organizations may not have the financial resources to implement a full-fledged Security Operation Centre (SOC), this section provides a cost-effective approach to cybersecurity operations, focusing on collaboration, threat intelligence sharing, and incident response.

The Organizational Cybersecurity Operations Center shall:

- (1) Utilize affordable or open-source cybersecurity tools to monitor network traffic and detect potential threats.
- (2) Leverage third-party security services such as Managed Security Service Providers (MSSPs) to enhance cybersecurity without significant capital investment.
- (3) Partner with National and Sectoral Cybersecurity Operations Centers to receive threat intelligence.

- (4) Collaborate with other Organizations to share insights on emerging cyber threats and best practices.
- (5) Develop a standardized incident response plan for handling cybersecurity breaches effectively.
- (6) Collaborate with government and private sector Computer Emergency Response Teams (CERTs) to coordinate responses to cyber incidents.
- (7) Conduct periodic training for employees on cybersecurity best practices, including phishing awareness, password management, and secure handling of customer data.
- (8) Establish minimum security requirements for third-party vendors in line with Third Party Management Guidelines
- (9) Participate in collaborative research initiatives to develop cost-effective cybersecurity solutions tailored to their specific needs.

5.0 SOC Deployment Models

Organizations are encouraged to choose a Cybersecurity Operations Center (SOC) deployment model that aligns with their operational needs, budget, and cybersecurity maturity. Selecting the right model ensures effective threat detection, incident response, and compliance with security best practices. Entities may opt for an in-house SOC, engage a Managed Security Service Provider (MSSP), or adopt a hybrid approach, depending on their specific requirements.

The following are considerations for SOC Deployment Models:

a. In-House SOC

This model involves building and managing a dedicated SOC within the organization. It requires investment in infrastructure, technology, and skilled personnel to handle security operations independently.

It offers full control over security, ensuring data privacy and regulatory compliance. Organizations benefit from faster threat response and seamless integration with internal systems. However, maintaining an in-house SOC demands continuous

investment in staff training, automation, and threat intelligence to stay ahead of evolving cyber risks.

b. Managed SOC (MSSP)

This model involves outsourcing SOC operations to a Managed Security Service Provider. It reduces costs and provides access to expert cybersecurity resources and advanced technology.

To address data security risks, organizations should enforce strong SLAs, ensure compliance with data localization laws, and implement encryption and access controls. Close collaboration with the MSSP enhances incident response and threat intelligence sharing.

c. Hybrid SOC

This model blends in-house security with outsourced services, balancing control and cost efficiency. Organizations retain critical security functions while leveraging external expertise for specialized tasks.

A successful hybrid SOC requires clear coordination between internal teams and the MSSP. Integrating security tools, ensuring real-time threat visibility, and defining responsibilities help maximize its effectiveness.

6.0 SOC Operationalization

The overall strategy for building a SOC involves the following key steps

a. Plan

- (1) Define the SOC Strategy
- (2) Establish the SOC capabilities
- (3) Conduct Maturity Assessment
- (4) Establish People Processes and Technologies

b. Design

- (1) Facilities
- (2) Infrastructure
- (3) Data collection
- (4) Event correlation and Data analysis
- (5) Incident Response plan
- (6) Vulnerability management
- (7) Evaluation Metrics
- (8) Collaboration flows

(9) Business continuity plan

c. Build

- (1) Facilities
- (2) Infrastructure
- (3) Use cases manual
- (4) Event correlation and Data analysis
- (5) Vulnerability management
- (6) Processes
- (7) Ticketing system integration

d. Operate

- (1) Collect measurements
- (2) Implement KPIs
- (3) Continuous assessments
- (4) Feed to risk management
- (5) Security intelligence
- (6) Incident response

7.0 Key Considerations for Implementing a SOC

For organizations that choose to implement the In-house and Hybrid SOC, the following considerations should be made:

a. Define the SOC architecture in your organization

Based on your business model, select your SOC architecture as either:

- (1) **Multi-Center Distributed Architectures:** This architecture relies on a hierarchical SOC approach and each organization unit is responsible for managing alerts in real time and only critical alerts are brought to the attention of the SOC staff.
- (2) **Fully Integrated Architecture:** This provides a real time monitoring for all business units in the utility – mostly used by large organizations.

b. Set up SOC Team Structure and Roles

A SOC should have a multi-tiered team with well-defined responsibilities to ensure seamless operations

- (1) **SOC Analysts (Tiers 1-3):** Responsible for monitoring security events, analyzing alerts, escalating incidents, and responding to threats.
- (2) **Incident Response Team:** Experts responsible for handling security incidents, conducting forensic investigations, and mitigating cyber threats.
- (3) **Threat Intelligence Analysts:** Focus on gathering and analyzing cyber threat intelligence to proactively defend against attacks.
- (4) **Security Engineers:** Ensure that security tools, systems, and network defenses are optimally configured and maintained.
- (5) **SOC Manager:** Oversee SOC operations, manage team workflows, and develop strategic security initiatives.

c. Establish Collaboration and Coordination Mechanisms

To enable compliance with CMCA regulations sec 12 (2) establish collaboration mechanisms between the 3 layers of governance which include;

- (1) National SOC
- (2) Sector SOC
- (3) Other CII SOC's

d. Establish key SOC Processes

- (1) **Threat Monitoring & Detection:** Implement continuous monitoring across networks, endpoints, and cloud environments using SIEM, IDS/IPS, and behavioral analytics to detect anomalies and potential threats.
- (2) **Incident Detection & Analysis:** Establish structured mechanisms for alert triage, correlation, and prioritization to ensure timely identification and classification of security incidents based on severity and impact.
- (3) **Incident Response & Containment:** Develop predefined incident response playbooks to enable rapid containment, isolation of affected systems, and mitigation of threats to minimize disruption.
- (4) **Threat Intelligence & Hunting:** Incorporate cyber threat intelligence (CTI) to proactively identify emerging threats, enhance defense strategies, and conduct threat-hunting activities to detect hidden adversaries.

- (5) **Vulnerability & Risk Management:** Conduct regular vulnerability assessments and penetration testing to identify, prioritize, and remediate security weaknesses before exploitation.
- (6) **Security Log Management & Compliance:** Ensure proper log collection, storage analysis to support regulatory compliance (CMCA Sec 12(2), NIST, ISO 27001) and forensic investigations.
- (7) **Post-Incident Review & Continuous Improvement:** Perform post-mortem analysis on security incidents to identify lessons learned, update SOC policies, and strengthen defenses against future threats.
- (8) **Security Awareness & Training:** Implement ongoing cybersecurity awareness programs for employees and conduct SOC training sessions to enhance skills and preparedness against cyber threats.
- (9) **Automation & Orchestration:** Leverage SOAR (Security Orchestration, Automation, and Response) solutions to streamline incident response, reduce manual workload, and improve operational efficiency.

e. Select and implement key technologies as stipulated in part 2 of this document

8.0 Coordination and Collaboration

Coordination and Collaboration Between National, Sector, CII and Organizational SOCs

- (1) The National SOC acts as the coordinator, receiving and analyzing threat intelligence and incident reports from other SOCs.
- (2) Sector SOCs facilitate sector-specific intelligence exchange and coordinate cybersecurity responses across CII SOCs within their jurisdiction.
- (3) CII SOCs engage in active threat monitoring and reporting to Sector SOCs, ensuring prompt response to security incidents.
- (4) All SOC levels participate in intelligence-sharing, joint cybersecurity exercises, and capacity-building programs to strengthen collective defense.
- (5) Organizations benefit from Sector and National SOC support through access to threat intelligence and incident reporting frameworks.

- (6) Organizational SOC should implement managed security services and align their response strategies with Sector SOC protocols to enhance resilience.
- (7) Organizations are encouraged to collaborate with national cybersecurity agencies to strengthen cybersecurity awareness and response capabilities.
- (8) Through established secure communication channels, SOC should adopt standardized frameworks to facilitate real-time exchange of threat data, ensuring consistency in intelligence reporting.
- (9) Through the National and Sector SOC, regular cybersecurity updates and reports are circulated among SOC to maintain situational awareness and informed decision-making.
- (10) All SOC should follow clear escalation protocols that define how security incidents are reported and resolved across SOC levels.
 - (a) Sector SOC should coordinate cross-sector cybersecurity responses, ensuring rapid containment and mitigation.
 - (b) The National SOC provides oversight for large-scale incidents, ensuring unified action for containment and recovery.

All SOC should collaborate in research and development initiatives to advance SOC efficiency and introducing innovative security solutions

9.0 Conclusion

NC4 recognizes each Sector regulators, and entities have their own unique mandates, systems and security challenges. To allow for flexibility, the guidelines are not made to be exhaustive or concussive. The Heads and Chief Executive Officers of the various CIIs entities must take initiative to ensure compliance design, development, deployment and operations of an appropriate SOC. At the same time, they should prioritize the building the necessary human resource critical mass and technical capabilities that will ensure Systems resilience to support their business operations and service to the people of Kenya.