MINISTRY OF COMMUNICATIONS, TECHNOLOGY AND INNOVATION

REPUBLIC OF SIERRA LEONE

SIERRA LEONE DIGITAL TRANSFORMATION PROJECT
IDA- E1130-SL

Terms of Reference
for

NC3 STAFF CAPACITY DEVELOPMENT FOR NEWLY RECRUITED STAFF

APRIL 2024

Terms of Reference

NC3 Staff Capacity Development For Newly Recruited Staff

I. Introduction

The Government of Sierra Leone (GoSL) has committed to transforming its economy based on a more inclusive and human-centric digital growth and development approach. A high-level vision for the digital economy is articulated in the new National Digital Development Policy (NDDP), which was approved by the Cabinet in December 2021 setting the GoSL's vision to transform Sierra Leone into an inclusive digital economy and society and to leverage digital technology to support the GoSL to deliver on its national development plan effectively and efficiently. The Sierra Leone Digital Transformation Project (SLDTP) aims to expand access to broadband internet, increase digital skills and improve government capacity to deliver public services digitally. The Project will support the development of a strong enabling environment for the nation's digital transformation and digital development agenda as articulated in the National Digital Development Strategy.

As Sierra Leone strives to leap-frog its socio-economic development with the catapultic force of the 4th Industrial revolution, the risks posed by cybersecurity and cybercrime cannot be easily brushed aside. Thus, to combat the growing rate of cybercrimes and protect the country's critical information infrastructure as it embarks on its digital transformation journey, the House of Parliament enacted the Cybersecurity and Crime Act through the Ministry of Information and Communications in 2021. This Act provides the legal provisions required to facilitate the investigation of cybercrimes and cyber-related crimes, clearly identifies the penal offences, and enables effective and efficient international cooperation to exchange digital evidence. Moreover, it stipulates the institutional framework for the fight against cybercrimes, including protecting the country's critical information infrastructure, which is crucial in ensuring essential societal services provision and safer cyberspace for all Sierra Leoneans.

II. Project Description

The Sierra Leone Digital Transformation Project (SLDTP) is a five-year International Development Association (IDA)-funded Project supported by a US$50 million grant. The Project's primary implementing agency is the Ministry of Information and Communications (MIC). The proposed Project Development Objective (PDO) is to expand access to broadband internet, enhance digital skills and improve government capacity to deliver public services digitally.

The SLDTP proposes four integrated and mutually reinforcing components, with a fifth component dedicated to contingent response to future emergencies (*Contingent Emergency Response Component*, *CERC)*.

- Component 1 – Expanding Digital Access and Increasing Resilience of the Digital Environment;
- Component 2 – Digital Skills Development and Innovation
- Component 3 - Laying Key Foundations for Digital Government Services and Systems
- Component 4 – Project Management and Implementation Support and
- Component 5 - Contingency Emergency Response Component (CERC).

The proposed activities integrated into Components 1, 2, and 3 are designed to support the Government in building resilient and inclusive policies by strengthening its legal and regulatory frameworks, scaling up the citizen-centric digital public service delivery by reinforcing the government portal and relevant Ministries, Departments, and Agencies (MDAs) capacity. By enhancing the service delivery infrastructure and platforms, the Project will support and ensure the continuity of public services in times of crisis.

The Project is being implemented by a Project Coordination Unit (PCU) in the Ministry of Communications Technology and Innovation (MCTI).

a. The National Cybersecurity Coordination Centre (NC3) is a sub-vented Agency established by the Cybersecurity and Crime Act 2021. This institution oversees all cybersecurity issues in Sierra Leone, including providing support to computer systems and networks in preventing and combating cybercrimes in Sierra Leone, formulating and implementing national cybersecurity policy and Strategy, overseeing the management of computer forensic laboratories, providing support to the Judiciary and other law enforcement agencies in the discharge of their functions concerning cybercrime in Sierra Leone, promoting Sierra Leone's involvement in international cybersecurity cooperation and doing other acts or things that are necessary for the adequate performance of the functions of the relevant security and enforcement agencies under the Act.
b. The government's vision for cybersecurity is to have an enabling environment that is secure, credible, and trustworthy for using ICTs while empowering citizens with the freedom to use the Internet safely for the nation's socio-economic benefits. This responsibility lies directly within the scope of Component One in the SLDTP project, which aims to enhance digital access and bolster the resilience of the digital environment.

III. Objectives

a. General Objectives

The main objective of this TOR is to recruit a competent consultancy firm to equip the newly recruited staff of the NC3 with the general skills, tools and organisational culture of working in a national cybersecurity agency and to build a resilient cyber team with a key focus on service delivery and implementation.

b. Specific Objectives

More concretely, the specific objectives include but are not limited to the following:

i. To design and implement an effective orientation program for newly recruited staff of the NC3, ensuring a comprehensive understanding of organisational policies, procedures, and values while fostering a sense of belonging within the cybersecurity ecosystem.

ii. To enhance staff capacity in IT service delivery methodologies by providing comprehensive training in the Information Technology Infrastructure Library (ITIL), preparing staff for certification and enabling them to apply best practices in IT service management, thereby improving service delivery efficiency and effectiveness.

iii. To equip staff with holistic knowledge and foundational skills in Scrum and Lean methodologies, emphasising their application in Agile project environments, fostering an environment of agility, adaptability, and continuous improvement within project management practices.

iv. To formulate a 3-year detailed strategic work plan aligned with the goals and priorities outlined in the National Cybersecurity Strategy.

IV. Scope of Work

The consulting firm will seek to create and implement a comprehensive, structured and interactive plan to onboard, develop and empower staff while aligning their skills with the overarching cybersecurity vision. The target audience is 22 staff members ranging from directors to junior-level staff. The activities to be performed by the Consulting Firm include the following:

1. Inception Report (Deliverable 1)
   A. Familiarise with the National Cybersecurity and Crime Act of 2021, the National Cybersecurity Strategy and the role of cybersecurity in the GoSL Digital Transformation process.
   B. Hold two (2) planning meetings with the SLDTP and NC3 to scope out the needs of the capacity-building initiatives.
   C. Prepare and develop tailor-made training agenda/content. The contents will be shared with the SLDTP project team and the NC3 for input and finalisation.
   D. Prepare and submit an inception report that includes an assessment of training objectives, delivery plan, training approach/techniques, roles and responsibilities and timelines.

2. Implementation

A. Finalise NC3 Staff Handbook and Conduct Staff Orientation (Deliverable 2)

- Review the institution's draft conditions of service for NC3 staff and provide expert HR feedback that can be incorporated into the text.
- Work with the NC3 and Ministry of Labour to finalise the text
- Print 30 high-quality copies of the Staff Hand for distribution during the orientation session.
- Conduct interactive staff orientation sessions covering organisational structure, roles and responsibilities and an overview of the Centre's culture and values.

B. Conduct Training on IT Service Management and Agile (Deliverable 3)

- The course shall include the ITIL 4 Foundation: Create, Deliver and Support
- Certified ScrumMaster (CSM)
- All training programs must be inclusive of the international certification exams.

C. Develop a Detailed 2024-2026 Workplan Aligned with the National Cybersecurity Strategy (Deliverable 4)

- Work with the NC3 team to develop and finalise a detailed 3-year strategic workplan incorporating actionable steps, timelines, identified stakeholders and owners in alignment with the National Cybersecurity Strategy.

V. Reporting, Time Schedules, and Payment Schedule

The Firm is expected to complete the assignment in full within nine (9) weeks, and the Firm will regularly report to the SLDTP Project Coordinator and the National Cybersecurity Coordinator on all aspects of the agreed activities.

No	Deliverable	Timeline	Indicative payment schedule
1	Inception Report	Commencement + 2 Weeks	10%
2	Finalise NC3 Staff Handbook and Conduct Staff Orientation	Commencement + 5 Weeks	25%
3	Conduct Training on IT Service Management and Agile	Commencement + 8 Weeks	50%

4	Develop a Detailed 2024-2026 Workplan Aligned with the National Cybersecurity Strategy (Deliverable 4)	Commencement + 9 Weeks	15%

VI. Delivery Method

The Consulting Firm shall work on documents or training materials in or outside Freetown, Sierra Leone. However, all courses and the orientation session should be done onsite at Freetown, Sierra Leone.

The services and deliverables provided by the Firm may be used by or shared with all the staff of the NC3. The SLDTP, in consultation with the NC3, may decide at reasonably short notice which training mode will be used for a specific requirement.

VII. General Requirements of the Training Courses

- The Consulting Firm shall conduct all training courses and assessments and provide all course material in the English language;
- The Consulting Firm shall provide onsite courses in Freetown, Sierra Leone, for audiences of an average class size of 20, with a maximum of 25 participants;
- The Consulting Firm shall offer extensive online training materials for delivered courses;
- When relevant, the Consulting Firm shall provide self-hosted or partner-based certification examinations in-person at Freetown, online, or at local testing facilities in Sierra Leone.
- Technology courses shall include relevant best practices from the industry.
- The Consulting Firm shall have:
    - Proper registration and all required licenses and accreditation for the provision of training courses and licenses for tools and software used for the delivery;
    - A pool of professional Instructors;
    - Positive experience in the provision and development of training. A proven record of at least three (3) satisfied customers to whom the relevant service was provided in the last five (5) years, among which at least one was an international organisation and

- Designated Account Manager/point of contact for training enquiries and coordination.
- Trainers/Instructors proposed for the Training Course delivery shall have "real-world"/industry-related expert knowledge in the requested training categories and shall have
- Good command of English language (written and oral) and communication skills, with a sensitivity towards a multicultural environment;
- A minimum of 5 years of experience in providing IT training and assessment services as described in this SOW;
- A proven record of at least 3 satisfied customers to whom the relevant service was provided in the last 3 years; and
- Industry accreditations and certifications or similar qualifications relevant to the services and assessments provided (e.g. PEOPLECERT for ITIL and ScrumMaster)

VIII. Qualification and Experience of Team Members

The assignment calls for a team of at least five (5) persons who will possess the following qualifications, skills and experience:

Key Position	**Experience**
(1) Team Leader	Minimum of 15 years of work experience, preferably including in Sierra Leone/West Africa and with public service providers; the team leader will be responsible for coordinating the team, communications with the SLDTP and the client (NC3), and the overall direction, quality and timeliness of all outputs;
(1) Cybersecurity Specialist	Minimum of 10 years of work experience in cybersecurity and implementing best practices. This specialist will provide domain knowledge and expertise in cybersecurity. The specialist must understand the current threat landscape. S/he will help integrate the ITIL and SCRUM framework effectively into NC3 work processes.

(1) HR Specialist	A minimum of 10 years working experience in the HR field. This specialist is responsible for providing expert advice on the draft NC3's Condition of Service and helping in the onboarding process and organisational cultural aspects.
(1) ITIL Expert	More than 5 years of conducting hands-on sessions for specific ITIL tools relevant to cybersecurity. This expert must provide in-depth knowledge and training on ITIL practices for efficient IT services.
(1) SCRUM Master	More than 5 years of conducting hands-on sessions for specific SCRUM tools relevant to cybersecurity. Guides the team in implementing SCRUM methodologies and ensures adherence to agile principles.