



► ILO External Collaboration Contract Terms of Reference:

Consultancy: Supporting the Development of a Cybersecurity Curriculum for TVET in Rwanda.

I. Background and purpose

Rwanda's *National Strategy for Transformation (NST2)* places digital transformation at the center of its ambition to build a knowledge-based economy. The country is positioning itself as a regional digital hub, with strong emphasis on digital skills development, innovation, and ICT-driven growth. The Government of Rwanda has made notable progress toward this vision through initiatives such as the Smart Rwanda Master Plan, investments in digital infrastructure, and the National Digital Skills Framework (NDSF), which sets standardized benchmarks for digital literacy and workforce readiness.

Ensuring the success of this transformation requires a skilled and adaptive workforce capable of meeting the growing demand for digitally competent professionals. Rwanda's rapid growth in online services across health, finance, education, and public administration presents a strong opportunity to position the country as a leader in secure digital innovation. By equipping youth with practical, industry-aligned skills in cybersecurity and data protection, Rwanda is well-placed to strengthen digital trust, enable business growth, and safeguard its expanding digital ecosystem.

To address these challenges, the Global Initiative on [Decent Jobs for Youth](#) is implementing the [Boosting Decent Jobs and Enhancing Skills for Youth in Rwanda's Digital Economy project](#). This four-year partnership, funded by the Government of Luxembourg and implemented by the International Labour Organization (ILO) is supporting the Government of Rwanda, employers' and workers' organizations, and young people to contribute to the country's structural transformation and digitalization agenda.

More specifically, it aims to empower young women and men (aged 18–30) in Kigali and secondary cities to access decent employment and entrepreneurship opportunities in the digital economy. The project is part of a broader ILO/ITU/AU Joint Programme spanning several African countries, focusing on:

- Job creation and entrepreneurship in the digital economy
- Digital skills development for young people
- Facilitating the transition to decent work in the digital economy

Under Outcome 2, the project focuses on improving digital skills of young men and women through strengthened partnerships for the delivery of training programmes and the establishment of digital campuses across the TVET system. To this end, the ILO seeks to engage a consultant/ service contract to support TVET and National Cyber Security program and the ILO in the development and integration of new cybersecurity, data protection, and privacy curricula (equivalent to RTB's Level 3 modules and potential some modelues at level 4 and 5) within selected TVET schools. This work will include the design of modular training aligned to labour market needs, the creation of hands-on lab-based learning resources, and the adaptation of teaching delivery to a digital campus model, with the aim of piloting Cybersecurity Centers of Excellence in Rwanda.

The Cybersecurity Curriculum Development initiative is a collaborative national programme designed to equip Rwanda's workforce with practical skills in cybersecurity, data protection, and privacy, essential for safeguarding the country's digital transformation. The programme is jointly led by the National Cyber Security Authority (NCSA), mandated to protect Rwanda's digital infrastructure and national assets, the Rwanda TVET Board (RTB), responsible for ensuring quality and alignment within the TVET system, and the International Labour Organization (ILO), which provides technical expertise in competency-based training and international standards.

The programme delivers Level 3 modules of the Rwanda TVET Qualification Framework (RTQF) through a modular curriculum that combines classroom learning, online resources, and lab-based exercises. The training covers key areas including Cybersecurity Essentials, Blue Teaming (SOC and Threat Hunting), Governance, Risk and Compliance (GRC), and Data Protection and Privacy, providing structured entry points into the cybersecurity profession and ensuring alignment with industry needs.

To build on Rwanda's digital skills agenda and strengthen pathways from foundational training to employment, the initiative will establish Cybersecurity Centers of Excellence in selected TVET schools. These centers will serve as stepping stones between basic digital literacy and advanced, hands-on learning experiences. By aligning national cybersecurity priorities with TVET curricula and fostering industry partnerships, the programme aims to improve the relevance and quality of training and better prepare young Rwandans for decent jobs in the digital economy, ultimately contributing to Rwanda's broader digital transformation agenda under NST2.

II. Scope of work

This initiative responds to the growing demand for cybersecurity professionals equipped not only with technical knowledge but also with the practical skills required to safeguard Rwanda's digital transformation. As part of the implementation of the ILO's Digital Skills for Decent Jobs Programme in Rwanda, the objective of this consultancy is to partner with the National Cyber Security Authority (NCSA), the Rwanda TVET Board (RTB), and the ILO in leading technically (1) the finalization and validation of a cybersecurity, data protection, and privacy curriculum, building on the existing NCSA programme and work with RTB to secure its accreditation under the Rwanda TVET Qualification Framework (RTF).

III. Detailed tasks

Deliverable 1 – Curriculum Finalization & Accreditation Dossier (technical leadership) (26 days)

1.1. Curriculum Review and Development (10 days)

- Review and consolidate existing materials developed under the NCSA programme including the concept note, expectation document, etc.; map to RTQF Level 3 outcomes and RTB QA policies.
- Develop full curriculum for cybersecurity in TVET.
- Develop the occupational standards as part of the curriculum development following TVET CBC Development Framework.

1.2. Curriculum Structure and Content Design (6days)

- Develop the programme description, competency standards, syllabi, sequencing, contact hours, and cross-cutting themes (safety, ethics, inclusivity).

1.3. Assessment and Accreditation Framework (7days)

- Develop a CBET-aligned assessment, moderation and quality assurance framework (formative & summative tools, logbooks, competency checklists, moderation plans).
- Prepare an accreditation dossier package that meets RTB requirements (application forms, annexes, trainer registration templates, evidence list).

Deliverable 2.a – Stakeholder Validation (2 day)

- Plan and facilitate a validation workshop with NCSA, RTB, industry/employer and worker representatives, document inputs and decisions.
- Revise curriculum and competency standards reflecting validated changes; produce a validation report with an issues log and resolutions.

Deliverable 2.b – Submission & Implementation Readiness(1 day)

- Submit the accreditation dossier to RTB and support the technical review process (responses to comments, crosswalks, document control).
- Produce a concise implementation-readiness note (LMS/metadata structure, materials list, pilot scheduling options, inclusive participation considerations).

Expected deliverables

The assignment will be carried out over approximately four (4) months from December 2025 to March 2026. The estimated Level of Effort (LoE) is approximately twenty six (26) working days distributed across the period for preparation, validation and submission. The duty station is Kigali, Rwanda, with missions to selected locations as required.

Deliverable	Description	Acceptance Criteria	Due Date
D1.a Inception & Curriculum Framework	Inception report (workplan, risks/QA), curriculum framework (programme description, structure, competency map), and accreditation dossier outline.	Complete and coherent; alignment to RTQF L3 & RTB QA evidenced; endorsed by RTB/NCSA/ILO.	2 weeks from signing the contract
D1.b Draft Curriculum Package	Full draft curriculum (modules, hours, learning outcomes, assessment & moderation framework) and complete accreditation dossier ready for RTB submission.	Meets dossier completeness checklist; accessible formatting; internal technical review cleared by RTB/NCSA/ILO.	6 weeks from signing the contract
D2.a. Validation Workshop	Validation workshop conducted; to present the report with stakeholders feedback; revised curriculum and competency standards submitted.	Workshop report accepted; revisions address agreed changes; version-controlled package delivered.	8 weeks from signing the contract
D2. b. Final Validation to Validate the Final curriculum & Submission Revised Curriculum and submission Accreditation Dossier	Final half day validation workshop to present a revised curriculum with competency standards with proposed changes with implementation-readiness note (2–3 pages)..	Curriculum, Accreditation dossier with the competency standards finalised and submitted to RTB; implementation note actionable.	10 weeks from the signing the contract.

IV. Reporting arrangements

The consultant reports to the ILO Project Manager, However, all technical deliverables are expected to be cleared by RTB and NCSA technical leads, who the consultant will be working closely with. All deliverables shall be submitted in English. Templates and forms required by RTB will be used where applicable.

V. Detailed qualifications, experience and skills required

A. Relevant Technical Expertise & Experience (maximum 40 points)

- Master's degree in Computer Science, Information Security, IoT, DataScience, ICT Education or a related STEM field.
- Completion certificates of Similar work in software development or Information technologies
- Proven professional experience in networking, software development, internet security/cybersecurity and hands-on lab design.
- Demonstrated experience in curriculum design/revision aligned to national qualification frameworks (preferably RTQF) and accreditation processes.
- Track record of collaboration with national institutions, notably NCSA and RTB, on programme development and accreditation.

B. Pedagogical & Training Skills (maximum 15 points)

- Ability to translate cybersecurity concepts into modular training packages with lab-based exercises, simulations and CTF challenges.
- Experience developing CBET-aligned assessment and moderation tools and inclusive approaches (gender equality, accessibility).

C. Proposed Approach & Workplan (maximum 30 points)

- Understanding of scope, realistic methodology, and risk/quality assurance plan tailored to Rwanda's skills ecosystem.

D. Quality of Sample Report (maximum 15 points)

- Analytical depth, clarity and utility demonstrated through submitted samples.

VI. Indicators for evaluation of outputs

Interested consultants must submit an Expression of Interest (EOI) including the following:

a) Cover Letter (maximum 2 pages)

- ▶ Brief statement on motivation and suitability for the consultancy.
- ▶ Overview of experience in cybersecurity skills integration, curriculum development.
- ▶ Availability for the proposed duration (December–March 2026).

b) Technical Proposal (maximum 5 pages)

- ▶ Understanding of the assignment objectives, scope, and expected deliverables.
- ▶ Proposed approach and methodology to achieve:
 - Finalization and validation of the cybersecurity curriculum and competency standards (in reference to the original NCSA programme).
 - Development of modular training tools, materials, and assessment frameworks aligned with RTQF Level 3 and RTB QA policies.

- ▶ Stakeholder consultation and validation process with NCSA, RTB, employers, and workers' representatives.
- ▶ Draft timeline and work plan by project phase (aligned with the indicative timeline above).
- ▶ Risk mitigation and quality assurance strategy to ensure accreditation, inclusivity, and sustainability of the programme.

c) Curriculum Vitae (CV)

- ▶ Experience in curriculum development, digital skills training (cybersecurity an advantage).
- ▶ Roles in similar assignments, with country, client, duration, and responsibilities.
- ▶ Relevant academic qualifications, professional certifications, and language skills.
- ▶ Contact details for at least two professional references.

d) Financial Proposal

***Deliverable Activity Cost = Daily Professional Fees X Total Activity Deliverable Days**

Complete the table below. "Up to" days and travel are indicative; only accepted deliverables and approved travel are payable.

e) Annexes / Supporting Documents

- ▶ At least **two examples of previous work** (e.g., revised curricula, training modules, reports).
- ▶ **Two references** (with contact information and description of working relationship).

f) Submission Instructions

- All applicant apply thorough: UNGM link: [ILO External Collaboration: Supporting the Development and Accreditation of a Cybersecurity Curriculum for TVET in Rwanda](#). By 17November 2025
- Any request for **clarification** will be sent via Jagger (refer to section X on how to Request one) by 12 November 2025
- **NB: Please note that applicants who applied under the previous TOR will not be considered.**

The subject line should read:

" Supporting the Development of a Cybersecurity Curriculum for TVET in Rwanda."

Deadline for submission: **17/November/2025, 23:59 CET**

Note to Consultants

- All CVs submitted should include the Date of Birth and Nationality of the Consultant;
- Consultant should quote in USD prices and/or using prices calculated using the Official UN Exchange Rates for the country;
- Candidates should be prepared to submit a copy of their national Passport upon Notification of Award;
- Consultants should be aware that all intellectual property rights arising from the contract are vested with the ILO however authorship will be acknowledged by the Organization;
- Consultants will bear all charges levied by their own bank in receiving of managing funds transferred by ILO.
- Consultant is responsible for their own taxes and banking charges.
- All submissions must be in English and in PDF format (editable annexes may be requested).

VII. Payment terms

- Payment of professional fees will be made in two instalments:
 - **1st payment – 38%** upon completion and validation of **Deliverable 1.1**
 - **2nd payment – 23%** upon completion and validation of **Deliverable 1.2**
 - **3rd payment – 27%** upon completion and validation of **Deliverable 1.3**
 - **4th payment – 8%** upon completion and validation of **Deliverable 2.a**
 - **5th payment – 4%** upon completion and validation of **Deliverable 2.b**

VIII. How to Apply

- Register on UNGM as an Individual Consultant by creating an account with your personal details and activating it via email.
- Complete the Basic Registration Form with your ID, address, areas of expertise (using UNSPSC codes), and eligibility declaration.
- Search for consultancy opportunities under the “Procurement Opportunities” section, filtering for calls for Individual Consultants. Or use this link to see the TOR: [ILO External Collaboration: Supporting the Development and Accreditation of a Cybersecurity Curriculum for TVET in Rwanda.](#)
- Apply by following instructions in each notice—either online through UNGM or via email, depending on the UN agency’s requirements.

IX. How to Request Clarification

- Register on UNGM as an Individual Consultant by creating an account with your personal details and activating it via email. :[UNGM individual consultant registration](#)
- Complete the Basic Registration Form with your ID, address, areas of expertise (using UNSPSC codes), and eligibility declaration.
- Complete BESAFE training and save the certificate to be included in the application documents
- Search for consultancy opportunities under the “Procurement Opportunities” section, filtering for calls for Individual Consultants. Or use this link to see the TOR : [Call for External Collaborator :Conducting a Training of Trainers \(ToT\) for TVET Teacher in Cybersecurity in Rwanda](#)

Apply by following instructions in each notice—either online through UNGM or via email, depending on the UN agency’s requirements.

