



► ILO External Collaboration Contract Terms of Reference

Consultancy: Conducting a Training of Trainers (ToT) for TVET Teacher in Cybersecurity in Rwanda

The Boosting Decent Jobs and Enhancing Skills for the youth in Rwanda's digital economy Project

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) 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 modules of the Rwanda TVET Framework (RTF) 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 the identification (in partnership with RTB), preparation, and training of teachers through a comprehensive Training of Trainers (ToT) programme supported with inclusive manuals, lab-based resources, and industry partnerships. These actions will contribute to strengthening pathways from foundational digital skills to employment and to piloting Cybersecurity Centers of Excellence within selected TVET schools.

III. Detailed tasks

WP1 – Design & Preparation (1day)

- Align ToT scope with the finalized curriculum and RTB/NCSA quality assurance policies.
- Agree target group and selection criteria with RTB; support screening and finalization of teacher cohort.
- Conduct a rapid Training Needs Assessment (TNA) addressing baseline skills and lab readiness (hardware, connectivity, cyber-range options).
- Produce a ToT framework (agenda, learning outcomes, assessment blueprint) and teacher-facing materials (trainer manual, slides, lab guides, checklists) aligned with CBET and Universal Design for Learning (UDL).

WP2.1 – ToT Facilitation and Micro-Teaching (10 days)

- Deliver a hands-on ToT using a teach-the-teacher cycle (demonstrate → practice → micro-teach → feedback).
- Track attendance, engagement, and daily learning outcomes; maintain an issues log.

WP2.2 – Lab-Based Exercises and Curriculum Implementation (10 days)

- Run lab-based exercises across the curriculum (Cybersecurity Essentials; Blue Teaming – SOC & Threat Hunting; GRC; Data Protection & Privacy), including CTF challenges.
- Track attendance, engagement, and daily learning outcomes; maintain an issues log.

WP3 – Evaluation & Support (1day)

- Administer pre/post assessments; compile a trainer readiness matrix and micro-teaching rubric.
- Provide implementation-readiness support (mentor hours/clinic) and document lab deployment options (on-prem/open-source/cloud-range with offline fallbacks).
- Submit a final ToT report with sex/age-disaggregated results, lessons learned, and recommendations for pilot rollout.

IV. Expected deliverables

The consultancy will be carried out over approximately for 22 days across 4 month, starting in **Deceber 2025 and ending in April 2026**. Duty station is Kigali, Rwanda; travel to selected TVET schools within Rwanda may be required.

The assignment will be structured into the following phases:

1.1. Deliverables & Acceptance Criteria

Deliverable	Description	Acceptance Criteria	Due Date
D1. Inception Report	Workplan, selection criteria, TNA plan; alignment note with curriculum consultant	Complete, practical, endorsed by RTB/NCSA/ILO	30 December 2025
D2. ToT Package	Trainer manual, slides, lab guides, CTFs, assessment tools	Aligned with RTF L3 & RTB QA; accessible formatting (contrast, alt-text); lab steps reproducible; peer-reviewed	20 February 2026
D3. ToT Delivery	20-days ToT; attendance; pre/post tests; satisfaction survey	≥85% completion; average knowledge gain ≥20%; key issues addressed	Feb – March 2026
D4. Implementation Readiness Note and Final Report	Mentor log; lab setup guidance; SOPs, and Final report with consolidated outcomes; disaggregated metrics; recommendations	Implementation Readiness Note with Two–three lab deployment options with costs/risks; actionable SOPs and Final report Complete; actionable; accepted by ILO	15 April 2026

V. 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.

VI. Detailed qualifications, experience and skills required

A. Technical expertise (max 40 points)

- Master's in computer science, Information Security, ICT Education, or related STEM.
- Professional cybersecurity practice (SOC/threat hunting/GRC) and lab design experience.
- Experience working with national institutions (RTB, NCSA) on capacity development and QA.

B. Pedagogy & CBET (max 15 points)

- Proven ToT design/delivery for TVET.

- CBET assessment tools (formative/summative, logbooks, competency checklists); inclusive/UDL practice.

C. Approach & workplan (max 30 points)

- Rwanda skills landscape insight; realistic, risk-aware plan with QA and safeguarding.

D. Sample report quality (max 15 points)

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

Minimum technical pass mark: 70/100.

VII. Indicators for evaluation of outputs

The consultant will be selected based on the following criteria:

A. Relevant Technical Expertise and Experience (40 points)

- Academic background: Master's degree in Computer Science, Information Security, ICT Education, or a related STEM field.
- Proven professional experience in cybersecurity, data protection, and privacy, including familiarity with SOC operations, threat hunting, GRC, and hands-on cyber labs.
- Experience delivering Training of Trainers (ToT) programmes for TVET
- Strong track record of working with national institutions, particularly with the National Cyber Security Authority (NCSA) and the Rwanda TVET Board (RTB) on capacity development and quality assurance.

B. Pedagogical and training skills (maximum mark: 15)

- Experience designing and delivering Training of Trainers (ToT) programmes for TVET.
- Demonstrated ability to translate complex cybersecurity concepts into modular training packages, including lab-based exercises, cyber-ranges, simulation environments, and Capture-the-Flag challenges.
- Competence in developing assessment tools (formative and summative tests, logbooks, competency checklists) aligned with competency-based education and training (CBET) principles.
- Proven capacity to integrate inclusivity, gender equality, and accessibility for learners with disabilities into both technical and pedagogical approaches.

C. Proposed approach to deliver the ToR's scope of work

- Applicant demonstrates (via submitted technical proposal) their expertise in the areas of skills development in Rwanda. The technical proposal includes a realistic workplan and technical assistance approach. The evaluation will assess the understanding of scope, objectives and completeness of response (maximum mark: 30).
- Quality of the sample report suggests that the applicant(s) possess the required level of knowledge and analytical skill (maximum mark: 15).

Application

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.
 - Delivery of Training of Trainers (ToT), including lab-based exercises, Capture-the-Flag (CTF) challenges, and industry engagement activities.
- ▶ 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), and ToT delivery.
- ▶ 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 : Only the Professional Daily Rate (in USD) and the estimated number of working days (22 days) will be applied. Please note that if travel is required for this assignment, the necessary travel costs will be covered separately by the ILO and should not be included in the professional daily rate.

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: [Call for External Collaborator :Conducting a Training of Trainers \(ToT\) for TVET Teacher in Cybersecurity in Rwanda](#) . By 17 November 2025
- Any request for **clarification** will be sent via UNGM (refer to section XI on how to Request one) by 12 November 2025
-

The subject line should read:

“Technical and Financial Proposals – Consultancy – Cybersecurity Curriculum Development and Training of Trainers (ToT) – Rwanda”

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

Only shortlisted applicants will be contacted. Incomplete or late applications will not be considered. Interviews may be held with shortlisted organizations.

► 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).

VIII. Payment terms

Payment of professional fees will be made in two instalments:

- **1st payment – 5%** upon completion and validation of **WP1 – Design & Preparation** (1 day)
 - **2nd payment – 45%** upon completion and validation of **WP2.1 – ToT Facilitation and Micro-Teaching** (10 days)
 - **3rd payment – 45%** upon completion and validation of **WP2.2 – Lab-Based Exercises and Curriculum Implementation** (10 days)
 - **4th payment – 5%** upon completion and validation of **WP3 – Evaluation & Support** (1 day)
- 100% of DSA** will be paid once all relevant receipts are submitted (5 days of travel to be budgeted for).

All reimbursable costs must reflect the Government practice 's commitment.

IX. Travel arrangements (if applicable)

Travel cost will be required for this assignment and the necessary travel costs will be covered by the ILO.

X. How to Apply

- 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.

XI. How to Request Clarification

- Log in to JAGGAER using the link from the notice or email.
- Open the relevant tender or event.
- Go to the Q&A or Messages section.
- Click "Ask a Question" or similar.
- Write your question clearly, referencing the specific section or requirement.

- Submit before the clarification deadline.
- Check back regularly for responses.

