Co-funded by
the European Union

Implemented by

Future Minds Lab Initiative

TERMS OF REFERENCE 81-17-25-1
Repeated Call

Title: External Trainer – Vocational Training in Cybersecurity: Governance, Strategy and Advanced Topics
Location: Bosnia and Herzegovina
Level of Effort: 5 training days, 5 days of mentoring (spanning across 6 month-period) and 2 preparation days
Reporting to: Project Manager, Future Minds Lab Initiative
Type of Contract: Short-term Individual Contract

1. Background

Bosnia and Herzegovina faces a persistent shortage of skilled professionals in the field of cybersecurity and digital technologies. According to international assessments such as the OECD and UNICEF, the country suffers from limited access to digital infrastructure, low levels of digital literacy, and a mismatch between education outputs and labour market needs. This digital gap is particularly evident among youth aged 19 – 29, who often lack opportunities for structured, market-relevant training that leads directly to employment in high-demand digital sectors.

At the same time, the cybersecurity threat landscape is rapidly expanding, with businesses and public institutions increasingly exposed to risks ranging from data breaches and ransomware to advanced persistent threats. Yet, the availability of trained cybersecurity professionals in Bosnia and Herzegovina remains critically low. This skills gap not only affects the security of local enterprises but also undermines the country's overall competitiveness and resilience in the digital economy.

The Future Minds Lab (FML) Initiative, implemented by the University Sarajevo School of Science and Technology (SSST) under the SEDEP program and supported by GIZ, was established to address these challenges. The Project operates across three strategic objectives:

- Enhancing industry innovation through stronger cooperation between innovators and businesses.
- Improving the enabling environment for innovation through expert advice, targeted training, and technical assistance.
- Increasing the supply of skilled entrepreneurs and digital workers through vocational training and education.

Within this third objective, the Project supports the creation of a 6-month vocational training program designed to provide market-relevant IT skills to young people. The training focuses on three high-demand tracks: Game Design, Cybersecurity, and Cloud Computing, all identified as critical for the domestic and regional labour markets.

This Call for Proposals relates to the Cybersecurity: Governance, Strategy and Advanced Topics component, designed to train participants in risk management, incident response plans, legal and regulatory compliance, as well as emerging trends such as artificial intelligence in security, Zero Trust architecture, and cloud security. Delivered through a combination of training days, mentoring sessions, and practical simulations, this module equips participants with knowledge and skills relevant to cybersecurity governance, compliance, and strategy.

2. Objective

To engage a qualified external trainer to deliver practical training modules on cybersecurity governance, strategy, and advanced topics, with the goal of introducing participants to key concepts of policy development, risk management, and incident response in line with best practices and regulatory frameworks

3. Key responsibilities

- Develop a detailed training curriculum and materials (presentations, labs, exercises) covering:
  - Risk management frameworks, secure coding practices, security policies, and incident response
  - Red vs. Blue team exercise (simulated attack/defense scenario)
  - Legal, ethical, and regulatory issues in cybersecurity
  - Emerging topics: AI in security, Zero Trust, and cloud security.
- Deliver in-person training sessions.
- Guide participants through case studies, tabletop exercises, and team-based simulations**.**
- Provide mentoring sessions to support participants in completing assignments and understanding real-world application.
- Adapt teaching to varying skill levels of participants.
- Participate in progress monitoring meetings with the Project Team.
- Submit a final report (max. 3 pages) summarizing the curriculum, content delivered, participant progress, and recommendations.

4. Deliverables

- **Training Curriculum – Structured curriculum with learning outcomes /2 days of preparation/** (First payment: 20%)
- **Module Delivery – Facilitation of 5 one-day modules + 5 days of mentoring, total 10 days/** (Second payment: 50%)
- **Final Report – Summary of training delivered and recommendations** (Third payment: 30%)

5. Timeline for delivery

Deliverable	Due Date
Preparation of Training Curriculum and materials	September 2025
Module Delivery	October 2025 - March, 2026
Final Report Submission	March 31, 2026

6. Qualifications

- Minimum 3 years of professional experience in cybersecurity governance, risk management, compliance, or related domains.
- Strong knowledge of incident response planning, security policies, and regulatory frameworks.
- Familiarity with emerging topics such as AI in security, Zero Trust, and cloud security.
- Ability to work with youth with mixed skill levels
- Excellent communication and presentation skills.
- Fluency in the local language; working proficiency in English.

7. Application requirements

Applicants must submit:

- CV detailing relevant experience
- Short motivation letter
- Short outline of proposed training approach (one page) including methodology, structure, tools to be used and learning outcomes
- Financial offer (daily fee rate).

8. Selection criteria

Criterion	Weight
Professional experience in cybersecurity governance, risk management and compliance or related domains	40%
Quality of proposed training approach	20%
Relevance to target group (youth, entry-level)	20%
Financial offer	20%

9. Language of the Assignment

Training will be conducted in the local language, while the final report must be submitted in English.

10. Submission Deadline

All interested candidates are to submit their bids with all supporting documents no later than September 15, 2025, 23:59. All bids are to be submitted electronically to the following email address:

info@ssst.edu.ba, with the subject line: *81-17-25-1 FML External Trainer – Cybersecurity: Governance, Strategy and Advanced topics. Repeated Call.* Any inquiries regarding the opportunity may be directed to the same address and subject line.

Co-funded by the European Union

Implemented by giz

Financial Proposal Form – 81-17-25-1

Name of Bidder:	[Insert Name of Bidder]	Date:	Select date

Bidders are required to prepare their financial proposals following the below format and submit it with the technical offer. Any financial information provided in the technical proposal shall lead to the Bidder's disqualification.

The Financial Proposal should align with the requirements in the Terms of Reference and the Bidder's Technical Proposal.

Currency of the proposal: BAM

Table 1: Summary of Overall Prices

	Amount(s)
Professional Fees (from Table 2)	
Other Costs (from Table 3)	
Total Amount of Financial Proposal	

Table 2: Breakdown of Professional Fees

Name	**Position**	**Fee Rate** *A*	**No. of Days/months/ hours** *B*	**Total Amount** *C=A+B*
In-Country				
Home Based				
			Subtotal Professional Fees:	

Table 3: Breakdown of Other Costs

Description	**UOM**	**Quantity**	**Unit Price**	**Total Amount**
Local transportation costs	Lump Sum			
Out-of-Pocket Expenses				
Other Costs: (please specify)				
			Subtotal Other Costs:	

Table 4: Breakdown of Price per Deliverable/Activity

Deliverable/ Activity description	**Time** (person days)	**Professional Fees**	**Other Costs**	**Total**
Deliverable 1				
Deliverable 2				
Deliverable 3				
…..				

Signature of authorized person:

Co-funded by
the European Union

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Inicijativa Future Minds Lab

PROJEKTNI ZADATAK 81-17-25-1
Ponovljeni poziv

Naziv pozicije: Spoljni trener – stručno osposobljavanje iz cyber sigurnosti: upravljanje, strategija i savremene teme
Lokacija: Bosna i Hercegovina
Angažman: 5 dana obuke, 5 dana mentorisanja (u periodu od 6 mjeseci) i 2 dana pripreme
Izvještavanje: Projektni menadžer, Inicijativa Future Minds Lab
Vrsta ugovora: Kratkoročni angažman pojedinačnog spoljnjeg trenera

1. Kontekst

Bosna i Hercegovina se suočava s kontinuiranim nedostatkom kvalifikovanih stručnjaka u oblasti cyber sigurnosti i digitalnih tehnologija. Prema međunarodnim procjenama (OECD, UNICEF), zemlja ima ograničen pristup digitalnoj infrastrukturi, nizak nivo digitalne pismenosti i izražen nesklad između obrazovnih programa i potreba tržišta rada. Ovaj digitalni jaz posebno pogađa mlade osobe od 19 do 29 godina, koje često nemaju priliku za strukturirane, tržišno relevantne obuke koje direktno vode do zaposlenja u sektorima s visokom potražnjom.

Istovremeno, prijetnje u oblasti cyber sigurnosti ubrzano rastu – od krađa podataka i ransomware napada do sofisticiranih trajnih prijetnji. Ipak, broj obučenih stručnjaka za cyber sigurnost u Bosni i Hercegovini ostaje kritično nizak. Ovaj nedostatak kadra ne utiče samo na sigurnost domaćih kompanija, već i na ukupnu konkurentnost i otpornost zemlje u digitalnoj ekonomiji.

Future Minds Lab (FML) Inicijativa, koju implementira Univerzitet Sarajevo School of Science and Technology (SSST) u okviru SEDEP programa i uz podršku GIZ-a, osnovana je kako bi se odgovorilo na ove izazove. Projekat djeluje kroz tri strateška cilja:

- jačanje inovacija u industriji kroz snažniju saradnju inovatora i poslovne zajednice,
- unapređenje okruženja za inovacije kroz ekspertske savjete, ciljane obuke i tehničku podršku,
- povećanje ponude mladih preduzetnika i digitalnih radnika kroz stručno osposobljavanje i obrazovanje.

U okviru trećeg cilja, Projekat razvija 6-mjesečni program stručnog osposobljavanja s ciljem da mladima pruži tržišno relevantne IT vještine. Program se fokusira na tri oblasti visoke potražnje: Game Design, Cybersecurity i Cloud Computing, prepoznate kao ključne za domaće i regionalno tržište rada.

Ovaj poziv se odnosi na komponentu Cybersecurity: Upravljanje, strategija i napredne teme, osmišljenu da obuči polaznike u upravljanju rizicima, planovima odgovora na incidente, pravnoj i regulatornoj usklađenosti, kao i u novim trendovima poput vještačke inteligencije u sigurnosti, Zero Trust arhitekture i could sigurnosti. Modul se realizuje kroz kombinaciju obuke, mentorskih sesija i praktičnih simulacija, te pruža polaznicima znanja i vještine relevantne za upravljanje, usklađenost i strategiju u oblasti cyber sigurnosti.

2. Cilj angažmana

Angažovati kvalifikovanog vanjskog trenera za realizaciju obuke iz oblasti upravljanja cyber sigurnošću, strategije i naprednih tema, s ciljem upoznavanja polaznika s ključnim konceptima razvoja politika, upravljanja rizicima i odgovora na incidente u skladu s najboljim praksama i regulatornim okvirima.

3. Ključne odgovornosti

- Razviti detaljan kurikulum obuke i materijale (prezentacije, laboratorijske vježbe, zadatke) pokrivajući:
  - okvire za upravljanje rizicima, prakse sigurnog kodiranja, sigurnosne politike i odgovor na incidente,
  - Red vs. Blue timsku vježbu (simulirani scenarij napada/odbrane),
  - pravna, etička i regulatorna pitanja u cyber sigurnosti,
  - napredne teme: AI u sigurnosti, Zero Trust i cloud sigurnost.
- Izvoditi obuku uživo.
- Voditi polaznike kroz studije slučaja, tabletop vježbe i timske simulacije.
- Mentorisati i pružiti podršku polaznicima u izvršavanju zadataka i razumijevanju praktične primjene.
- Prilagoditi podučavanje različitim nivoima znanja polaznika.
- Učestvovati u sastancima za praćenje napretka s projektnim timom.
- Dostaviti završni izvještaj (max 3 stranice) sa sažetkom sadržaja i kurikuluma, napretka polaznika i preporukama.

4. Rezultati angažmana (Deliverables)

- **Kurikulum obuke – strukturiran plan obuke sa definisanim ishodima učenja /2 dana pripreme/** (prva uplata – 20%)
- **Realizacija modula – 5 jednodnevnih modula i 5 dana mentorisanja /ukupno 10 dana/** (druga uplata – 50%)
- **Završni izvještaj – sažetak obuke i preporuke** (treća uplata – 30%)

5. Vremenski okvir isporuke

Rezultati angažmana	Rok za isporuku
Priprema kurikuluma i materijala	septembar 2025.
Realizacija obuke	oktobar 2025. – mart 2026.
Predaja završnog izvještaja	31. mart 2026.

6. Kvalifikacije

- Minimalno 3 godine profesionalnog iskustva u upravljanju cyber sigurnošću, upravljanju rizicima, usklađenosti ili srodnim oblastima.
- Odlično poznavanje planiranja odgovora na incidente, sigurnosnih politika i regulatornih okvira.

- Poznavanje savremenih tema poput umjetne inteligencije u sigurnosti, Zero trust i cloud sigurnosti.
- Prilagoditi način rada različitim nivoima znanja polaznika.
- Odlične komunikacijske i prezentacijske vještine.
- Tečno poznavanje lokalnog jezika; sposobnost korištenja engleskog jezika u profesionalnom kontekstu.

7. Potrebna dokumentacija za prijavu

- CV sa relevantnim iskustvom
- Kratko motivaciono pismo
- Kratki pregled predloženog pristupa obuci (jedna stranica) uključujući metodologiju, strukturu, alate koji će se koristiti i ishode učenja
- Finansijska ponuda (cijena po danu).

8. Kriteriji za odabir

Kriterij	Težina
Profesionalno iskustvo u upravljanju cyber sigurnošću, upravljanju rizicima i usklađenosti, ili srodnim oblastima	40%
Kvalitet predloženog pristupa obuci	20%
Relevantnost za ciljnu grupu (mladi, početnici)	20%
Finansijska ponuda	20%

9. Jezik angažmana

Obuka će se izvoditi na lokalnom jeziku, dok se završni izvještaj predaje na engleskom.

10. Rok za prijavu

Svi zainteresirani kandidati dužni su poslati svoje prijave sa pratećom dokumentacijom najkasnije do **15. septembra 2025. godine do 23:59 sati.** Prijave se dostavljaju isključivo elektronskim putem na slijedeću e-mail adresu: *info@ssst.edu.ba*, uz napomenu u predmetu e-maila: *81-17-25-1 FML External Trainer – Cybersecurity: Governance, Strategy and Advanced Topics. Ponovljeni poziv.* Pitanja i pojašnjenja u vezi sa pozivom mogu se poslati na istu adresu i uz isti predmet emaila.

Co-funded by the European Union

Implemented by giz

Forma finansijske ponude – 81-17-25-1

Ime ponuđača	[ime ponuđača]	Datum:	Odaberi datum

Ponuđači su obavezni pripremiti svoje finansijske prijedloge prema dole navedenom formatu i dostaviti ih zajedno sa tehničkom ponudom. Svaka finansijska informacija koja bude pružena u tehničkoj ponudi rezultirat će diskvalifikacijom ponuđača.

Finansijski prijedlog treba biti usklađen sa zahtjevima iz Projektnog zadatka i tehničkom ponudom ponuđača.

Valuta ponude: KM

Tabela 1: Sažetak ukupnih cijena

	Iznos(i)
Profesionalne naknade (iz Tabele 2)	
Ostali troškovi (iz Tabele 3)	
Ukupni iznos finansijskog prijedloga	

Tabela 2: Raspodjela profesionalnih naknada

Ime	**Pozicija**	**Tarifa** *A*	**Broja dana/mjeseci/sati** *B*	**Ukupni iznos** *C=A+B*
U zemlji				
Kod kuće				
			Podzbir profesionalnih naknada:	

Tabela 3: Raspodjela drugih troškova

Opis	**Mjera jedinice**	**Količina**	**Jedinična cijena**	**Ukupni iznos**
Troškovi lokalnog transporta	Paušalni iznos			
Troškovi "iz džepa"				
Ostali troškovi: (molimo navedite)				
			Podzbir drugih troškova:	

Tabela 4: Raspodjela cijene po isporuci/aktivnosti

Isporuka/Opis aktivnosti	**Vrijeme** (osoba/dani)	**Profesionalne naknade**	**Ostali troškovi**	**Ukupno**
Isporuka 1				
Isporuka 2				
Isporuka 3				
…..				

Potpis ovlaštene osobe: