



Open Call for Consultancy Services

Reference Number: 025-026

Type and period of engagement: Service Contract until 31 December 2026

Location: Sarajevo, Bosnia and Herzegovina

Deadline: 26 March 2026

Terms of Reference for Cybersecurity Expert

The Integrative Internal Security Governance (IISG) process was initiated as part of the European Union's (EU) strategic efforts to enhance cooperation with the Western Balkans region in the field of security. The concept enables coordinated, aligned, and sustainable engagement across key areas of internal security governance reform by the EU and relevant international donors providing external assistance. The process has progressively evolved and has been endorsed at the level of the Justice and Home Affairs Council through the adoption of Council Conclusions. The IISG was endorsed by the Council of the European Union in late 2016 and officially launched by the Ministers of Interior/Security of the Western Balkans Six (WB6) in September 2017 during the IISG Kick-Off Conference – Brdo Process Ministerial Meeting held in Brdo pri Kranju, Slovenia.

The Regional Cooperation Council (RCC) was established in 2008 as a regionally owned and led cooperation framework. It operates under the political guidance of the South-East European Cooperation Process (SEECP) and aims to promote regional cooperation and support European and Euro-Atlantic integration of South East Europe (SEE). The RCC comprises 45 participants and receives operational guidance and oversight from the RCC Board, composed of RCC participants contributing to the budget of the RCC Secretariat.

The RCC Secretariat is headquartered in Sarajevo, Bosnia and Herzegovina, and is headed by the Secretary General. The RCC also maintains a Liaison Office in Brussels, ensuring regular communication and cooperation with European and Euro-Atlantic institutions.

The RCC serves as the political umbrella and regional implementing mechanism for the IISG, which is fully funded by the European Union. The core objective of the IISG is to strengthen regional security through enhanced coordination and cooperation among WB6 partners. In addition to its political umbrella role, the RCC is increasingly assuming a more integrated and operational leadership function in regional security coordination.

Following the adoption of the latest Terms of Reference (ToR) by the IISG Board in December 2025, the platform has evolved into the **Security Governance Hub for the Western Balkans**,





with the objective of strengthening strategic regional cooperation and coordination in the field of internal security.

The main areas of focus include counter-terrorism and preventing and countering violent extremism (P/CVE), combating organised crime, border/boundary security, and cybersecurity. These thematic pillars have been integrated into the operations of the Security Governance Hub through structured needs mapping and the development of a comprehensive project database, supporting evidence-based strategic planning across all pillars.

Outline of the Position

The Cybersecurity Expert will work under the framework of **IISG**, operating within the structures of the **Regional Cooperation Council** and supporting regional cybersecurity coordination among Western Balkans partners.

Specifically, the incumbent will support the implementation, coordination, analysis, and visibility of activities under the Cybersecurity Pillar, including support to the Cybersecurity Database, stakeholder coordination, and preparation of analytical and reporting products.

Reporting

The incumbent will report to the Database Coordinator and RCC Senior Expert on Security.

Duties and Responsibilities

- Provides support to the Cybersecurity Database Coordinator / Analyst, specifically in relation to the Cybersecurity Pillar and the Cybersecurity Database.
- Supports the IISG Secretariat in communication with target groups and PR outreach on matters related to cybersecurity activities, including the visibility of events, initiatives, and key deliverables. The role entails regular interaction with WB Partners' cybersecurity institutions (including CERTs/CSIRTs, line ministries, and law enforcement where relevant) as well as other stakeholders active in cyber capacity-building and internal RCC/IISG structures to ensure coherence across IISG pillars and reporting processes.
- Liaise with the Cybersecurity Working Group, including designated contact points from WB Partners and relevant stakeholders, to support coordination, information exchange, and follow-up on agreed actions.
- Responsible for preparing statistical information and reports on gaps and possible overlaps in the ongoing projects. This includes coordinating the work processes, needs and response



mapping in order to deliver the mapping products as well as reporting on activities related to the pillars.

Key Outputs

The incumbent will contribute to and coordinate the following key outputs:

- Bridge and coordinate the operational cybersecurity activities between RCC and IISG Secretariat;
- Prepare statistical information, reports on gaps and possible overlaps in the ongoing projects;
- Coordinate cybersecurity pillar activities under the guidance of Cybersecurity Database Coordinator / Analyst;
- Support the IISG Secretariat in communication with target groups and PR outreach on matters related to cybersecurity activities, including the visibility of events, initiatives, and key deliverables.

Job Knowledge and Technical Expertise

The incumbent is expected to demonstrate:

- Sound knowledge of the relevant professional field;
- Understanding and application of organisational policies and procedures;
- Ability to analyse requirements and formulate proposals;
- Commitment to continuous professional development;
- Strong information technology skills relevant to the position;
- Ability to monitor implementation of action plans and prepare progress reports for stakeholder review.

Key Requirements

- Advanced university degree (Master's degree or equivalent) in ICT or a related field;
- Minimum experience of five years in cyber capacity-building, cyber policy, CERT/CSIRT environments, or cyber-related project coordination;
- Strong analytical skills, including experience in collecting and analysing quantitative and qualitative data;
- In-depth knowledge of the Western Balkans region and experience in regional cooperation, EU enlargement, and related policy fields;
- Experience in regional cooperation in SEE and in managing EU-funded projects;





- Experience supporting intergovernmental processes and policy development;
- Excellent command of written and spoken English.

Location

The service provider will work in a hybrid mode in cooperation with the Head of IISG Secretariat. The service provider could expect that some time would be spent on business-related travel.

Application Rules

Qualified candidates are invited to send their motivation letter, CV highlighting relevant experience and three references until **26 March 2026**. Only shortlisted candidates will be contacted. Selection process is based on a written test and a competency-based interview.

The applications should be submitted through the website link [Apply now](#).

Disclaimer: We are dedicated to ensuring a working environment that guarantees freedom, cooperation, inclusion, acceptance of diversity, and equal opportunities for others. We select partners we cooperate with solely on the basis of competence and integrity of the candidate, making a decision based on relevant documentation and an interview. We ensure the performance of work tasks and advancement on the principles of equality by prohibiting any form of discrimination based on race, religion, gender, sexual orientation, gender identity or expression, age, disability, marital status or national origin. We operate with zero tolerance towards mobbing, harassment and sexual harassment in the workplace and demand the same of all employees and business partners. We strongly encourage women, minorities, and vulnerable groups to apply.