**Cyber Range Technical Requirements**

Norway for You - Serbia Project

**Table of Contents**

[**1 Background**](#_30j0zll) **3**

[**2 Introduction**](#_s9udri9revi) **3**

[**3 General requirements, extendibility and licensing**](#_qv0e6evto826) **4**

[3.1 General requirements](#_wa65wlw0mi53) 4

[3.2 Extendibility](#_3ydbv7s6fjxw) 4

[3.3 Licensing](#_idkfyzdbjleh) 4

[3.4 Training infrastructure](#_2et92p0) 5

[**4 CEP management environment**](#_tyjcwt) **6**

[4.1 Management interface](#_3dy6vkm) 6

[4.2 Trainee interface](#_1t3h5sf) 7

[**5 Hardware and Software**](#_twhhlme2zsmn) **7**

[**6 Delivery and Maintenance**](#_2s8eyo1) **8**

[**7 Supplier and Vendor Requirements**](#_2xcytpi) **9**

[7.1 References](#_1ci93xb) 9

[7.2 Project team](#_3whwml4) 9

[7.3 Standard certificates](#_2bn6wsx) 10

[7.4 Quality evaluation](#_qsh70q) 10

[7.5 Testing and quality assurance](#_679bemc0r8nx) 10

[7.6 Project Plan](#_9g2y2xigpqn6) 10

[**APPENDIX I: Evaluation criteria**](#_1i73uvvesqmn) **10**

[Supplier and vendor references](#_6f6yhb1j34qr) 10

[Project team](#_36u8yj5r406e) 11

[Technical requirements](#_2xmxyr6q7nlm) 12

# 1 Background

The Norwegian Support to the Western Balkans Development “Norway for You – Serbia” is a project financed by the Government of the Kingdom of Norway and implemented by the United Nations Office for Project Services (UNOPS).

The overall objective of the Project is to contribute to a more balanced socio-economic development in Serbia by increasing employment opportunities, supporting social cohesion and improving local infrastructure in the less developed areas. Special focus will be given to inclusion of youth, women and vulnerable groups in the labour market. Also, the Project will strengthen information security of the Government of Serbia and support the process of European Union (EU) integration.

The Project is designed to be implemented on the territory of underdeveloped areas in Serbia, in total 91 local self-governments (LSG) classified in the third and fourth group of development.

There are five results that the Project will achieve:

* Result 1: Improved Access to Employment
* Result 2: Enhanced Social Inclusion
* Result 3: Improved Living Conditions and Local Infrastructure
* Result 4: Information Security of the Government of Serbia Strengthened
* Result 5: Process of EU Integration of the Republic of Serbia Supported

Key stakeholders and direct beneficiaries of the Project are 91 LSGs from the third and fourth group of development and their institutions and organisations, regional development agencies, civil society organisations (CSOs), business support entities (BSEs), as well as individual beneficiaries, especially women and youth. Final beneficiaries are the inhabitants of underdeveloped areas where the Project will be implemented, as well as line ministries of the Republic of Serbia (RS), such as the Ministry of European Integration, the Ministry of Trade, Tourism and Telecommunications, and the Regulatory Agency for Electronic Communications and Postal Services.

All Project activities will be undertaken in partnership with the Government of the RS, in cooperation with national and local institutions, with the aim of allowing them to respect legal requirements and, where relevant, the EU accession criteria. This will ensure national ownership and help develop national capacities. Activities will also have good governance, human rights, gender equality, environment and climate and anti-corruption as transversal themes, the application of which in local policies and regulations will increase social cohesion.

# 2 Introduction

The importance of enhancing resilience in the area of cyber security is recognised as one of the EU Cyber Security Strategy[[1]](#footnote-0) main goals, as well as the goals in the Strategy for Development of Information Security in the Republic of Serbia 2017-2020[[2]](#footnote-1). In order to reach a certain level of cyber security resilience in Serbia, the Project team, together with the Regulatory Agency for Electronic Communications and Postal Services (RATEL) have identified the need to provide a platform for National Cyber Security Drills to contribute to the improvement of professional and technical capacities of relevant institutions, improve incident response management and provide training for the employees of relevant institutions. The Platform will be set up on the premises of the National CERT (RATEL), but the access and the drills will be by all CERTs, with the possibility of including different actors from the financial sector, private sector, etc. By providing a platform (hardware and software) for the Government of Serbia, regular drills can be organised as they are highly important in the area of cyber security.

The main purpose of this document is to define the mandatory requirements for a Cyber Exercise Platform (CEP). The CEP is a system which includes all the required hardware, software, licenses, scenarios and documentation to perform cyber exercises which reflect real-life cyber-attack and defense scenarios.

It is expected that the CEP will consist of the following components:

* Training environment
* Trainee interface
* Management environment
* Management interface

Apart from the above components, this document describes the general, extendability, licensing, as well as the hardware and software requirements.

# 3 General requirements, extendibility and licensing

All the requirements will be considered as mandatory and eliminatory. Each requirement must be verifiable and the evaluation process would include oral presentation of the offered solution. The bidder must provide live POC demonstration of each requirement if needed or optionally a Factory Acceptance Test at no additional costs.

## 3.1 General requirements

The CEP shall meet the following general requirements:

* The CEP deliverables must include all the necessary hardware, software, licenses, content and documentation required for its correct operation.
* It is required that the CEP can be deployed and operated locally in the data center of the Customer.
* The CEP must be a hybrid type, combining physical (Hardware) and virtual (Software) solutions.
* The CEP must allow the execution of real cyberattack training scenarios to provide trainees with the experience of different realistic scenarios. Each scenario must have at least three levels of difficulty.
* The CEP must simulate networks, traffic and attack scenarios, to train and test trainees, procedures and technologies in a safe and controllable environment.

## 3.2 Extendibility

The CEP shall meet the following extendibility requirements:

* The CEP must be extendable to simulate ICS/OT/SCADA attacks. The ICS/OT/SCADA extension must provide capability to perform SCADA/ICS systems exploitation techniques, using physical PLC SCADA systems, HMI and SCADA server and SCADA IDS (Intrusion Detection System). The expansion must include an out-of-the-box pool of IT & OT (SCADA/ICS) attack scenarios.
* The CEP must be extendable with a module which allows customization of the already supplied cyber-attack scenarios and creation of new custom cyber-attack scenarios.
* The CEP must be able to extend with additional concurrent team / class capacity as an ability of future extension of the platform.

## 3.3 Licensing

The CEP shall meet the following licensing requirements:

* The licensing of the CEP must be perpetual. i.e. once the period of contracted support ends, it will not be disabled in any of its functionalities.
* The license for the CEP must allow 1 (one) full environment: 1 (one) trainer and 1 (one) concurrent class/scenario supporting up to 10 parallel trainees as a part of one team, regardless of whether they are on-site or connected via VPN.
* The license for the CEP must allow at least 10 different out-of-the-box “blue team”-oriented scenarios. Scenarios must simulate complex real-world infrastructure and processes which include multiple machines and appliances. Exercises like cyber challenges within just one or two virtual elements (virtual machines) would not be considered as a scenario.
* The CEP must be shipped with a license for at least one class but has to be expandable to multiple classes.

## 3.4 Training infrastructure

The list of training environment requirements are the following:

* The platform’s training environment must be able to be isolated and must not require connectivity to the internet or to the organization’s operational network.
* The platform’s training environment must be easily reverted to the default "clean" state prior to a new training.
* The CEP must allow remote training, by connecting remote users to the CEP system via VPN. The CEP must be shipped with a VPN server to achieve this functionality in a secure way, without a need for additional external appliance/element.
* The CEP must provide simulations of multiple automatic and repeatable cyber-attack scenarios.
* The CEP must provide virtualization and emulation of network devices and protocols including security components, network appliances, servers and applications, user computer end-points.
* The CEP must support running multiple, independent classes simultaneously using a single architecture, by a single trainer. In case of future expansion, with additional simultaneous classes it will be supported using the same interface.
* The CEP must simulate real life ICT environments, which include over 30 components (FW, Servers, endpoints, SIEM ets.)
* The CEP must include multiple segments of IP subnets, VLANs and DMZ to represent a real operation organization network.
* The CEP must include a traffic generator running various traffic, at least IP, HTTP, HTTPS, SSH, SMTP, FTP and ICMP. The traffic generator shall be configurable to allow at least: source and destination of generated traffic, traffic type, protocol and duration of the generated traffic.
* The CEP must include options for the attack machine (i.e. the workstation or other CEP infrastructure element which initiates a cyberattack) to run attack flows into the network, from various network segments, according to the scenario configuration (external: simulates an external threat and internal: simulates user misuse or a malicious user).
* The CEP must include a simulation machine to run predefined attack scenarios without the need for human resources for running the attacks, i.e. without a need for a human "red team".
* The CEP must provide multiple attack vectors, at least: Web, Mail, FTP.
* The CEP must provide multiple exploits scenarios, at least information theft, web crawling, SQL injection, port scanning, ping sweep, password brute force, backdoor scripting, website spoofing, spear phishing, DNS Poisoning.
* The CEP must provide attack scenarios with high tangible effect on the network as: stop domain services (DOS), information theft, deface website.
* The CEP must provide attack scenarios which involve exercises with Linux logs, Windows PC and server logs. SIEM logs, firewall logs, mail relay logs, reverse engineering and web and networking forensics, MSSQL server logs.
* The CEP must have an optional module which should allow customization of the training network and/or creation of a new training network. This module is only required as an option for extension of the CEP. The module should have a designer user interface to set the network properties of IP, networking, system and operating systems settings.
* The system must have an optional working module of extension of a catalog of pre-scripted, "out of the box", Pen-Testing\Red scenarios. The scenarios should include a network and a "Flag" the trainees have to access/obtain during the training.

# 4 CEP management environment

The management environment of the CEP shall have the following functionalities:

* The CEP must have a control interface to monitor the simulated network (service activity time).
* The CEP must support user-friendly training session setup, e.g. - assignment of trainees, networks and scenarios.
* The CEP must provide an option to score the class performance at each milestone of each scenario.
* The CEP must provide an option to store and run previous scenario recordings.
* The CEP must provide a view of the complete training history.
* The CEP must provide an option to edit goals and steps of existing scenarios.
* The CEP must provide a time line bar monitoring of the scenario progress and the attack milestones through a trainer management interface system console.
* The CEP must provide monitoring of SIEM events in the time line through a trainer management interface system console.
* The CEP must provide a summary of all training events on the timeline through a trainer management interface system console.
* The CEP must provide an option to add text comments by the trainer via the training interface and marked on the timeline of the activity during the training.
* The CEP must provide a debriefing mode - running the training captured video of trainees workstations and the option to navigate in the video to points of interest.
* The network shall include "detectors" which detect student activity and send feedback to the trainer application.
* The CEP must allow storage and analysis of all practices and exercises performed by instructors and trainees in video format. The CEP shall have the capacity to store practices and exercises, at least 20 training sessions with 10 students, 5 hours per session.

## 4.1 Management interface

The management interface of the CEP will have the following functionalities:

* The CEP must provide a trainer management interface with an ability to detach a window for each trainee view with the option to enlarge to full screen.
* The CEP must provide a trainer management interface with an option to view the timeline progress as absolute or relative during a training.
* The CEP must provide a trainer management interface which allows the trainer to jump from point to point on the timeline in debrief mode and the recordings will sync accordingly.
* The CEP must provide a trainer management interface with an evaluation module interface to evaluate and add comments to each trainee.
* The CEP must provide a full video capturing of the trainee workstations where the instructor can view all screens simultaneously and open a specific trainee screen in full screen mode.

## 4.2 Trainee interface

The trainee interface of the CEP shall have the following functionalities:

* The CEP must provide for the trainees via the training interface the following: tools of control, detection and investigation as: SIEM, Firewall, station logs, server logs, Putty and Wireshark, which the trainees will use for security analysis.
* The CEP must provide trainee interface with a console showing network information, IP addresses, access credentials so trainees can access and diagnose each network asset.
* The CEP must provide a trainee interface with a console showing the lesson time progress and score.
* The CEP must provide a trainee interface with access to the virtualization management which provides access to all machines in the network.
* The CEP must provide a trainee interface which allows RDP connections to all Windows machines in the network.
* The system must have a working module of automatic scoring mechanism (self evaluation), to automatically detect the students’ achievements.
* The trainee application must include an interactive collaboration tool for the students, where they can add their insights and evidence on the attack scenarios they are investigating.

# 5 Hardware and Software

The CEP shall consist of the following hardware and software components:

* The CEP must be delivered with all the necessary hardware for the software to be hosted, which includes: rack, storage, servers, ethernet switches, ethernet cables, power cables
  + Servers should be provided as enterprise-grade 19” rack mountable devices, with a suitable amount of CPU, memory and storage for the required purpose and with the required amount of storage to store practices and exercises, at least 20 training sessions with 10 students, 5 hours per session. The servers should have redundant power supplies and redundant disk storage.
  + Ethernet switches should be provided as enterprise-grade 19” rack mountable devices, with at least in total 48 1G interfaces and 4 10G interfaces with redundant power supplies.
* The CEP must be supplied with all the required software components which includes: Windows, Microsoft Office, SIEM, Firewall, COTS (commercial of-the-shelf) virtualization platform.
* The CEP must be delivered with 11 mobile workstations / laptops. The mobile workstations must have the following specification:
  + Laptop PC computer with at least quad core i5 processor
  + At least 8 GB RAM
  + At least 256 GB SSD disk
  + At least 15” size display
  + Supplied with external 24" LED monitor (minimum resolution 1920x1080) and all necessary cables
  + Supplied with external mouse and keyboard
  + Supplied with carrying case
  + Supplied with Windows 10 PRO OS
* The CEP must be delivered with an interactive display. The interactive display must have the following specification:
  + At least 65” LED display with at least 4K resolution
  + Touch-screen with at least 10 points touch
  + Whiteboard functionality
  + Supporting software for Windows OS for annotations
  + Input function with pen or finger
  + Built-in or external PC with Windows 10 OS
  + Built-in Android OS
  + A stand providing mobility of the display
* The CEP must include a fully operational and licensed COTS (commercial of-the-shelf) perimeter firewall and an internal firewall.
* The CEP must include an application to monitor network server and services status.
* The CEP must include a fully operational and licensed COTS (commercial of-the-shelf) SIEM, including a pre-configured rule set for each attack scenario in order to generate scenario-specific alerts.
* The CEP training infrastructure must include the following elements:
  + Mail relay server
  + Domain Controller server
  + DHCP server
  + Server segments including SQL, DC, DHCP, File server, etc.
  + Users segment including Workstation with Linux and Windows OS
  + Web segment including FTP application server, Apache-based web server and Microsoft Internet Information Services (IIS)-based web server
  + VPN segment (trainee stations connect to the training network via the VPN Server in this segment)
  + ISP segment to simulate Internet network which includes: Domain Name Services (DNS), IIS Web Server and WebMail
  + Custom segment so the Trainer can add additional tools and virtual machines to the network
* The CEP must include VLAN and IP segmentation of the various segments detailed (e.g. Users segment, SIEM segment, ISP, VPN, etc.) in order to maintain a network structure similar to real life.

# 6 Delivery and Maintenance

The CEP shall meet the following delivery and maintenance requirements:

* The CEP must be provided with the following types of documentation:
  + Operating manual – short description of system modules, detailed overview of system operation, including interdependencies, periodically being checked system functions; estimated average growth data storage required;
  + User guide – based on the processes supported by the system, i.e. a process -oriented user manual;
  + User manual – detailed system function descriptions based on the menus within the system;
  + White Team guide: scenario guide with specific and detailed instructions on how to solve each scenario.
* The CEP must be delivered in term of 90 days upon signing the contract and must be installed and fully implemented on-site (achieve all the defined functionalities) in a term of 30 days upon the delivery.
* The installation of the CEP will be confirmed by performing and signing the Site Acceptance Test (SAT).
* The CEP must be provided with a 3 years term of maintenance and support services with the following terms:
  + Vendor maintenance and support for software (including provided COTS software) which includes new software updates, workarounds in case of bugs and defects, access to vendor’s Technical Assistance Center (TAC)
  + Vendor maintenance and support for the provided hardware which includes replacement of any malfunctioning hardware system or subsystem
  + Supplier support and assistance which includes:
    - Assistance and first line support for all software and hardware issues/incidents
    - Deliver and perform incidental software updates, workarounds
    - Quarterly system checks and software updates (if updates are available)
    - Performing RMA (Return Material Authorization) activities in case of malfunctioning hardware system or subsystem
    - TAC support with at least 8x5x4 (8 hours of availability during working days with 4 hours response time) in case of critical issues/incidents
  + The beneficiary should not have any additional costs in maintenance and support activities (eg. shipping malfunctioning hardware and/or replacements, etc.)
  + The 3 years term of maintenance and support period starts from the day of the signed SAT.
* The delivery of the CEP must include two train-the-trainers courses with a duration of at least 5 days:
  + Training should be provided for ten (10) trainers selected by the Beneficiary.
  + The first training will be delivered by the Supplier or Vendor to ten (10) trainers prior or upon the SAT.
  + The second training will be delivered by the Supplier or Vendor to ten (10) trainers in a period of 6 months after the SAT.
  + The training must provide guidance through the system and CEP (scenarios). All this will be realised with detailed training by modules and functionalities corresponding to user roles.
  + Through the training, users should acquire the following skills: ability to use CEP for drills and training.
  + The users must understand the need and the way of using the support which will be provided by the Supplier.
  + The training must explain the way the CEP works, all options in the user menus/procedures must be thoroughly explained and trained.

# 7 Supplier and Vendor Requirements

## 7.1 References

* The supplier should have a local agent (vendo) engaged for maintenance/support. The vendor should be a registered ICT company present in the Republic of Serbia for at least three (3) consecutive years.
* The supplier’s reference for at least two successfully completed similar projects within the area of cyber security with the cumulative value of at least 500.000 EUR provided with a reference list containing client name, responsible person and contact information in the last five years.
* The supplier’s turnover over the last 3 years should be cumulative value of over 500.000 EUR.

## 7.2 Project team

The project team (Vendor and Supplier) should have at least the following team structure:

* A **Team Leader** must have at least a Bachelor’s Degree in a relevant field, three (3) years relevant experience in cyber security, at least the last one (1) of which must include team leadership for staff over extended periods which involved supply, configuration, integration, implementation, operation and support.
* At least **one Team Member** with experience of setting up the proposed hardware and ensuring the functionality of the proposed virtualisation software with a minimum of 3 years’ experience, supported by CV and reference letters.
* At least **one Trainer** with experience in implementation of training in the area of cyber security and virtualisation software with a minimum of two (2) years’ experience, supported by CV and reference letters.
* At least **one Team member** as focal point for support and maintenance of the CEP with a minimum of 3 years’ experience supported by CV and reference letters.

All Project team members must be fluent in English.

## 7.3 Standard certificates

The supplier will be certified for:

* ISO 27001
* ISO 9001

## 7.4 Quality evaluation

The quality of proposed solutions will be assessed as specified in Appendix I: Evaluation criteria.

## 7.5 Testing and quality assurance

The inspection of the supplied software system/acceptance testing will be performed at the RATEL’s site. Test plan and quality assurance requirements are given in the Appendix I: Evaluation criteria.

The Test Plan (TP) shall contain detailed verification steps for at least ten (10) functionalities defined in this technical requirements document,all of which will be tested on site, and should be provided together with the Inception Report and approved by the Contractor. The functionalities proposed by the Supplier are subject to modification by the Contractor. The supplier must execute test cases in accordance with the agreed Test Plan.

## 7.6 Project Plan

The bidder should prepare a preliminary project plan for the delivery, installation at RATEL’s site, testing in accordance with the Test Plan provided and elaboration on the content of two-sessions training for 10 representatives named by the beneficiary. It will include estimated duration of each major project activity, providing for 10 months maximum time limit for the project to finish, from the time of signing the contract. It will also include milestones for:

* Inception Report with the timeline of the Project plan
* Delivery and installation of the CEP
* Testing of the CEP and first round of trainings
* Second round of trainings

# APPENDIX I: Evaluation criteria

## 

References: 30 points in total

1. Previous experience of the company in similar projects (similar project – delivery of cyber range solution):

* Two (2) similar projects with a total value of more than 500.000 EUR - 2 point (minimum requirement)
* For each references to additional similar projects more than 500.000 EUR - additional 1 point per project; For each references to additional similar projects more than 1.000.000 EUR - additional 3 point per project up to 12 points
* Project with similar solution implemented with National security related organizations (National CSIRT, Government CSIRT, law enforcement or military) - additional 2 points per project up to 4 points
* Project with similar solution implemented in an academic institution - additional 2 points per project up to 4 points
* Project with similar solution implemented with the Operators of Essential Services/Critical Information Infrastructure - additional 1 point per project up to 2 points
* Project with similar solution which is implemented and in use for at least 5 years - additional 3 point per project up to 6 points

The minimum requirements must be documented by a signed reference letter from the end users. Additional references should be proved by a signed document from the vendor stating: the end user, the project description, project value, year of implementation and duration of the project and end user contacts (name, title and email).

## Technical requirements

The solution is acceptable only if all the **[mandatory]** requirements are fulfilled; if any of these is graded 0, it will disqualify the solution.

The technical requirements of the proposed Cyber Education Platform (CEP) will be assessed as follows:

Quality of the offered solution – total of 33 points

* **[mandatory]** 10 mandatory scenarios provided - 6 points
* **[additional]** Number of additional provided scenarios provided - 1 points per additional scenarios above the mandatory 10, up to maximum of 3 points
* **[mandatory]** Complexity of the simulated ICT environment – the mandatory requirement of 30 components – 6 points
* **[additional]** Complexity of the simulated ICT environment – 1 points per 10 additional components, up to maximum 3 points
* **[additional]** Providing market-leading (based on Gartner reports) COTS SIEM and firewall as part of the simulated environment – 3 points
* **[additional]** Graphical scenario editor for customisation of existing scenarios and creation of custom scenarios – 2 points
* Oral presentation of the offered solution - 10 points

Interface – total of 17 points

* **[mandatory]** Ability to connect remote trainees via VPN – 4 points
* **[additional]** Ability to connect remote trainees without downloading a software agent (client) - 2 points
* **[additional]** Chat tool for users to chat with each other even while connected from remote locations and availability of chat sessions - 2 points
* **[mandatory]** Interface with a time line bar monitoring the scenario progress and the attack milestones through a trainer management console – 4 points
* **[additional]** Observing ability which allows decision makers to have a bird's-eye view of the attack to evaluate how was the cyber-attack developed and was countered (real-time representation, accompanying attack logs) – 2 points
* **[additional]** Ability to provide hints to the trainees within the trainee interface – 2 points
* **[additional]** Built-in quiz mechanism managed and operated by the trainer application – 1 point

## Project team

The quality of the proposed Project Team will be assessed as follows:

Team Leader experience - total of 6 points:

* At least Bachelor’s Degree in the relevant field, at least three (3) years of relevant working experience in the area of cyber security or cyber range delivery, at least the last one (1) of which must include team leadership for staff over extended periods which involved supply, configuration, integration, implementation, operation and support - 1 point
* From three to five (5) years of relevant working experience in the area of cyber security exercise or cyber range delivery – 1 additional point
* More than eight (8) years of relevant working experience in the area of cyber security exercise or cyber range delivery - 1 additional point
* More than three (3) years experience with team leadership for staff which involved supply, configuration, integration, implementation, operation and support - 1 point
* Relevant experience on similar projects worth more than EUR 800.000 per project - additional 1 point; Relevant experience on similar projects worth more than EUR 1.000.000 per project - additional 2 point

The Team consisted of minimum 4 members (but not more than 10):- total of 14 points:

* At least one Team member with a minimum of three (3) years of experience of setting up the proposed hardware and ensuring the functionality of the proposed virtualisation software; At least one Team Trainer with a minimum of three (3) years experience in implementation of training in the area of cyber security; At least one Team Member with a minimum of three (3) years experience as focal point for support in the implementation/delivery of the projects, supported by CV and reference letters - 3 points
* One Team Member with more than four of experience in setting up and ensuring functionality of the proposed solution - additional 1 point
* One Team Trainer with more than four years experience in implementation of training in the area of cyber security - additional 1 point
* Each female team member - additional 1 point up to 3 points per member
* Gender balanced team - 1 additional point
* Team members have relevant certifications in cybersecurity – one point per certificate, max 5 in total (need to provide the certification):
  + ISACA: CISM - Certified Information Security Manager
  + ISACA: CIRSC - Certified in Risk and Information Systems Control
  + ISACA: CISA - Certified Information Systems Auditor
  + ISC2: CISSP - Certified Information Systems Security Professional
  + EC-Council: CEH – Certified Ethical Hacker

1. <https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf> [↑](#footnote-ref-0)
2. <http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2017/53/1/reg> [↑](#footnote-ref-1)