



Tender Document

**Invitation to tender in accordance with
the European open procedure for the
execution of services for Cyber Team
Europe initiative 'Safe Digital Boost for
Africa (SDBA) Continental'**

Publication date:	1 October 2026
Status:	Final
Reference:	202607140

Contents

Definition of terms.....	4
1. Introduction	6
1.1 Tendering Authority and IUC-EZK/LVVN.....	6
1.2 Reason for this invitation to tender	6
1.3 Time schedule	8
2. Description of assignment	9
2.1 Description and objective of the assignment	9
2.2 Lots.....	16
2.3 Contract Period	16
2.4 Scope of the assignment.....	16
3. Requirements to this assignment	17
3.1 Requirements relating to the requested services.....	17
3.2 Requirements relating to the project coordinator	17
3.3 Requirements relating to the cybersecurity role.....	18
3.4 Requirements relating to the prices/rates.....	18
3.5 Tax-related requirements	19
3.6 Invoicing requirements	20
4. Requirements concerning the Tenderer.....	21
4.1 Introduction	21
4.2 Exclusion Grounds.....	21
4.3 Suitability Requirements.....	21
4.3.1 <i>Financial and economic standing</i>	22
4.3.2 <i>Reference data (technical qualifications)</i>	22
4.4 Professional/trade register extract.....	23
5. Award criteria and assessment.....	24
5.1 Introduction	24
5.2 Quality criteria	24
5.2.1 Award criteria relating to the plan, approach and methodology	24
5.2.2 Award criteria relating to the project scoping, implementation and sustainability.....	25
5.2.3 Award criteria relating to the implementation team	25
5.3 Assessment method for qualitative award criteria	26
5.4 Assessment of preferences in relation to prices/rates.....	26
6. Assessment of the Tender	28
6.1 Assessment of the Tender's completeness and legal validity	28
6.2 Assessment of requirements relating to the assignment	28
6.3 Assessment of award criteria relating to the assignment	28
6.4 Determination of definitive total score	28

6.5	Assessment of evidence.....	28
7.	Submission procedure for Tenders.....	30
7.1	Statement of agreement.....	30
7.2	Schedule.....	30
7.3	General procedure	30
7.3.1	<i>Communication</i>	30
7.3.2	<i>eHerkenning</i>	30
7.3.3	<i>Questions and additional information/changes</i>	31
7.3.4	<i>Validity period and submission of Tender</i>	31
7.3.5	<i>Variants on Tender</i>	31
7.3.6	<i>Costs of submitting a Tender</i>	31
7.3.7	<i>Termination of tendering process</i>	31
7.3.8	<i>Order of precedence of documents</i>	31
7.3.9	<i>Information about the Tenderer's obligations</i>	32
7.3.10	<i>Guide Information security and Privacy for suppliers</i>	32
7.3.11	<i>Inconsistencies and objections</i>	32
7.3.12	<i>Complaints procedure</i>	32
7.3.13	<i>Dispute resolution</i>	32
7.3.14	<i>Submission of the Tender</i>	32
7.3.15	<i>Structure and content of the Tender</i>	33
7.3.16	<i>Legally binding signature</i>	33
7.3.17	<i>Submission of a Tender in collaboration with other organisations</i>	34
7.3.18	<i>Single Tender</i>	35
7.3.19	<i>Violation of the fundamental principles of procurement law and restriction of fair competition</i>	35
7.3.20	<i>Communication and language</i>	35
7.3.21	<i>General terms and conditions</i>	35
7.3.22	<i>Contract conditions</i>	35
7.3.23	<i>Explanation and verification of the Tender</i>	36
7.3.24	<i>Request for supplementary information concerning the Tender</i>	36
7.3.25	<i>Announcement of the award of the Contract</i>	36
7.3.26	<i>Use of AI (Including generative AI)</i>	36
	Annexes.....	38

Definition of terms

Tendering authority	Department of the Ministry of Economic Affairs and Climate Policy.
Tender Document	This document and all of its annexes.
Public Procurement Act	The Public Procurement Act 2012 (<i>Aanbestedingswet 2012</i> , wetten.nl - Regeling - Aanbestedingswet 2012 - BWBR0032203).
General Government Terms and Conditions	General Government Terms and Conditions for Public Service Contracts 2025 (ARVODI-2025: <i>Algemene Rijksvoorwaarden voor het verstrekken van Opdrachten tot het verrichten van Diensten</i>).
Most Economically Advantageous Tender	The Tender that achieves the highest definitive total score based on the best price-quality.
Suitability requirements	The requirements with which Tenderers must comply in order to be eligible to win the tender.
Tenderer	An entrepreneur or entrepreneurs who have submitted a Tender or is/are planning to submit a Tender. In this document, the word 'you' is taken to mean the Tenderer.
Tender	A quotation submitted by the Tenderer in response to this Tender Document.
IUC-EZK/LVVN	The Procurement Office (IUC) – part of the Netherlands Enterprise Agency (RVO.nl), which in turn is part of the Ministry of Economic Affairs and Climate Policy (EZK) – will serve as process manager during this tendering process.
Memorandum of Information	A document containing all questions asked and answers given, in anonymised form and, if applicable, additional information. This includes the questions and answers submitted via TenderNed.
Contracting Authority	The State of the Netherlands, represented by the Minister of Economic Affairs, who concludes the Contract with the Contractor on behalf of the Contracting Authority.
Contractor	The party with whom the Contracting Authority concludes the Contract.
Contract	The written agreement between the Contracting Authority and the Contractor in which the conditions of the assignment are recorded.
Exclusion Ground	A circumstance applicable to the Tenderer or a person affiliated with the Tenderer that results in exclusion of the Tenderer from participating in the tendering process.
European Single Procurement Document	A statement in which the Tenderer declares his compliance with the requirements specified in this document.

Data processing Agreement

An agreement signed by the Contracting Authority and the Contractor concerning the processing of personal data by the Contractor. When a Contract is awarded on the basis of the ARVODI, the Contract may require the Contractor to process Personal Data on behalf of the Contracting Authority. If so, the Parties must conclude a Data Processing Agreement under article 28, paragraph 3 of the General Data Protection Regulation ('the Regulation'). In a Data Processing Agreement the Contracting Authority and the Contractor make agreements on the Processing of Personal Data in the context of the Contract.

1. Introduction

The Tender Document at hand contains information regarding this invitation to tender conducted in accordance with the European open procedure of the service "Safe Digital Boost for Africa (SDBA) Continental".

You are hereby invited to submit a Tender based on this Tender Document.

1.1 Tendering Authority and IUC-EZK/LVVN

This tendering process is being conducted on the instructions of RVO, team Private Sector Development. IUC-EZK/LVVN will act as process manager during this tendering process.

About RVO

The Netherlands Enterprise Agency (Rijksdienst voor Ondernemend Nederland, RVO) is an executive body of the Dutch Ministry of Economic Affairs and Climate Policy. RVO helps business owners run sustainable, agricultural, innovative or international businesses. RVO operates in the Netherlands and abroad in partnership with governments, knowledge centres, international organisations and numerous other bodies. The Netherlands Enterprise Agency's overall aim is to improve opportunities for business owners and help them become more competitive. As part of the Sustainable Development Department, several RVO teams work on development cooperation.

About (P)PSD

The RVO (P)PSD programme (Public and Private Sector Development) helps to promote the sustainable growth of small and medium-sized enterprises (SMEs) in around 40 low- and middle-income countries. This programme supports Dutch embassies and local entrepreneurs by providing knowledge, tools and innovation. The Digital team of (P)PSD focusses on European Digital for development programs, including joint EU initiatives to support cyber security capacity building.

1.2 Reason for this invitation to tender

1.2.1 New RVO Africa implementation partner

The European project 'Safe Digital Boost for Africa (SDBA) - Continental' aims to strengthen cyber governance at the pan-African level, in collaboration with the African Union Commission (AUC). It is commissioned by the European Union (EU) delegation in Ethiopia, the Ministries of Foreign affairs of Germany & the Netherlands and implemented by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and the Netherlands Enterprise Agency (RVO).

Due to the unforeseen withdrawal of the intended partner for financial reasons, Tendering authority is looking for a new Africa implementation partner (hereafter: Contractor) regarding this project. This Tender leads to a public service contract for an African partner to support the implementation of key activities of the four main RVO themes of this joint EU action: Critical information infrastructure protection (CIIP), Public- private partnerships (PPP), Cyber skills development/Human capital agenda (HCA) & Cyber hygiene awareness.

The Contractor will work in close collaboration with network partner Smart Africa and the two Dutch partners: Netherlands cyber security centre (NCSC-NL) and the Netherlands cybersecurity coordination centre (NCC-NL). The overall aim is to strengthen cyber security capacity at a continental level and contribute to a resilient cyber ecosystem in Africa.

1.2.2 Background & Problem statement

Given the increasing reliance on digital platforms and the Internet, the potential for cyber threats poses a significant risk to both the African Union's (AU) and the European Union's (EU) socio-economic growth. Both have acknowledged the growing threats posed by cyberattacks, cybercrime, and other malicious cyber activities, which jeopardize the safety and prosperity of their respective regions.

African countries face significant, divergent cybersecurity challenges due to their very different political, social, and cultural contexts – extant approaches towards the rule of law are similarly reflected in cybersecurity governance dynamics. Although there have been improvements, they are also consistently ranked lower in global indices, such as the International Telecommunication Union's (ITU) Global Cybersecurity Index or the e-Governance Academy's (eGA) National Cyber Security Index (NCSI). Not a single African state features in the NCSI's 30 highest-ranked countries and just four African countries are listed in the top fifty percentile. In the Global Cybersecurity Index 2024, just nine African countries are ranked as role-modelling (Tier 1) or advancing (Tier 2). Most African countries are ranked as establishing (Tier 3) or evolving (Tier 4), whilst four remain stuck in the lowest tier of cybersecurity performance. This points to significant vulnerabilities both at a legal and technical level that could be exploited by threat actors. Given that cyber threats do not respect borders, regional and international collaboration is imperative. While cybersecurity has been addressed at AU policy-level, a harmonised strategic approach to tackle current threats is still lacking, and practical application and implementation of existing frameworks remains fragmented.

With the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention), African countries have had a broad common framework on cybersecurity and cybercrime, personal data protection, electronic transactions and international cooperation since its adoption in 2014. It marks the first legal instrument on digitalization to be enacted at the continental level in Africa. For ratification parties, it requires that domestic laws address each policy area and conform to the standards and principles outlined in the convention. However, implementation remains weak – as of June 2025, only 21 countries out of 55 have signed and 16 countries have ratified the Convention, which allowed for its entry into force in June 2023. While it is important to understand specific hindrances for member states to ratify the Convention, there is a lack of continental guidance and role models or champions to increase incentives for implementation. In addition, developments since 2014 on the evolving threat landscape and international frameworks also need to be reflected.

Although Regional Economic Communities (RECs) including the Economic Community of West African States (ECOWAS), the Southern African Development Community (SADC) and the East African Community (EAC) have progressed on regional cybersecurity cooperation, a harmonised approach at continental and regional levels remains challenging. A Continental Cybersecurity Strategy is currently being drafted, but still needs to be finalised, adopted and implemented in a harmonised way. The absence or inconsistent enforcement of cohesive cybersecurity strategies and regulations at continental level leaves gaping vulnerabilities. Without robust regulations, governments are unable to counter sophisticated cyber threats, industries fail to protect their assets, and citizens are left vulnerable to cybercrime. The multilayered nature of cybersecurity requires a strategic perspective that harmonises various policy objectives – from safeguarding critical infrastructure to ensuring individual privacy. Most African countries struggle with adopting international cybersecurity standards, with challenges ranging from legislative shortfalls, fragmented enforcement mechanisms, lack of financial means, and limited capacity to manage cyber threats.

Within the AU system, the topic of cybersecurity is handled by a range of actors in the AU Commission (AUC) as well as further AU bodies. The AU's Peace and Security Council (PSC) has also addressed the impact of cybersecurity on peace and security in Africa and highlighted the need to further explore and address these threats. Jointly with the AU Commission on International Law (AUCIL), the PSC further spearheaded the adoption of a Common African Position on the Application of International Law in Cyberspace in January 2024, which marked the first regional position to be taken on the issue worldwide. So far, there is no coordination mechanism in place that would contribute to comprehensive approaches or a joint vision, combining the perspectives of digital policy, political affairs, peace and security, and international law. Moreover, large-scale cyber-attacks in March 2023 have demonstrated the vulnerability of internal information technology (IT) systems in the AUC and the need for more diversified,

comprehensive and resilient posture in line with international IT and information security standards, as well as increased management awareness and competences to recognise and cope with cyber threats.

Educating and building capacity is vital in creating a cybersecurity-aware society. Yet, in many African countries, there is an evident shortage of qualified professionals and awareness programmes, which applies even more to women. According to ISC2 (International Information System Security Certification), a world leading organisation for cybersecurity professionals, women make up for a mere quarter of the global workforce in the field, while Sans Institute estimates only 9% of cybersecurity professionals in Africa are female. The general population often lacks basic cybersecurity awareness, making them easy prey for cyber-attacks. While larger enterprises might have some cybersecurity mechanisms and regulations in place, small and medium-sized enterprises (SMEs) remain highly vulnerable, due to the high associated costs and lack of expertise. Even where there is awareness, businesses might lack the resources to transform this knowledge into actionable defences due to financial constraints or lack of expert guidance.

Despite these challenges, the private sector has shown a growing interest in strengthening Africa's cyber landscape, assisted by regulatory support from some governments and international investments. A holistic multi-stakeholder approach involving governmental bodies, non-profits, academia, and the private sector is essential for creating a cyber-resilient ecosystem. Currently, there is a lack of platforms that promote multi-stakeholder engagement, resulting in fragmented efforts. Effective partnerships can facilitate the exchange of best practices, resources, and intelligence to counter common threats. But complexities arising from differing institutional mandates, objectives, and capacities often hinder these collaborations.

1.3 Time schedule

The schedule below applies to this tendering process.

1 October 2026	Issuing of publication, start of tendering period.
19 October 2026, 12:00 AM CEST	Closure of round of questions: deadline for the Tenderer to submit questions regarding this Tender Document, the Data Processing Agreement and the Contract (including the general terms and conditions) and/or proposals for textual amendments to the draft Contract (including the general terms and conditions).
30 October 2026	Issuing of Memorandum of Information
11 November 2026, 12:00 AM CET	Deadline for the receipt of Tenders and opening of new Tenders by the Tendering Authority.
11 November 2026 up to and including 7 December 2026	Assessment of Tenders.
8 December 2026	Announcement of the award of the Contract.
23 December 2026	Deadline for the winning Tenderer to provide the evidence requested by the Tendering Authority.
28 December 2026	Deadline for asking questions and/or filing an application for a preliminary injunction in relation to the announcement of the award of the Contract.
1 January 2027	Starting date of Contract.

If – in the opinion of the Tendering Authority – circumstances provide cause to do so, the Tendering Authority is entitled to amend the specified period(s). In such a case, timely notification of the new period(s) will be provided digitally.

2. Description of assignment

2.1 Description and objective of the assignment

2.1.1 Purpose of the assignment

The purpose of this Tender is a public service contract to support the implementation of RVO activities of the European project Safe Digital Boost for Africa (SDBA) – Continental, with the African Union (AU). Particularly focusing on the four RVO themes for cyber security capacity building: Critical information infrastructure protection (CIIP), Public- private partnerships (PPPs), Cyber skills development/Human capital agenda (HCA) and Cyber hygiene awareness.

Tendering authority is looking for an African partner that can play a 'linking pin' role between the (pan-) African stakeholders and key RVO implementation partners of this initiative for cyber security capacity building. The implementation partners are: network partner Smart Africa and Dutch cyber partners: Netherlands cyber security centre (NCSC-NL) and the Netherlands cybersecurity coordination centre (NCC-NL). The overall aim is to strengthen cyber security capacity at a continental level and contribute to a resilient cyber ecosystem in all of Africa.

2.1.2 Cyber Team Europe Initiative

Safe Digital Boost for Africa

The "Safe Digital Boost for Africa" (SDBA) is a key initiative under the European Union's Team Europe framework that aims to accelerate the digital transformation across Sub-Saharan Africa. It is designed to improve the region's digital infrastructure, promote safe digital services, and foster the development of a sustainable digital economy. The initiative focuses on ensuring secure access to digital technologies, enhancing connectivity, and building resilience against cyber threats. It addresses challenges such as the digital divide, cybersecurity, and data protection.

The continental pillar of SDBA will focus on tackling the essential aspects of cybersecurity at the pan-African level. It aims to support the development of harmonised cyber strategies, laws and regulations, enhancing capacity for the protection of critical infrastructure and promoting cyber hygiene at the level of the African Union. Such an approach shall not only ensure a unified political strategy against cross-border cyber threats but also facilitate cooperation at a technical level across Africa in preventing, deterring and responding to cyber-attacks. This shall be achieved jointly by this multi-Donor Action and a separate EU Contribution Agreement with the African Union Development Agency-NEPAD (AUDA-NEPAD).

SDBA Continental project

The "Safe Digital Boost for Africa (SDBA)' – Continental project is implemented by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and the Netherlands Enterprise Agency (RVO). It started in July 2025 and will end in June 2028 (36 months). RVO will be working with two African partners: Smart Africa & RVO Africa implementation partner (hereafter: Contractor) and two Dutch partners: Netherlands cyber security centre (NCSC-NL) & the Netherlands cybersecurity coordination centre (NCC-NL).

2.1.3 Strategic embedding

The objective of the Cyber Team Europe Initiatives program is to enhance (via RVO) the impact of Dutch policy priorities in the field of cyber capacity building through European implementation instruments, in particular on the African continent and in the Indo-Pacific region (both priority regions of the International Cyber Strategy 2023–2028).

2.1.4 Institutional Setting

For the Cyber Team Europe Initiatives program two layers of institutional stakeholders can be identified. The first layer consists of the relevant stakeholders for the project coordination, and the second layer consists of the relevant stakeholders for the project implementation.

Layer 1:

EU delegation in Ethiopia:

- Contracting authority Team Europe initiative SDBA Continental (On behalf of EU INTPA)
- Project oversight

Africa Union Commission (AUC):

- Primary African stakeholder SDBA Continental
- Cyber working group

African Union Development Agency-NEPAD (AUDA-NEPAD):

- Implementation separate EU contribution agreement under SDBA Continental to support AU Member States in strengthening cybersecurity governance and capacity

Regional economic commissions (RECs, such as ECOWAS, SADC & EAC):

- Link between SDBA continental and regional cyber initiatives

Netherlands Permanent Representation to the African Union:

- Liaison role with African Union Commission

Layer 2:

GIZ (German Development agency):

- Lead implementor of Team Europe initiative SDBA Continental
- Coordination of implementation of GIZ activities of the Team Europe initiative SDBA Continental
- Responsible for project planning, finance, monitoring & evaluation and annual reporting

RVO (Netherlands Enterprise Agency):

- Coordination of implementation of RVO activities of the Team Europe initiative SDBA Continental
- Responsible for project planning, finance, monitoring & evaluation and annual reporting

Smart Africa:

- RVO Africa network partner to bring together stakeholders of the African Network of Cybersecurity Authorities (ANCA)

Netherlands Cybersecurity Coordination centre (NCSC-NL):

- Technical implementation partner of RVO activities

Pan-African stakeholders, such as: Private sector bodies (CIIP & PPP), Educational institutions/Centers of excellence (Cyber skills) and Civil society (Cyber hygiene awareness).

Contractor:

- 'Linking pin' role to bring together needs of (pan-) African stakeholders (e.g. African Union commission, Smart Africa) with African and Dutch cyber expertise, to facilitate smooth implementation of RVO activities in Africa

2.1.5 Scope of work

The main aim of SDBA Continental is that a robust cybersecurity environment at African continental level is enhanced, with the specific objective to improve the development of regionally harmonised cybersecurity frameworks and protection of critical information infrastructure at African continental level.

Outputs

The joint EU action consists of three outputs. The Dutch contribution focuses on outputs two and three of the Description of the Action (DOA):

- Output 1: Capacities of competent authorities to design and implement cybersecurity norms, strategies and regulations are increased at continental level;
- Output 2: Mechanisms and operational capacities for the identification and protection of critical infrastructure and incident response are enhanced at continental level;
- Output 3: Cyber hygiene and awareness of cybersecurity threats are improved through regional and international cooperation at continental level.

RVO outputs

Specifically, RVO, as Contracting authority, and its partners are responsible for the following sub-outputs in bold (2.3, 2.4, 3.1 and 3.2). All the other outputs will be implemented by GIZ.

The action aims to achieve the following outputs and indicative results:

Output 1: Capacities of competent authorities to design and implement cybersecurity norms, strategies and regulations are increased at the continental level.

- 1.1 The AUC is enabled to accelerate the implementation and ratification of the Malabo Convention
- 1.2 The AUC has expanded its strategic role and engagement for cybersecurity at continental level.

Output 2: Mechanisms and operational capacities for the identification and protection of critical infrastructure and incident response are enhanced at the continental level.

- 2.1 AUC internal information and cyber security have improved.
- 2.2 Continental cybersecurity maturity and international collaboration have advanced.
- **2.3 A continental network of critical information infrastructure protection (CIIP) providers is in place.**
- **2.4 A continental approach for Public and Private Partnerships (PPPs) for critical information infrastructure is promoted.**

Output 3: Cyber hygiene and awareness of cybersecurity threats are improved through regional and international cooperation at the continental level.

- **3.1 A continental 'Human capital agenda' and expert network is set up to address cyber skills needs on the continent.**
- **3.2 An Africa-centred cyber hygiene campaign has been developed and piloted.**

2.1.6 Role of the Contractor

The Contractor is responsible for the following three components:

- 1) Inception phase: Conduct a scoping study and facilitate updating work plans 2027 and 2028, based on conclusions and recommendations of the inception report, carried out by the 2) project coordinator and 3) cybersecurity expert(s);
- 2) Provide a project coordinator position for the duration of the project (Jan. 2027 – June 2028), to be based in Addis Ababa, Ethiopia or Kigali, Rwanda;
- 3) Providing implementation support with providing cyber security expert(s) of Contracting authority on the activities under outputs 2.3, 2.4, 3.1 (Output lead) & 3.2 (Output lead).

Ad 1) Scoping study/inception phase

The purpose of this scoping study is to:

1. Identify key stakeholders for collaboration at the African Union Commission (AUC) and pan-African level and assess their needs;
2. Develop practical recommendations for effective implementation of RVO activities that contribute to strengthening cybersecurity capacity at the African continent.

As for the scoping study we envision the following activities:

- Perform an African stakeholder (needs) mapping to identify potential partners for RVO activities within SDBA Continental. Focus on Critical Information Infrastructure Protection (CIIP), Public-Private Partnerships (PPPs), an African Human Capital Agenda (HCA) for cyber skills and Cyber Hygiene awareness at continental level;

- Explore how to organize the local implementation of RVO activities in Africa. Provide recommendations for: Effective coordination with African Union Commission (AUC), the GIZ office to the AU, Smart Africa and the NL Permanent Representation at the Netherlands embassy in Ethiopia. Including the role of a local RVO coordinator in Addis Ababa for day-to-day implementation management;
- Identify specific implementation risks for effective Cybersecurity capacity building (CCB) for the RVO activities and suggest ways to mitigate these;
- Advise on updating the monitoring framework and provide indicator guidance notes on the relevant RVO output and outcome indicators;
- Analyse assumptions in programme logic and provide verification or verification strategies
- Organise a scoping and stakeholders needs workshop with AUC & Smart Africa to validate the findings;
- Conduct a learning session with NL cyber partners to incorporate findings from the scoping study into the 2027 and 2028 RVO workplans;
- Based on the activities above, develop an inception report with recommendations on key stakeholder needs, network establishment and a practical implementation plan that contribute to an impactful Cybersecurity capacity building partnership with AUC, Smart Africa and (pan-) African stakeholders.

The following deliverables are expected:

- An African stakeholder (needs) mapping study, including a visual stakeholder map and interactive network database in collaboration with Smart Africa;
- Scoping workshop report with validated stakeholder (needs) mapping and recommendations on network establishment (Annex to the stakeholder mapping study above);
- Learning session report with recommendations for the 2027 & 2028 workplans;
- Inception report with:
 - o Practical implementation plan per NL theme (CIIP, PPP, HCA, Cyber Hygiene);
 - o Recommendations on effective implementation, including the role & responsibilities of the local RVO coordinator;
 - o Implementation risk analysis with mitigation strategies;
 - o Feedback on monitoring framework and indicator guidance notes;
 - o Baseline values on relevant monitoring indicators.

Ad 2) RVO Project coordinator position

The project coordinator will support the planning, organization and implementation of RVO SDBA Continental activities in Africa. The project coordinator will be the 'linking pin' between the RVO team and (pan) African stakeholders. Based in Addis Ababa, Ethiopia or Kigali, Rwanda, the project coordinator will liaise between the Dutch implementation team in the Netherlands and African partners to facilitate effective collaboration on Cybersecurity capacity building. This coordination role requires regular interaction with Smart Africa, RVO, the two Dutch partners Netherlands cyber security centre (NCSC-NL), the Netherlands cybersecurity coordination centre (NCC-NL), the African Union (AU), AUDA-NEPAD, GIZ office Smart Africa & AUC and Netherlands permanent representation to the AU to ensure smooth and timely implementation of the RVO activities of the project, contributing to its overall success and impact.

Purpose: Coordination role to bring together (pan-) African stakeholders' needs with African and Dutch cyber expertise.

Role: Facilitate effective implementation of RVO activities of the SDBA Continental initiative in Africa, in close collaboration with Smart Africa, Dutch cyber partners and RVO.

Coordinate:

- Establish/Maintain a network with relevant partners at the African Union, AUDA-NEPAD, Smart Africa, Regional economic commissions (RECs) and other (pan-)African stakeholders;

- Be the local point of contact and support setting up and implementing RVO activities of the SDBA continental joint action at the African Union (AU) in Ethiopia and Smart Africa;
- Coordinate implementation of planned activities in Ethiopia/Rwanda for the Dutch cyber expert partners: Netherlands cybersecurity Centre (NCSC-NL) and the Netherlands cybersecurity coordination Centre (NCC-NL)
- Liaise with relevant departments at the African Union, Smart Africa, GIZ and other relevant continental stakeholders to align on the implementation planning and creating the envisioned impact of NL activities
- Liaise with GIZ and Dutch expert partners involved in the implementation of this joint EU action to facilitate implementation of Netherlands' activities that focus on: Critical information infrastructure protection (CIIP), Public- private partnerships (PPPs), Human capital agenda/Cyber skills and Cyber hygiene promotion at continental level.
- Connect Dutch cyber expert partners to relevant directorates at the AU & Smart Africa and look for ways to create synergies with other continental African initiatives

Implement:

- Project Planning and Scheduling: Assisting with the development of project plans, timelines, and schedules.
- Communication: Facilitating communication between project stakeholders, team members, and management.
- Progress Tracking: Monitoring project progress, identifying potential risks or delays, and escalating issues as needed.
- Meeting Coordination: Scheduling and facilitating project meetings, preparing agendas, and distributing meeting minutes.
- Quality Assurance: Ensuring project activities comply with organizational policies
- Monitoring & evaluation: Assist with results-based monitoring during implementation of activities and annual EU reporting.

Ad 3) Cybersecurity expert(s) for implementation (support) RVO activities SDBA Continental

This expert role requires regular interaction with the African Union Commission (AUC), Smart Africa and the two Dutch technical partners Netherlands cyber security centre (NCSC-NL), the Netherlands cybersecurity coordination centre (NCC-NL), to ensure smooth and timely implementation of RVO activities. Specifically, outputs 2.3, 2.4, 3.1 (Role of output lead) and 3.2 (Role of output lead) of the joint EU action, contributing to its overall success and impact.

Purpose: Subject-matter experts that will work on continental frameworks CIIP, PPP, HCA/Cyber skills & Cyber hygiene, together with African and Dutch cyber experts.

Role: Cybersecurity expert(s) to facilitate effective implementation (support) of RVO activities related to CIIP, PPP, Cyber skills and Cyber hygiene awareness. in close collaboration with Smart Africa, Netherlands cyber security centre (NCSC-NL), the Netherlands cybersecurity coordination centre (NCC-NL) and RVO.

Coordinate:

- Establish/Maintain a network with relevant policy staff at the African Union Commission (AUC), Smart Africa, Regional economic commissions (RECs) and other (pan-) African stakeholders;
- Perform a 'linking pin' role for Dutch expert partners, NCSC-NL & NCC-NL, involved in this joint EU action to facilitate effective implementation with (pan-) African stakeholders. To contribute to implementation of RVO activities that focus on: Critical information infrastructure protection (CIIP), Public- private partnerships (PPPs), Human capital agenda/Cyber skills and Cyber hygiene promotion at continental level;
- Networking: Connect Dutch cyber expert partners to relevant directorates at the AUC & Smart Africa and look for ways to create synergies with other continental African Cybersecurity capacity building initiatives;
- Output lead role 3.1/3.2: Planning output implementation and scheduling: Facilitation of the development of implementation plans, timelines, and schedules;

- Output lead role 3.1/3.2: Facilitating communication between output stakeholders, team members, and management;
- Output lead role 3.1/3.2: Progress tracking: Monitoring progress of output implementation, identifying potential risks or delays, and escalating issues as needed;
- Output lead role 3.1/3.2: Monitoring & evaluation: Assist with results-based monitoring during implementation of activities within the outputs and annual EU reporting.

Implement:

- Support with contextualisation of output 2.3: Experts to research & co-create CIIP framework, setting up a pan-African CIIP coordination network, co-facilitation of workshops on crisis preparation, incident response and tabletop exercises. In close collaboration with output lead 2.3 (CIIP), the Netherlands cyber security centre (NCSC-NL);
- Implement output 2.4.2: Experts to research & design PPP toolkit, conduct validation workshop, contextualisation and drafting of policy briefs. In close collaboration with output lead 2.4 (PPPs), Netherlands cybersecurity coordination centre (NCC-NL);
- Output lead role 3.1 (Human capital agenda/Cyber skills);
- Implement output 3.1.1: Experts to conduct workshops on Institutional Mapping/Network Design & Collaboration, co-design position paper and knowledge sharing events;
- Output lead role: 3.2 (Cyber Hygiene awareness);
- Implement output 3.2.1 and 3.2.2: Experts to conduct research and content development, co-design workshop, explainer videos, AU wide awareness campaign, incl. advocacy event during cyber awareness month.

2.1.7 Results (activities, outputs & deliverables)

The Contractor will be responsible for the following activities and deliverables, in close collaboration with Smart Africa (Africa network of Cybersecurity authorities) and Dutch partners Netherlands Cybersecurity Centre (NCSC-NL) and Netherlands Cybersecurity Coordination Centre (NCC-NL):

Support with contextualisation of continental Critical information infrastructure protection (CIIP) network in Africa:

Output 2.3: A continental network of critical information infrastructure protection (CIIP) providers is in place

- Indicative activities, in close collaboration with output lead Netherlands Cybersecurity Centre (NCSC-NL), Smart Africa, the African Union commission (AUC) & Regional economic commissions (RECs): Experts to research & co-create CIIP framework, setting up a pan-African CIIP coordination network, co-facilitation of workshops on crisis preparation, incident response & tabletop exercises.
- Indicative deliverable: Contextualised continental CIIP methodology.

Implementation of specific sub- outputs on Public private partnerships, Human capital agenda & Cyber hygiene awareness:

Output 2.4: A continental approach for Public and Private Partnerships (PPPs) for critical information infrastructure is promoted

Sub-output 2.4.2: Develop a contextualised PPP toolkit, based on international best practices and standards, such as ENISA guidelines.

- Indicative activities, in close collaboration with output lead Netherlands Cybersecurity Coordination Centre (NCC-NL): Experts to research & design PPP toolkit, conduct validation workshop, contextualisation & drafting of policy briefs.
- Indicative deliverable: Policy Briefs on PPP Use Cases Across Africa.

Output 3.1: A continental 'Human capital agenda' and expert network is set up to address cyber skills needs on the continent

Sub-output 3.1.1: Set up an expert network of regional African training institutions & Universities involved in cyber security capacity building and identify continental needs related to the African Agenda on Cyber Capacity Building (AA-CCB)

- Indicative activities, as output lead of this activity in close collaboration with Smart Africa and Netherlands Cybersecurity Coordination Centre (NCC-NL): Experts to conduct workshops on Institutional Mapping/ Network Design & Collaboration, co-design position paper and knowledge sharing events.
- Indicative deliverable: Co-designed position paper continental African human capital agenda / Cyber skills development.

Output 3.2: An Africa-centred cyber hygiene campaign has been developed and piloted

Sub-output 3.2.1: Develop a cyber hygiene campaign that is tailored to the unique needs and context of the African continent, including awareness raising on threats stemming from AI

Sub-output 3.2.2: Launch a cyber hygiene advocacy campaign during the Cyber Security Month, targeting AU member states

- Indicative activities, as output lead of this activity and in close collaboration with Netherlands Cybersecurity Centre (NCSC-NL): Experts to conduct research and content development, co-design workshop, explainer videos, AU wide awareness campaign, incl. advocacy event during cyber awareness month.
- Indicative deliverables: Co-designed continental African cyber hygiene awareness campaign and launch event.

Out of scope of this Contract: activities implemented by other RVO partners:

Smart Africa – RVO Africa network partner:

- Needs assessment, Network facilitation & hosting of (online) workshops.

Netherlands Cybersecurity Coordination centre (NCSC-NL):

- Implementation of activities:
 - o Output 2.3 (Output lead): Creating a continental network of players in the field of critical information infrastructure protection.
 - o Work with AU to define a methodology for selection of CIIP & their dependencies, based on existing global and regional best practices.
 - o Develop an informal CIIP coordination network of regional counterparts, to exchange on views, advances and milestones for increased collaboration on sectorial cyber resilience.
 - o Organise workshop with RECs to co-design a continental training toolkit on crisis-preparation & management, an Incident Response toolbox and tabletop exercises, based on global best practices.
 - o Output 2.4.3: Experts to conduct needs assessment, follow-up workshops to develop, review and refine Train-the-Trainer (ToT) on joint sector-wide risk analyses.

Netherlands Cybersecurity Coordination centre (NCC-NL):

- Implementation activities:
 - o Output 2.4 (PPP, Output lead):
 - Output 2.4.1: The development of a methodology for a continental approach to public-private partnerships
 - o Output 3.1.1 (HCA/Cyber skills):
 - Support the development of a roadmap to foster a robust cyber security market and community, based on best practices of the European

2.1.8 Organisation

The Contractor will report to the RVO project manager for SDBA Continental. They will work closely with the African Union Commission (AUC), Smart Africa and (pan-)African Cybersecurity capacity building (CCB) stakeholders, GIZ/NL representation to the AUC, as well as the Dutch cyber partners National Cybersecurity Centre (NCSC-NL) and Netherlands Cybersecurity Coordination Centre (NCC-NL).

2.2 Lots

The invitation to tender has not been divided into lots, because the assignment is a homogenous service, the components are inter-related. The performance specifications necessitate coordinated implementation and the technical interdependencies between the components require integrated procurement. Besides, the assignment and its requirements are accessible to meet and proportional for small and medium- sized enterprises.

2.3 Contract Period

The Contracting Authority intends to conclude a Contract for a period of eighteen (18) months, starting from January 2027 until and including June 2028, including a unilateral option for the Contracting Authority for a no-cost extension of the Contract by six (6) months if this would be agreed with the EU delegation in Ethiopia, Team Europe initiative lead partner GIZ and the Netherlands Ministry of Foreign affairs.

If the maximum value is exceeded (or is threatened to be exceeded), the Contracting Authority has the right to unilaterally terminate the Agreement without compensating the Contractor for this, in whatever form. See further in this regard the provisions in the (draft) Agreement.

2.4 Scope of the assignment

The Tendering Authority has estimated a total contract value (including optional extension months) of EUR 431.700 (exclusive of Dutch VAT and including (if applicable) all local VAT and other local costs and fees).

The value is estimated as follows (exclusive of Dutch VAT and including (if applicable) all local VAT and other local costs and fees).

Indicative budget division*

Support contextualisation output 2.3	€ 50.000
Implementation Output 2.4.2	€ 80.000
Implementation Output 3.1.1	€ 108.100
Implementation Output 3.2.1	€ 98.000
Implementation Output 3.2.2	€ 20.600
RVO project coordinator in Addis Ababa, Ethiopia	€ 75.000
Total	€ 431.700

**exclusive of Dutch VAT and including (if applicable) all local VAT and other local costs and fees*

The estimated value is an indication from which no rights can be derived. This Tender Document was created using up-to-date knowledge and insights valid at the time of its formulation.

It is possible that the services specified in the contract may change in the event of political, budgetary, administrative or organisational developments within the Dutch government and the Contracting Authority's expansion or contraction resulting from this, or changes to the Contracting Authority's position within the government or to the targets that must be met. In the event such circumstances occur, the Contracting Authority will consult with the Contractor.

3. Requirements to this assignment

This section includes the requirements set by the Tendering Authority concerning the requested services and the prices and rates.

By submitting a Tender, you as Tenderer, explicitly consent to all requirements and conditions specified in this Tender document and declare that you will continue to comply with these throughout the entirety of the contract period and that you agree to the statement in Annex 7, arising from EU Regulation 2022/576 of 8 April 2022. Furthermore, you confirm that you will comply with all of the specified prices and rates, including any agreed indexation. Failure to comply with one or more requirements will result in your Tender being disqualified from the assessment process and therefore excluded from the tendering process.

3.1 Requirements relating to the requested services

- 3.1.1 The project coordinator role must be fulfilled by one (1) person, as single point of contact with Contracting authority.
- 3.1.2 The cybersecurity focal roles must be fulfilled by one (1) person, assisted by other experts if required. This cybersecurity expert (the focal person) must be present during stakeholder implementation activities and events such as co-design workshops.
- 3.1.3 The maximum amount of team members, including the project coordinator, cybersecurity expert and (if applicable) assisting experts, must be seven (7) persons.
- 3.1.4 The scoping study must be carried out by the proposed project coordinator and cybersecurity expert(s) of Contractor.
- 3.1.5 At least every (1) month a progress meeting regarding project implementation takes place with Contracting authority.
- 3.1.6 Replacement team member: In case of a replacement of one of the team members, this is only possible in exceptional cases and after approval by Contracting authority, and only if the new expert has at least equal qualifications as the expert proposed in the Tender and meets the requirements specified in chapter 3, as well as the generally applicable conditions under this Tender and the team must continue to comply with the proposal of Contractor in this Tender procedure. In the event of the replacement of one of the experts in the team, the costs of the transition will be borne by the Contractor. This includes, but is not limited to, costs for building a trust relationship with the companies and sector associations in the project, as well as costs for getting sufficiently acquainted with the Contracting authority's working methods and procedures.
- 3.1.7 Activities under each sub-output should result in a co-designed continental approach document. This deliverable should be shared with (pan-) African stakeholders, i.e.:
 - Contextualised PPP toolkit/policy briefs (output 2.4.2)
 - Position paper, Human capital agenda/Cyber skills (output 3.1)
 - Contextualised continental Cyber hygiene awareness campaign (output 3.2).The final versions of these continental frameworks must be translated in the key African Union languages and comply with web content accessibility guidelines (WCAG 2.2, i.e. PDF accessibility check).

3.2 Requirements relating to the project coordinator

- 3.2.1 The project coordinator must be based within a travel distance of two (2) hours by road of Addis Ababa, Ethiopia or Kigali, Rwanda, with occasional travel in Africa.
- 3.2.2 The project coordinator must be familiar with the African Union (AU), Smart Africa and have (the ability to build) an active network within the AU and with other relevant continental stakeholders in the cyber or & digital policy field.
- 3.2.3 The project coordinator is able to bring in and develop a functional network, and to find creative ways of managing relationships at the African Union, Smart Africa and with other (pan-)African stakeholder.
- 3.2.4 The project coordinator has an advanced university degree (a master's degree or equivalent) in a relevant area for this position, such as Business administration/ICT or international relations.

- 3.2.5 The project coordinator has a minimum of five (5) years relevant working experience at medior/senior level, implementing projects with the African Union/Smart Africa/international organization on the African continent or project management in the cyber or digital policy field.
- 3.2.6 The project coordinator has a proven track-record of effective and timely project implementation at an international policy level.
- 3.2.7 The project coordinator has experience with international capacity building projects.
- 3.2.8 The project coordinator has written and verbal communication skills in English (minimal CEFR level B2, both verbal & written).

3.3 Requirements relating to the cybersecurity role

- 3.3.1 All proposed cybersecurity experts must be based in Africa, with focal persons proposed for every sub-output (2.3, 2.4, 3.1 & 3.2).
- 3.3.2 All proposed cybersecurity experts should be specialised in at least one relevant field of cyber security capacity building, i.e. Critical information infrastructure protection (CIIP), Public private partnerships (PPPs), Cyber skills or cyber hygiene awareness. The whole team should cover all of these four fields of expertise.
- 3.3.3 All proposed cybersecurity experts have written and verbal communication skills in English (minimal CEFR level B2, both verbal and written).
- 3.3.4 At least one cybersecurity expert must be familiar with the African Union (AU), Smart Africa and have (the ability to build) an active network within the AU and with other relevant continental stakeholders in the cyber or & digital policy field.
- 3.3.5 For the outputs 2.3 (CIIP) & 2.4 (PPPs): At least one cybersecurity expert has an advanced university degree (a master's degree or equivalent) in a relevant business/engineering field, such as Business administration, ICT engineering or Economics/International relations.
- 3.3.6 For the outputs 3.1 (Cyber skills) & 3.2 (Cyber Hygiene awareness: At least one cybersecurity expert has an advanced university degree (a master's degree or equivalent) in a relevant field, such as Education (Learning & curriculum development) or Communications.
- 3.3.7 At least one cybersecurity expert has a minimum of five (5) years working experience in at least one relevant field of cyber security capacity building, e.g. CIIP, PPPs, Cyber skills and Cyber hygiene awareness.
- 3.3.8 At least one cybersecurity expert has a strong network with the African Union, Smart Africa and other relevant African continental stakeholders.
- 3.3.9 At least one cybersecurity expert has experience with international capacity building projects.

3.4 Requirements relating to the prices/rates

- 3.4.1 The Tenderer will provide an overview of the prices and rates applicable to this assignment by filling in the Annex 2 entitled 'Budget breakdown'.
- 3.4.2 The price/rates must be all inclusive. In any event, they must include all of the following: wage costs, overheads (e.g. accommodation and wage costs for support staff), costs relating to the use of equipment and machinery during the assignment, insurance costs, any applicable costs for e-invoicing, and local travel and accommodation expenses.
- 3.4.3 The agreed (maximum) rates are fixed and invariable for the duration of this Agreement.
- 3.4.4 The Tenderer will not submit any zero or negative prices/rates.
- 3.4.5 The Tenderer will provide a budget breakdown with fixed hourly/daily rates, specified according to the various duties. The Tenderer will charge as stated in section 2.4 of this document.

3.5 Tax-related requirements

- 3.5.1 The Tenderer indemnifies the Contracting Authority against any claims from the Dutch Tax and Customs Administration (*Belastingdienst*) or other tax authorities.
- 3.5.2 The Tenderer will quote the prices according to the following structure:
- the amount excluding Dutch VAT and any VAT due outside the EU;
 - the amount of Dutch VAT due (if applicable) and the amount of any VAT due outside the EU, and;
 - the amount including Dutch VAT (if applicable) and any VAT due outside the EU.
- 3.5.3 If the Tenderer indicates that no VAT is applicable, then he agrees to provide documentary proof of the grounds for this to the Contracting Authority within fifteen calendar days of the request to do so.
- 3.5.4 You are liable for any extra costs for Dutch and/or foreign VAT due if you incorrectly charge no VAT or an incorrect amount of VAT to the Contracting Authority. If applicable, you are liable for accurate payment of VAT in the Netherlands and outside the EU, with the exception of the case stipulated in the following sentence. If the Contracting Authority procures a service from a foreign business and Dutch tax law considers the work to have been performed in the Netherlands, then the Contracting Authority is liable for the payment of VAT to the Dutch Tax and Customs Administration for this/these service(s) performed in the Netherlands.
- 3.5.5 You guarantee that the amounts specified in the quotation are inclusive of all taxes and levies (including amounts considered equivalent to taxes or levies), regardless of their description and wherever in the world they may have been levied.
- 3.5.6 You indemnify the Contracting Authority against any claims from any tax authority for any taxes, levies or contributions considered equivalent to taxes or levies, originating from either the Netherlands or outside the Netherlands.
- 3.5.7 Given the nature of this assignment, which includes development cooperation that exclusively benefits a developing country, a VAT rate of 0% applies to the amount specified on the quotation provided the Contractor is established in the Netherlands and his organisation is registered as an entrepreneur for VAT purposes. **For extra certainty in this matter**, you can request a declaration of exemption from VAT from the tax inspector. More information on this matter can be found within the decree issued by the Ministry of Finance on 21 September 2015 (no. BLKB/2015/76M).
If you submit a statement from the tax inspector within 60 days of the award of the Contract that specifies that a **different** VAT rate applies, then the contract price will be increased to include the applicable VAT rate.
You are liable for any costs (extra or otherwise) in the event that you incorrectly charge no VAT or an incorrect amount of VAT to the Contracting Authority.
- 3.5.8 If you believe that your work is being taxed simultaneously (in part or in full) in both the Netherlands and a foreign country (outside the EU), then you agree to provide evidence from the foreign tax authorities in question that prove VAT has been levied on one of the services/amounts substantiated by you in the quotation. You will provide this statement in English. If the statement from the foreign tax authorities is not in English, then you agree to provide a sworn translation of this statement, the costs of which will be borne by you.

3.6 Invoicing requirements

- 3.6.1 Invoices will be submitted on a quarterly basis, meaning every three (3) months, based on the actual costs. All invoices include an activity report with a planning for the following three (3) months.
- 3.6.2 You must include a summary of the actual hours/days worked in accordance with the applicable rates.
- 3.6.3 **For companies established in the Netherlands only**

E-invoicing

The general terms and conditions that apply to this contract contain a provision that invoices must be sent electronically (not in pdf). This can be done in the following ways:

- Through the supplier portal;
- Through a service provider;
- Through Digipoort;
- Through accounting software.

For a more detailed explanation, please visit: www.helpdesk-efactureren.nl.

For companies not established in the Netherlands

The paragraph concerning e invoicing does not apply to companies located outside of the Netherlands.

4. Requirements concerning the Tenderer

4.1 Introduction

In this section you can find the requirements set by the Tendering Authority to determine whether particular Tenderers are suitable to be awarded the Contract. For this purpose, Exclusion Grounds and Suitability Requirements have been set.

You can indicate whether or not the Exclusion Grounds apply to you and whether or not you are in compliance with the Suitability Requirements by completing the 'European Single Procurement Document'.

The 'European Single Procurement Document' is a PDF file that has been partially filled in for you. You must fill in the rest of the form, legally sign it, submit it together with your Tender via TenderNed (see paragraph 7.3.14).

4.2 Exclusion Grounds

The following Exclusion Grounds are specified in the annex 'European Single Procurement Document':

- all Exclusion Grounds specified in Part III A and B;
- the Exclusion Grounds in Part III C of the 'European Single Procurement Document' that have been selected by the Tendering Authority by means of the tick boxes.

See Section 7 for information on how to submit a Tender in collaboration with other organisations. This section specifies who must provide a completed and signed European Single Procurement Document during the process of submitting a Tender.

The evidence relating to the Exclusion Grounds does not have to be submitted together with the Tender: it is only required once the Tendering Authority requests it.

Please note: The process of applying for a GVA (certificate of conduct) can take several weeks.

For information on types of evidence, see Section 2.89 of the Public Procurement Act. wetten.nl - Regeling - Aanbestedingswet 2012 - BWBR0032203

The evidence consists of:

1. Extract of Trade Register (no older than 6 months, see §4.4)
2. 'Certificate of Conduct for procurement' ('Gedragsverklaring Aanbesteden' -no older than 2 years)
3. Tax statement (no older than 6 months)

Please refer to [eCertis](#)

eCertis is the information system that helps you identify different certificates requested in procurement procedures across the EU.

The Tendering Authority, to which a Tenderer submits data in order to prove that the exclusion grounds referred to in Article 2.86 or Article 2.87 do not apply to the Tenderer, also accepts data and documents from another Member State, from the country of origin of the Tenderer or from the country where the Tenderer is established, that serve an equivalent purpose or that show that the exclusion ground does not apply to Tenderer.

4.3 Suitability Requirements

The purpose of the Suitability Requirements is to assess whether the Tenderer is suitable to fulfil the Contract in the opinion of the Tendering Authority.

By signing the annex 'European Single Procurement Document' (which uses the term 'Selection Criteria' to refer to the Suitability Requirements), the Tenderer declares that he complies with the Suitability Requirements as specified in this subsection of the Tender document. These Suitability Requirements are further specified in the subsequent paragraphs in this section.

4.3.1 Financial and economic standing

By signing the 'European Single Procurement Document', the Tenderer declares:

- a. That he possesses sufficient financial and economic capacity to fulfil the contractual obligations;
- b. That the Tenderer is unaware of any possible claims against him that may compromise his organisation's financial-economic capacity or continuity, and that no investment is required during the Contract period that may have a similar compromising effect;
- c. That the Tenderer has a sufficient level of professional and/or statutory liability insurance for the fulfilment of the assignment and that in the event of the Contract being awarded to him, will remain sufficiently insured throughout the duration of the assignment(s).

Evidence (do not submit together with the Tender – only submit it when requested to do so):

Proof of the economic operator's economic and financial standing may, as a general rule, be furnished by one or more of the following references:

- a. appropriate statements from banks or, where appropriate, evidence of relevant professional risk indemnity insurance;
- b. the presentation of financial statements or extracts from the financial statements, where publication of financial statements is required under the law of the country in which the economic operator is established;
- c. a statement of the undertaking's overall turnover and, where appropriate, of turnover in the area covered by the contract for a maximum of the last three financial years available, depending on the date on which the undertaking was set up or the economic operator started trading, as far as the information on these turnovers is available.

If the data of the Tenderer's parent/holding company is used in relation to the aspect of financial-economic capacity, then the Tenderer must provide a statement from the parent/holding company that specifies that the parent/holding company unconditionally acts as a guarantor for the obligations to be undertaken by the subsidiary company and any debts arising from the Contract incurred by the subsidiary company. The statement by the parent/holding company must be signed by a legally authorised representative.

4.3.2 Reference data (technical qualifications)

The Tendering Authority has set the following core competences, which demonstrate experience with essential aspects of the assignment:

1. Experience with capacity building in the Cyber/Digital domain in Africa;
2. Experience with implementing projects with international consortia & reporting (Annual narrative & financial reporting must adhere to EU guidelines).

By filling in and submitting the reference assignment(s) with Annex 6, the Tenderer declares that he has carried out at least one reference assignment for each of the core competences listed above that meets the following minimum requirements:

- The subject of the reference assignment must be comparable to the core competence in question.
- The reference assignment must have been executed or completed within five (5) years prior to the closing date for the submission of tenders. If the Tenderer uses an assignment that is not yet fully complete, then only the completed results of the ongoing assignment can be submitted for reference purposes: projected results cannot be taken into consideration.

The total value of each reference assignment must be at least EUR 250.000. This reference-

assignment value must exclusively consist of the value of the aspects of the assignment that are equivalent to the service specified in this document. In case a series of separate yet significantly comparable assignments was carried out for the same client during the reference period, then the turnover of these separate assignments can be combined into a cumulative total.

Assignments including one or more subcontractors can only be used as reference assignments if the subcontractor(s) in question will be involved in the fulfilment of the Contract and if the Tenderer can and will make use of the knowledge and experience of the subcontractor(s) in question during the fulfilment of the assignment.

Evidence (do submit together with the Tender):

You may not provide more than one reference for each core competence. If a single reference testifies to multiple competences that comply with the applicable requirements, then you can use the same reference for these different core competences.

The reference(s) must be signed by the referee (the client in question).

The references must also demonstrate that each has a value of at least EUR 250.000.

If required, the Tendering Authority reserves the right to check the accuracy and completeness of the references and to contact one or more of the reference parties without the Tenderer's involvement or permission.

4.4 Professional/trade register extract

The Tendering Authority expects the Tenderer to be authorised to practise his trade. For this reason, the Tendering Authority reserves the right to ask the Tenderer to demonstrate that he is registered in the professional register or in the trade register referred to in Annex XI of EU Directive 2014/24/EU in accordance with the regulations applicable in the country in which he is established.

It is also vital that the signed documents included in the Tender have been signed by a legally authorised representative of the Tenderer. For this reason, the Tendering Authority can also ask the Tenderer who is awarded the contract to demonstrate the legal validity of the signature.

Evidence (do not submit together with the Tender – only submit when requested by the Tendering Authority):

In order to establish the legal validity of the signed statements, declarations and other evidence, it is vital that a recent and up-to-date (**max. six months old**, counted from the time of submission of the Tender) extract from the professional register or trade register is provided in compliance with the provisions stipulated in Section 2.98 of the Public Procurement Act. The extract must demonstrate the legal authorisation of the signatory.

If the signatory of the statements, declarations and other evidence is not featured on the extract, then authorisation of the signatory must be provided by one of the parties featured on the extract, in the form of a statement declaring that the signatory was authorised to legally bind the Tenderer at the time that he signed the documents.

In the event that the Tender involves a collaboration (consortium), then every member of this collaboration must provide the aforementioned evidence separately.

5. Award criteria and assessment

5.1 Introduction

This Section concerns the award criteria. The Tenders are assessed based on the award criteria. Your response to the award criteria must be included in your Tender. In your response, you must take into account the requirements set in Sections 3 and 4.

A maximum of 100 points can be obtained for your response to the award criteria.

1. The Tenderer must score a minimum of 50 out of 100 points that can be obtained on these quality award criteria. If the quality award criteria are valued with a lower score than 50 points out of the 100 points, the Tender is set aside and excluded from further participation in the tendering process.
2. The total score (responses to quality award criteria questions) will be determined. The maximum total points that can be obtained is 100 points.

Your Tender will be assessed solely on the basis of quality, the price is a fixed total price (see also section 5.4) and will not be assessed.

Content of the award criteria

Tendering authority invites interested Tenderers to respond with a proposal, containing the following:

- The proposed plan, approach and methodology – award criterion 1, section 5.2.1;
- The proposed approach regarding the project scoping, implementation and sustainability – award criterion 2, section 5.2.2;
- The proposed implementation team including the CVs of each proposed implementation team member – award criterion 3, section 5.2.3.

A complete checklist of the to be submitted documents by Tenderer is stated in section 7.3.15 of this document.

5.2 Quality criteria

5.2.1 Award criteria relating to the plan, approach and methodology

Max. no. of points available	Assessment aspects
30	The extent to which a convincing plan for the inception phase including scoping study and inception report is presented, by assessing to what degree (15 points): - an identification of key (pan-) African stakeholders including their needs is elaborated; - a practical implementation plan is elaborated; - the roles and responsibilities of the proposed project coordinator and cyber experts are elaborated; - the implementation risks and mitigation strategies and feedback on monitoring framework are elaborated. The extent to which an overview of the approach and methodology used for the execution of the total assignment is presented, by assessing to what degree (15 points): - the planning of activities is elaborated; - the description of the deliverables is elaborated; - the project deployment division, including the number of working days of the project coordinator and per expert and per activity, by filling in Annex 2: Budget breakdown, is elaborated;

	- the Monitoring Evaluation and Learning Framework for annual EU reporting is elaborated. Your response must be written in Verdana, minimum font size 9, or in another font of comparable readability, and shall not exceed ten (10) A4 pages. Please note: any pages exceeding this limit will not be considered in the assessment. Any hyperlinks will not be considered in the assessment. Your answer will be assessed per topic separately (1. Plan inception phase, and 2. Approach and methodology total assignment), using the table in section 5.3. The Tenderer can score in total a maximum of 30 points for this award criterion.
--	---

5.2.2 Award criteria relating to the project scoping, implementation and sustainability

Max. no. of points available	Assessment aspects
30	The extent to which a convincing approach is presented on: - Scoping: Focus on key aspects of strengthening continental cyber governance, with a clear distinction of elements that will be covered by subsequent regional components of SDBA (10 points); - Effective implementation: A comprehensive and inclusive approach to involve (pan-)African stakeholders. Balanced with practical co-designed deliverables in the form of continental methodologies/frameworks for the African Union/Smart Africa (e.g. on resilient cyber ecosystems, Cyber skills & Cyber hygiene awareness). The extent to which the process is inclusive and will lead to practical deliverables for (pan-)African stakeholders will be assessed (10 points); - Sustainability of the project implementation: A clear plan how the capacity building efforts during a relatively short implementation period of 1,5 years will be anchored in long term sustainability (10 points). Your response must be written in Verdana, minimum font size 9, or in another font of comparable readability, and shall not exceed five (5) A4 pages. Please note: any pages exceeding this limit will not be considered in the assessment. Any hyperlinks will not be considered in the assessment. Your answer will be assessed per topic separately (1. Scoping, 2. Effective implementation, and 3. Sustainability of the project implementation), using the table in section 5.3. The Tenderer can score in total a maximum of 30 points for this award criterion.

5.2.3 Award criteria relating to the implementation team

Max. no. of points available	Assessment aspects
------------------------------	--------------------

40	The extent to which the proposed implementation team (including both the proposed project coordinator and cyber security experts): - Demonstrates qualifications and experience regarding cybersecurity capacity building/digital policy for each of the proposed implementation team members; - Demonstrates an active (strategic) network in the AUC/RECs, Smart Africa and Cyber governance field; - Consists of a balanced continental and gender representation (diversity); - Covers a well-balanced team from strategic (political) to operational level. Next to the written elaboration on these assessment aspects, submit the CVs of each proposed implementation team member, including their assigned role, tasks & responsibilities. Your response must be written in Verdana, minimum font size 9, or in another font of comparable readability, and shall not exceed five (5) A4 pages, excluding the provided CVs. Each submitted CV shall not exceed two (2) pages A4 with relevant cyber/digital skills & experience. Please note: any pages exceeding this limit will not be considered in the assessment. Any hyperlinks will not be considered in the assessment. Your answer will be assessed on all named topics together as a whole, using the table in section 5.3. The Tenderer can score in total a maximum of 40 points for this award criterion.
----	--

5.3 Assessment method for qualitative award criteria

During the assessment, the assessment team will work in accordance with the following scale for the weighting of the quality criteria.

Quality of the response	Weighting percentage of the maximum points available per preference
Excellent, with great added value	100%
Very good, with some added value	90%
Good	80%
Ample	70%
Satisfactory	60%
Average	50%
Fair, not completely satisfactory	40%
Unsatisfactory	30%
Poor, insufficient	20%
Very poor, insufficient	10%
No response provided	0%

5.4 Assessment of preferences in relation to prices/rates

In this tender, the 'budget' method is used to determine the successful Tenderer. The given available budget translates into a fixed total price for the Contract to be awarded, which is set by the Tendering Authority. The fixed total price for this tender is EUR 431.700 excluding Dutch VAT, and including (if applicable) all local VAT and all other costs and/or fees. If the total price of your Tender differs from this amount, your Tender will be rejected.

The total price including the breakdown of the costs has to be submitted only via the provided Annex 2 "Budget breakdown".

As the total price is fixed and therefore does not differentiate between Tenders, the Contract will be awarded on the basis of the best price-quality ratio, whereby the ranking of Tenders will be determined solely by the quality score. The Tender with the highest quality score is the winner of this tender and will be awarded the Contract.

All rates offered must be excluding Dutch VAT, and including (if applicable) all local VAT and all other costs and/or fees.

Failure to comply with this requirement will result in your Tender being disqualified from the assessment process and therefore elimination from this tender procedure.

6. Assessment of the Tender

6.1 Assessment of the Tender's completeness and legal validity

The Tender will be assessed according to the following procedure. The Tendering Authority will check whether:

1. all required documents have been provided (see the checklist in the subsection 'Structure and content of the Tender' in Section 7);
2. the information is correct and complete, and no adjustments have been made to the documents provided by the Tendering Authority;
3. no provisos have been made by the Tenderer (e.g. specifying that the Tenderer's own terms and conditions apply);
4. the 'European Single Procurement Document' has been completed in full and has been legally signed.

In the event that the aforementioned requirements have not been complied with, the Tender will be excluded from assessment and further participation in the tendering process, unless rectification is permitted within the boundaries of public procurement legislation.

6.2 Assessment of requirements relating to the assignment

Subsequently, the Tender's compliance with the requirements set out in Sections 3 and 4 will be assessed. Any Tender that does not comply, will be excluded from further participation in the tendering process.

6.3 Assessment of award criteria relating to the assignment

Subsequently, all Tenders not excluded from the tendering process, will be assessed according to the award criteria stipulated in Section 5.

6.4 Determination of definitive total score

The Contract will be awarded according to the principle of the Most Economically Advantageous Tender. The Most Economically Advantageous Tender will be determined on the basis of the best price-quality ratio. As the total price is fixed by the Contracting Authority and is the same for all Tenderers, price does not differentiate between Tenders. Therefore, the ranking of Tenders will be determined by the total quality score obtained on the award criteria set out in section 5.2. The Tender with the highest total quality score will be considered the Most Economically Advantageous Tender.

If two or more Tenderers have an equal highest total quality score, then the Tendering Authority will award the Contract to the Tenderer with the highest final score for the subcriterion "5.2.3 Implementation team". In the event that the highest scoring Tenderers also achieve an equal score for this subcriterion, then determination of the Tenderer to which the Contract will be awarded will be made by drawing lots.

6.5 Assessment of evidence

At the moment that the Tenderer legally signs the 'European Single Procurement Document' and submits the Tender, the Tenderer is not (yet) required to provide any evidence, unless expressly asked to do so in this Tender document.

By signing the 'European Single Procurement Document' and submitting his Tender, the Tenderer agrees that, at a later date, the Tendering Authority is entitled to request that the winning Tenderer provides the required evidence.

Upon awarding the Contract, the Tendering Authority will only request evidence from the winning Tenderer. The Tendering Authority is entitled to request this evidence at an earlier stage and from all Tenderers if it believes such a course of action is necessary to facilitate the progress of the tendering process.

The evidence must demonstrate that the Tenderer indeed complies with the content of both the 'European Single Procurement Document' and the Tender. Following the Tendering Authority's request to provide the evidence, the Tenderer has 15 (fifteen) calendar days to hand over the required evidence. If the Tendering Authority does not agree with the content and/or validity of one or more of the pieces of evidence provided by the winning Tenderer, then this could result in the winning Tenderer being excluded from further participation in the process. In such a case, the Tendering Authority will inform every Tenderer of this situation. The Tendering Authority will then again determine the next Most Economically Advantageous Tender. The score of the Tenderer that has just been excluded will be removed. The calculations will then be carried out once more and a new ranking will be created. The award process will then be conducted again.

In the event a winning Tenderer does not qualify for the definitive award of the Contract, then all Tenderers will be notified of this and the consequences thereof concerning the award of the Contract.

7. Submission procedure for Tenders

7.1 Statement of agreement

By submitting a Tender, including the 'European Single Procurement Document', the Tenderer explicitly consents to all requirements and conditions stipulated in this Tender document and the Memorandum(s) of Information and declares that he will continue to comply therewith throughout the entirety of the contract period and that Tenderer agrees to the statement in Annex ..., arising from EU Regulation 2022/576 of 8 April 2022. Furthermore, the Tenderer confirms that he will comply with all of the specified prices and rates, including any agreed indexation. Failing to comply with one or more requirements will result in his Tender being disqualified from the assessment process and therefore excluded from the tendering process.

7.2 Schedule

See schedule in Subsection 1.3.

7.3 General procedure

This tendering process will be carried out in compliance with the Public Procurement Act. In this case, the 'open procedure' was selected. An announcement thereof was published on www.tenderned.nl and on Tender European Daily (TED).

In the event that a Tender is not submitted in accordance with the provisions and regulations stipulated in this section, the Tendering Authority can set aside the Tender and exclude the Tenderer from further participation in this tender procedure.

7.3.1 Communication

All communication relating to this tender procedure will be conducted via TenderNed (www.tenderned.nl), unless otherwise specified.

Once you have indicated your interest in this invitation to tender on TenderNed, you can send and receive messages about this tender process via 'My Tenders'. Any questions concerning the tender process can be sent to the Tendering Authority's contact person via TenderNed. You will receive messages via TenderNed. Via your personal TenderNed settings, you can turn on automatic notifications, including notifications to your private email address. It is your responsibility to ensure that these emails are not blocked by your email provider's security system. If the communication cannot be conducted via TenderNed, you can contact the following contact person(s): Quintin.Stoutjesdijk@rvo.nl.

Attempts to directly contact parties other than the contact person(s) stated above in relation to this tender process are prohibited.

If you have any functional or technical questions regarding TenderNed, you can contact the TenderNed service desk on weekdays between 08:30 and 17:00 CET on 0800-8363376 or via servicedesk@tenderned.nl. You can also consult [TenderNed voor ondernemingen | TenderNed](#) or [TenderNed for foreign businesses | TenderNed](#).

7.3.2 eHerkenning

All TenderNed users affiliated with a *Dutch* company registered with the Dutch Chamber of Commerce are obliged to log in and register using eHerkenning.

This obligation does not apply to companies not registered in the Netherlands.

Visit [eHerkenning gebruiken voor TenderNed | TenderNed](#) for more information about eHerkenning, including the terms and conditions. You are responsible for any consequences arising from the failure to register with eHerkenning in a timely manner.

7.3.3 Questions and additional information/changes

During the procedure, you have the opportunity to ask questions. Ask your questions as soon as possible. All questions will be answered anonymously. The Tendering Authority can answer your questions via TenderNed in two ways:

- Via one or more Memoranda of Information.
- By means of the TenderNed 'Questions and Answers' facility.

The deadline for submission of your questions is specified in the schedule (see section 1.3). In any event, all questions asked will be answered at least 10 days prior to the deadline for submission of the Tender.

Submitting a question to the Tendering Authority

Questions are to be asked via TenderNed. See <https://www.tenderned.nl/cms/voor-ondernemingen/aanmelden-en-inschrijven/vragen-stellen-een-aanbesteding> or [English | TenderNed](#). For each question, clearly indicate which chapter, section, article and/or page your question relates to.

All questions and answers will be published anonymously for all interested parties to view. If you have a compelling reason why you do not wish your question (and its answer) to be revealed to the other interested parties, then tick the 'Answer Individually' box. However, the Tendering Authority will decide whether or not to process your question individually.

Answers from the Tendering Authority

The Memoranda of Information are an integral part of this Tender document. The Tendering Authority assumes that all sections for which no questions have been asked have been clearly and fully understood.

7.3.4 Validity period and submission of Tender

The Tender must be valid for at least four months after the deadline for submitting the Tenders. In the event that an application for a preliminary injunction is filed with the competent court in The Hague against the award decision, then the Tenderers must in any event ensure that their Tenders are valid until four weeks subsequent to the initial decision by the court.

7.3.5 Variants on Tender

Upon submitting a Tender in accordance with the Tender document, the Tenderer is not permitted to submit a variant of this Tender.

7.3.6 Costs of submitting a Tender

The Tendering Authority will not reimburse any Tenderers for any costs resulting from the drafting and submitting of a Tender, including any further information requested of the Tenderer.

Any costs or damage that (may) arise as a result of not awarding this Tender are for the account and risk of the Tenderer.

7.3.7 Termination of tendering process

Until the moment that the Contract is signed, the Tendering Authority reserves the right to partially, fully, temporarily or permanently terminate the tendering process. In such cases, Tenderers will not be entitled to receive compensation for any costs incurred by them in connection with this Tender, unless the Contracting Authority is of the opinion that a (small) contribution to the tender costs is appropriate in view of the circumstances.

7.3.8 Order of precedence of documents

In the event of inconsistencies between the Tender document and the Memorandum of Information, the Memorandum of Information takes precedence.

In the event that there are multiple Memoranda of Information, then the provisions in the most recent Memorandum of Information take precedence in the event of inconsistencies between the different Memoranda.

7.3.9 Information about the Tenderer's obligations

The Tenderer must take into account his obligations relating to environmental, social and employment law in compliance with article 2.81 paragraph 2 of the Public Procurement Act.

Information on obligations resulting from Dutch legal provisions with regard to taxes, environmental protection, occupational health and safety and terms of employment that will be applicable to the Tenderer's activities throughout the Contract period is available from the following sources:

- Information on taxes: the Dutch Tax and Customs Administration: (www.belastingdienst.nl).
- Provisions concerning environmental protection: the Ministry of Infrastructure and Water Management (www.rijksoverheid.nl).
- Provisions pertaining to occupational health and safety and terms of employment: the Ministry of Social Affairs and Employment: (www.rijksoverheid.nl).

7.3.10 Guide Information security and Privacy for suppliers

Protecting information and personal data is the top priority for the Ministry of Economic Affairs and Climate Policy (EZK). That requires significant effort from our own employees, but also from our suppliers. You can read more about it in this concise guide.

[Suppliers guide Information Security and Privacy EZK](#)

7.3.11 Inconsistencies and objections

If the Tenderer is of the opinion that the documents contain inconsistencies, errors or matters that are unclear or if the Tenderer has any objections, then the Tenderer must report this to the contact person in writing, including substantiation.

7.3.12 Complaints procedure

If a Tenderer disputes a response given by the Tendering Authority to a question, request, comment or objection from the Tenderer, or if the Tenderer receives no response, then he can submit a complaint. More detailed information on this matter can be found in the 'Complaints Procedure' annex.

7.3.13 Dispute resolution

In addition to the provisions in the 'Complaints Procedure' subsection, any dispute arising from this tendering process can be presented to the Public Procurement Experts Committee (www.commissievanaanbestedingsexperts.nl) and/or to the competent court in The Hague. Dutch law applies exclusively to such proceedings.

7.3.14 Submission of the Tender

The deadline (date and time) for submission of Tenders is stipulated in the 'Time schedule' (1.3).

- In order to submit a Tender, you must register with TenderNed. One or more registered users must be connected and authorised to submit the Tender via TenderNed on behalf of your company.
- The Tendering Authority advises that you start the TenderNed registration process immediately rather than postponing it until the tendering period is coming to a close. Upon registering your organisation, you must add your tender via TenderNed's announcements platform.
- For more information on registering and establishing your organisation with TenderNed and digital submission of your Tender, visit [TenderNed gebruiken als ondernemer | TenderNed](#) or [TenderNed for foreign businesses | TenderNed](#).
- Only Tenders that have been submitted to the digital safe for this invitation to tender either prior to or on the day of the deadline (prior to the time of the deadline) will be processed by the Tendering Authority.
- The time and date as displayed on the digital countdown clock in TenderNed serves as the definitive deadline for the submission of Tenders.

- The Tendering Authority is only able to see the Tenders once the digital safe opens in TenderNed. This safe can only be opened upon expiry of the deadline for the submission of Tenders.
- In the event you have technical issues or questions regarding submission of your Tender via TenderNed, you can contact the TenderNed service desk via servicedesk@tenderned.nl or +31 (0)70-3798899. If you believe that the TenderNed service desk is taking too long to answer your question or comment, then you can contact your contact person within the Tendering Authority.
- Any risks resulting from late submission of the Tender and/or submission of an incomplete Tender is borne by the Tenderer.
- The Tendering Authority is neither responsible nor liable for any consequences resulting from a Tender that is submitted too late, incorrectly or incompletely.

The Tendering Authority will treat confidential information provided by the Tenderer with due care.

7.3.15 Structure and content of the Tender

The Tender must be submitted entirely via TenderNed and the 'European Single Procurement Document' must be legally signed.

You can use the following checklist during the submission of your quotation.

Subject	Description	Action required from tenderer
Annex 1	European Single Procurement Document*	Fill in, legally sign and add to TenderNed
Annex 2	Prices/rates and all other costs included in the budget breakdown	Fill in, legally sign and add to TenderNed
Annex 6	The reference(s) with which you substantiate that you have the required core competences	Fill in, legally sign and add to TenderNed
Requirements and award criteria	The CVs of the project coordinator and the cybersecurity expert(s) that demonstrate their experience and knowledge for the purpose of the requirements and award criteria stated in this Tender Document	Add to TenderNed
Award criteria	A separate response to each of the Tendering Authority's award criteria	Add to TenderNed

* See Subsection 7.3.16 in the event your Tender is submitted in collaboration with other companies.

7.3.16 Legally binding signature

A legally binding signature means that a document has been signed by a duly authorized representative.

If it is recorded in the professional or company register that two or more persons only have joint powers of representation, then the documents requiring a legally binding signature must be signed by those two or more persons. If any restrictions are in place regarding the authorization to represent the organization, then these must be taken into account.

Where a legally binding signature is required, the Contracting Authority accepts either an original handwritten signature, or the qualified electronic signature within the meaning of article 3: 15a of the Civil Code (or EU Regulation no. 910/2014, article 3, part 12).

There are 3 ways to sign the ESPD:

1. Print, sign and scan;
2. Digitally insert an electronic (certified) signature or a scan of a pen-written signature;

3. Create and insert a certification ID online.

The lack of a legally binding signature in principle will lead to exclusion from the tendering procedure. In that case, however, you will be given one single opportunity to correct it within 48 hours.

7.3.17 Submission of a Tender in collaboration with other organisations

If you cannot carry out the assignment independently, you can set up a collaboration with other organisations.

There are two ways in which you can submit a Tender in collaboration:

- 1) As a consortium in which each member of the consortium is jointly and severally liable for the fulfilment of the obligations arising from the Tender as well as the fulfilment of the Contract.
- 2) In a principal contractor-subcontractor structure in which the Contractor is liable for the fulfilment of all obligations, including the obligations that will be subcontracted.

Tendering as a consortium

If a Tender is submitted by a consortium, then:

- Every member of the consortium must fill in and legally sign a separate 'European Single Procurement Document', which also includes a specification of who the consortium members are (see Part II of the 'European Single Procurement Document'). Indicate the role each member plays within the consortium. In the 'European Single Procurement Document', you must indicate who is in charge of the consortium (who is lead manager) and will act as its authorised representative.
- All organisations in the consortium accept joint and several liability for the fulfilment of the obligations arising from the Tender and the eventual fulfilment of the Contract. If a consortium member relies upon the capacity of another entity in order to demonstrate compliance with the applicable Suitability Requirements (see section 4 of this document), then the subcontractor(s) in question must also complete a separate 'European Single Procurement Document', filling in parts II A, II B, III and IV and legally sign it (see the information under II C in the ESPD).
- Every member of the consortium, for their part, must provide the evidence requested for the Tender.

Submitting a tender as a principal contractor together with subcontractors

If a Tender is submitted by a principal contractor that does not rely upon the capacity of any subcontractors, then only the principal contractor is required to complete and legally sign Part II D of the 'European Single Procurement Document'.

If the principal contractor does rely on the capacity of subcontractors in order to demonstrate compliance with the applicable Suitability Requirements, (see section 4 of this document), then the subcontractor(s) in question must also complete a separate 'European Single Procurement Document', filling in parts II A, II B, III and IV and legally sign it (see the information under II C in the ESPD).

The subcontractor on whose capacity the principal contractor *does* rely must provide the evidence requested for the Tender.

The principal contractor is fully liable for the fulfilment of the obligations arising from the Tender as well as the fulfilment of the contract (if awarded). In addition, the principal contractor is liable for the fulfilment of the obligations for which he has hired the subcontractor(s).

All completed and legally signed 'European Single Procurement Document' forms must be added to the Tender.

7.3.18 Single Tender

All natural persons, legal entities and organisations may only submit a single Tender (either individually or in combination with other natural persons, legal entities and/or organisations). Tenderers who are mutually connected via a relationship of dependence (group link) are permitted to participate separately in this tendering procedure. However, this is on the express condition that they participate as competitors in this tendering process. For this purpose, they must demonstrate that their mutual relationship has not influenced their behaviour within the scope of this tendering procedure nor has it restricted fair competition.

By submitting a Tender, the Tenderer in question agrees to this condition.

7.3.19 Violation of the fundamental principles of procurement law and restriction of fair competition

Any Tenderer whose actions violate a fundamental principle of procurement law (such as the equality principle), the result of which restricts or could restrict fair competition, will be excluded from this tendering procedure. This is also the case if the violation or the restriction of fair competition only comes to light after the announcement of the award of the Contract to all Tenderers. Prior to making the decision to exclude the Tenderer in question, the Tendering Authority will notify the Tenderer of this intention, at which point the Tenderer will be given the opportunity to demonstrate to the Tendering Authority that no violation of a fundamental principle of procurement law or restriction of fair competition has taken place.

By submitting this Tender, the Tenderer declares his awareness that actions contravening any fundamental principle of procurement law can result in the aforementioned consequences. The Tendering Authority can use all resources available to him in order to identify any violation of the fundamental principles of procurement law or the restriction of fair competition. A judicial decision will not be a necessary requirement in such cases.

7.3.20 Communication and language

During the tendering process, communication with the Tendering Authority must be conducted in English.

The Tender must be submitted in English.

Additional documents (such as informational materials etc.) must also be provided in English.

During the fulfilment of the contract, communication must be conducted in English.

7.3.21 General terms and conditions

The applicability of any of the Tenderer's general terms and conditions concerning delivery, payment and/or any other matters is explicitly excluded. The General Government Terms and Conditions apply to the Contract.

7.3.22 Contract conditions

The draft Contract, Data processing Agreement and the corresponding General Government Terms and Conditions are included in the annexes. The Tenderers have the opportunity to ask questions, make comments and propose substantiated textual amendments.

The Tendering Authority is free to accept or reject the proposed textual amendments. The Tendering Authority will indicate whether or not the proposals have been accepted or rejected in the Memorandum of Information. By submitting the Tender, the Tenderer declares his consent to the (possibly amended) Contract. Only the definitive Contract will apply during the execution of the assignment.

7.3.23 Explanation and verification of the Tender

The Tendering Authority can request that the Tenderer explains his Tender in greater detail and/or provide substantiating documents. The Tendering Authority is entitled – although not obliged – to check the accuracy of all data and statements submitted within the scope of the Tender.

7.3.24 Request for supplementary information concerning the Tender

The Tendering Authority can ask Tenderers to provide supplementary information and/or clarification of their Tender.

7.3.25 Announcement of the award of the Contract

All Tenderers will receive a message simultaneously that announces the award of the Contract and substantiates its decision. All Tenderers are entitled to request further information regarding this decision from the Tendering Authority.

Standstill period

All Tenderers and stakeholders who dispute the award of the Contract and/or the verbal/written substantiation thereof can apply for a preliminary injunction at the competent civil court in The Hague. The summons must be served within 20 calendar days subsequent to the sending of the digital notifications concerning the award of the Contract. Upon expiry of this period, no more applications for a preliminary injunction can be submitted. In the event a Tenderer applies for a preliminary injunction, we kindly request that you send a copy of the summons to the Tendering Authority.

On the grounds of Section 2.129 of the Public Procurement Act the award of the Contract does not yet mean the Tenderer's Tender has been accepted. For the 20 calendar days subsequent to the sending of the digital notification of the award of the Contract, the Tendering Authority is not permitted to definitively award the assignment by concluding the Contract.

If a preliminary injunction is applied for during these 20 calendar days, then a waiting period will be required pending a judgement in the preliminary injunction proceedings. The judgement will serve as the basis for further decision making by the Tendering Authority.

If preliminary injunction proceedings are brought against the award of the Contract, then the Tendering Authority will notify the Tenderer of this fact. The Tenderer must ensure that his Tender remains valid for at least four weeks subsequent to the judgement in the preliminary injunction proceedings.

Interest in relation to the judgement

Tenderers who have an interest in the judgement in these preliminary injunction proceedings can only engage in these proceedings by means of intervention or joinder. The Tenderer cannot initiate separate proceedings or other judicial proceedings.

7.3.26 Use of AI (Including generative AI)

AI is defined as: artificial intelligence, including generative AI (text, image and code generation).

The use of AI in the preparation of (parts of) the Tender is permitted. The Tenderer remains fully responsible for the content, accuracy and timely submission; errors, omissions or factually incorrect AI output are at the Tenderer's own expense and risk. The Tenderer shall not input any tender-related and/or business-confidential information and/or personal data into AI systems (including cloud services), unless this is lawful and appropriate legal and technical safeguards have been put in place.

The Tenderer shall ensure human review and validation prior to submission and compliance with the applicable obligations under the AI Act (Regulation (EU) 2024/1689).

Upon request, the Tenderer shall provide a verifiable explanation of the use of AI (tool/version, purpose/application and checks carried out), insofar as this can reasonably be expected of the

Tenderer, and shall specify which parts of the Tender have been produced using AI. The Tenderer guarantees that the Tender does not infringe the rights of third parties and indemnifies the Contracting Authority against any claims in this regard.

Annexes

The following annexes constitute an integral part of this Tender document. These annexes were published together with the Tender document.

Annex 1: European Single Procurement Document

Annex 2: Budget breakdown

Annex 3: Draft Public Service Contract

Annex 3a: Draft Data processing Agreement

Annex 4: ARVODI-2025

Annex 5: Complaints Procedure

Annex 6: Reference assignments

Annex 7: Statement pursuant to EU Regulation 2022/576 of 8 April 2022 (Russian involvement)