Annex 1 to the Framework Agreement - Technical Specifications

The object of the framework agreement is the purchase of the goods and services necessary for the implementation of cyber security projects carried out by the Estonian Centre for International Development (ESTDEV).

1. Background information

1.1. ESTDEV implements ICT and cyber security projects initiated within the framework of international development cooperation, using the experience and know-how of the private and public sectors. With the framework agreements to be signed, we want to involve companies that contribute to projects coordinated by ESTDEV by developing and implementing innovative solutions related to information and cyber security, which may include (or partially or fully consist of) the relevant software, applications, technical infrastructure and its components, as well as installation, configuration, training and consulting activities related to or not related to the above.

2. General

2.1. The purpose of the public procurement is to conclude framework agreements with partners (hereinafter jointly referred to as ***the contractor***) for ordering cyber security-related matters and services within the framework of Estonian development cooperation.

2.2. The procurement contract for the performance of the order submitted in the mini-competition is concluded between ESTDEV (hereinafter also ***the contracting entity or contracting authority or customer***) and **the contractor who won the procurement**. The customer adds the project-specific content and technical requirements **of the procurement** to each commissioned work separately.

2.3. The contracting authority shall apply the control of international sanctions prior to the conclusion of contracts with contractors. The contracting authority shall not enter into a public contract and shall exclude from the procurement procedure a tenderer or applicant with whom the conclusion of the public contract would violate an international sanction or a sanction imposed by the Government of the Republic within the meaning of the International Sanctions Act.

2.4. The beneficiaries of the works and services performed within the framework agreement are often people and institutions located in foreign countries. Therefore, it is necessary to consider the specifics of the destination country in each case. The contractor is responsible for complying with the norms of the destination country (electricity, occupational safety, communications, etc.) and is responsible for the work of its subcontractors and on-site staff. Employees sent to work in the destination country must meet the requirements described in the basic document of this public procurement "PEE Annex 1 – Requirements for the tenderer's team and CV form". The contracting entity has the right to demand the involvement of partners located in the countries of destination in mini-competitions, the respective conditions will be presented in the mini-competition.

2.5. All equipment and configurations supplied by the contractor must comply with EU data protection and information security standards.

2.6. The contractor must ensure that the installation, maintenance and warranty services of the equipment supplied under the framework agreement are available in the country of installation. The contractor ensures that it has sufficient technical capacity, resources and, if necessary, local partners to carry out the work in the destination country. All local laws, standards and requirements (including occupational safety, electrical and communication regulations) must be complied with at the contractor's expense and responsibility.

2.7. The public procurement for the conclusion of framework agreements is divided into the following parts, in all of which tenders can be submitted if desired:

2.7.1. Lot/Part 1 - Information and cybersecurity consulting services;

2.7.2. Lot/Part 2 - Information and cybersecurity software analysis, development and applications;

2.7.3. Lot/Part 3 – Various IT and cybersecurity infrastructure components, installation and configuration.

2.8. If a notice has been made within the framework of a mini-competition, it is mandatory to apply the internal rules of the contracting entity in the performance of the contract.

3. Lot/Part 1 - Information and cybersecurity consulting services

3.1. Information and cyber security consulting services include, for example, the following services:

3.1.1. various analytical tasks, including identifying training needs and creating training plans;

3.1.2. Cybersecurity-related advisory services;

3.1.3. Conducting various seminars, workshops and other events related to cyber security;

3.1.4. conducting Cyber Range-based technical and non-technical tabletop exercises and other forms of cyber security-related training;

3.1.5. preparation of security monitoring and response plans (incl. information security risk analyses, creation and implementation of security management rules and strategies);

3.1.6. developing solutions that ensure cybersecurity;

3.1.7. Security penetration testing, vulnerability and risk assessment;

3.1.8. Development of training programmes and materials;

3.1.9. Target group and level-based training for different target groups in different ways and languages;

3.1.10. Other work that is intrinsically in the field of cybersecurity consulting.

3.2. Requirements for the provision of services:

3.2.1. Mode – onsite, remote or hybrid work;

3.2.2. Languages – English (other local language by agreement). The language of performance of the contract is specified in the framework agreement and the public contract each time in a mini-competition, if it differs from the provisions of the framework agreement;

3.2.3. In the case of technical training, it is assumed that the trainer will be able to use their own practical and technical laboratories.

3.3. The topics of possible on-demand consultation services (including its various forms, such as trainings) are also listed as examples, but the list is not exhaustive:

3.3.1. Cyber hygiene (for different levels);

3.3.2. Training on the implementation of various standards and frameworks (NIST, ISO, CIS, GDPR, NIS2, etc.);
3.3.3. Risk management and management;
3.3.4. *Blue team* an *Red team*, i.e. technical defense and attack trainings;
3.3.5. *Threat hunting* Workshops;
3.3.6. CERT / CSIRT / SOC / CSOC operational and technical training to meet the needs;
3.3.7. Training and workshops on the protection of network equipment and other IT infrastructure *(*hardening);
3.3.8. End Devices and Identity: EDR/XDR *(*Entpoint Detection and Response / Extended Detection and Response), Windows/Linux/macOS karastamine, AD/AAD/Entra (Active Directory/Azure Active Directory), PAM (Privileged access management);
3.3.9. Cloud & Containers: AWS/Azure/GCP turve, Kubernetes, IaC (Terraform) turve, CI/CD (Continuous Integration / Continuous Deployment) & DevSecOps (SAST/DAST/SCA (Static Application Security Testing / Dynamic Application Security Testing / Software Composition Analysis));
3.3.10. Applications: OWASP (Open Web Application Security Project) Top 10, Secure Programming (Java/.NET/JS/Python), API Security;
3.3.11. Intelligence and threat models; web/application/API testing; AD attacks; Wi-Fi; Phishing campaigns;
3.3.12. Telemetry and data readiness, methodology, query design (SIEM/EDR/XDR, Wasuh, Elastic);
3.3.13. SIEM/SOAR/Case Management (Security Information and Event Management / Security Orchestration, Automation, and Response): Splunk, Microsoft Sentinel, Elastic, TheHive/Cortex, MISP;
3.3.14. Network/Network Expertise: Zeek, Suricata, Wireshark, Arkime, Velociraptor, Autopsy;
3.3.15. AppSec/DevSecOps: OWASP ZAP, Burp Suite, Trivy, Semgrep, GitHub/GitLab Security.

4. Lot/Part 2 - Information and cybersecurity software analysis, development and applications

4.1. Tasks related to the analysis and procurement of information and cyber security software solutions, as well as the implementation and configuration of applications, include::
4.1.1. Ex-ante analysis and requirements mapping – business needs, information security and compliance requirements (e.g. GDPR/NIS2/ISO 27001);
4.1.2. Solution architecture – HLD (High-level Design) and detailed (LLD, *Low-level Design*) architecture and transition plan (as-is → to-be);
4.1.3. Procurement support – comparison of manufacturers/resellers, analysis of licensing models and total costs, request tenders and comparison tables;
4.1.4. Pilot/PoC (Proof of Concept) – validation of suitability, performance and security assumptions in a controlled environment;
4.1.5. Environment preparation – network and access models, servers/cloud accounts, roles/permissions, log sources;
4.1.6. Installation and setup – manufacturer's best practices, hardening and safe base configurations;
4.1.7. Integrations– AD/AAD/Entra, IAM/PAM (Identity Access Management / Privileged Access Management), SIEM/SOAR, EDR/XDR, ticketing, CMDB (configuration management database), email and cloud services;

4.1.8. Software development – software development from scratch according to the wishes of customers, modification or upgrade of existing software;
4.1.9. Data migration – transfer of rules, settings, logs, identities, and integrations; *rollback* plan;
4.1.10. Automation and IaC (Infrastructure as Code) – scalable deploy (e.g Terraform/Ansible), CI/CD (Continuous Integration / Continuous Deployment) integration, version control;
4.1.11. Testing and Acceptance Criteria – Functional, Security, Performance and Load Tests; UAT/SAT (User Acceptance Test / System Acceptance Test) criteria;
4.1.12. Documentation– HLD/LLD, configuration templates, runbooks and SOPs (Standard Operating Procedures), Asset Management/CMDB Updates;
4.1.13. Training and handover – admin, user and ops training, handover seminar and knowledge transfer;
4.1.14. Availability and reliability of services, data and information systems– RTO/RPO (Recovery Time Objective/Recovery Point Objective), backup and restore, DR procedures, maintenance windows;
4.1.15. Performance and scalability of information systems and IT solutions – metrics/KPIs (throughput, latency, number of agents), scaling and archiving strategy;
4.1.16. Security and quality control – CIS benchmarks, vulnerability scans.
4.1.17. Maintenance and support of IT systems and software solutions (SLA) – patching and upgrades;
4.1.18. Licenses and IP – license management (CAPEX/OPEX (Operational Expenditure / Capital Expenditure)), mitigation of dependencies/*vendor lock-in* risk;
4.1.19. Open Source - Community vs Enterprise Support, Security Patch Policy, Configuration to Production Ready;
4.1.20. Other activities intrinsically related to the analysis, development and implementation of cybersecurity software.

4.2. Other terms:
4.2.1. Mode – on-site, remote or hybrid work;
4.2.2. Languages – English (other local language by agreement). The language of performance of the contract is specified in the framework agreement and the public contract each time in a mini-competition, if it differs from the provisions of the framework agreement;
4.2.3. Delivery and other work documents – issued as a single package (architecture, test plans, configurations, handover report).

4.3. Categories of sample solutions (by topic):
4.3.1. SIEM/SOAR and case management– log collection, use case engineering, automation, and escalation; e.g. MS Sentinel, Elastic, Splunk; TheHive/Cortex, SOAR Tools;
4.3.2. EDR/XDR/AV – end and server protection, telemetry, response; e.g. Defender for Endpoint, CrowdStrike, Wazuh, Elastic Agent;
4.3.3. IAM/SSO/MFA/PAM – ideidentity, access and privilege management; e.g. Entra ID/AD, Okta/Keycloak, CyberArk/Teleport;
4.3.4. NDR/IDS/IPS/NTA – detection of network behavior and intrusions; e.g. Zeek, Suricata, Security Onion/Corelight;
4.3.5. Perimeter and remote access – firewalls, WAF, DDoS, ZTNA/SASE/SSE; segmentation and VPN;
4.3.6. Email and web security– SEG, Sandboxes, DMARC/DKIM/SPF, phishing protection;

4.3.7. Cloud security– CSPM/CNAPP/CWPP, Cloud-KMS/HSM, Cloud-native controls (AWS/Azure/GCP);
4.3.8. Container and Kubernetes - image scanning (e.g. Trivy), runtime protection (Falco), policies (OPA/Gatekeeper), registry security;
4.3.9. AppSec/DevSecOps – SAST/DAST/SCA, secrets-admin (e.g. Vault), CI/CD integration, code scanning;
4.3.10. Vulnerability and installation management – scanners (e.g. Nessus/OpenVAS), site management (WSUS/SCCM, repos), correction workflows;
4.3.11. Backup, Archiving & DR – Immutable Backups, Tested Restore, Retention Periods;
4.3.12. Cryptography, PKI and Key Management - Certificate Lifecycle (ACME), PKI/CA, Vault/KMS/HSM;
4.3.13. Threat intelligence (TIP/TI, (Threat Intelligence Platform / Threat Intelligence)) – MISP, OpenCTI, feeds and enrichment; integration into the SOC workflow;
4.3.14. DFIR and data analytics – tools for forensics and log/data warehouses (e.g. Velociraptor, Autopsy, Elastic);
4.3.15. OT/ICS/IoT Security – discovery, protocols, segmentation, monitoring;
4.3.16. MDM/UEM and mobile security – device management, app and data protection;
4.3.17. API security - API gateway, mTLS, attack protection, and discovery.

5. Lot/Part 3 – Various IT and cybersecurity infrastructure components, installation and configuration

5.1. The service of acquiring, installing, configuring and training ICT infrastructure components includes, for example:
5.1.1. Architecture & Design– HLD/LLD, network and system architecture, IP plans, address spaces, naming conventions, „as-is → to-be" transition plan;
5.1.2. Procurement support– comparison of manufacturers/distributors, requests for quotations and comparison tables, licensing and maintenance models, delivery plan;
5.1.3. Pilot/PoC – validating suitability, performance, and security assumptions in a controlled environment;
5.1.4. Supply and logistics – supply planning, customs/formalizations (if applicable);
5.1.5. Facility and infrastructure preparation – racks, *patch* panels, cabling (network/FO), marking and marking, power/UPS/PDU, cooling, grounding; documentation (rack elevations);
5.1.6. Installation – physical installation, cabling and optics, initial configurations, access, secure primary access;
5.1.7. Configuration and hardening – manufacturer best practices, password policies, RBAC, cryptography, log and audit settings, time synchronization (NTP/PTP), management networks;
5.1.8. Integrations and corresponding software solutions – AD/AAD/Entra, DNS/DHCP/NTP, SIEM/SOAR, EDR/XDR, backup management, CMDB, ticketing system, monitoring;
5.1.9. Virtualization and platforms – configuration of hypervisor clusters (e.g. VMware/Hyper-V/Proxmox), HCI, creation of container nodes, implementation of resource plans (CPU/RAM/IO);
5.1.10. Data Storage and Backup – SAN/NAS/Object Storage, Replication, Snapshots, NFS/SMB/iSCSI/FC, Backup and Recovery Procedures, RPO/RTO;
5.1.11. Remote access and management – VPN/ZTNA appliances, bastion hosts, PAM, secure remote control and audit trail;

5.1.12. Network Protection & Detection – Firewalls, IDS/IPS/NDR Sensors, WAF/Load Balancer, Segmentation/ACLs, QoS;
5.1.13. Testing and admission criteria – FAT/SAT/UAT; throughput and latency tests, IOPS/latency on the recorder, failover/HA test, backup recovery test; Acts of Acceptance;
5.1.14. Documentation – HLD/LLD, as-built, IP and VLAN plans, cabling diagrams, configuration files, runbooks/SOPs, maintenance and DR manuals;
5.1.15. Training and handover – admin/operator training, maintenance procedures, knowledge transfer, handover seminar;
5.1.16. Security and compliance requirements – access levels, logging/auditing, encryption, device and image signatures/SBOM (if applicable), supply chain security;
5.1.17. Service and Support (SLA) – Manufacturer's Warranty and Extensions, Firmware/Patch Process, Escalation to the Manufacturer, Spare Parts;
5.1.18. Performance and scalability – KPIs (throughput, CPU/RAM utilisation, IOPS/latency), scaling and archiving strategy, capacity planning;
5.1.19. Lifecycle Management – EOL/EOS Monitoring, Upgrade/Replacement Plans, Asset Id/*Serial*, CMDB Updates;
5.1.20. Migration and migration – migration of services/VMs/data, deployment of cloud services, maintenance windows, rollback plan;
5.1.21. Eviction and disposal – safe data destruction (e.g. NIST 800-88), environmental requirements, proof of disposal;
5.1.22. Other goods and services intrinsically linked to the subject-matter of the framework agreement.

5.2. Other terms:
5.2.1. Mode – on-site, remote or hybrid work (secure remote control);
5.2.2. Languages – English (other local language by agreement). The language of performance of the contract is specified in the framework agreement and the public contract each time in a mini-competition, if it differs from the provisions of the framework agreement;
5.2.3. Delivery and receipt – complete delivery (all documentation in English (and other local languages by agreement, incl. architecture, tests, configurations, user manuals, act of receipt and equipment) to the beneficiary at its location in accordance with the terms and conditions of the mini-competition.
5.2.4. The contractor is obliged to provide a warranty of at least 24 months for the delivered goods from the date of delivery and receipt of the goods, including outside the European Union. The warranty offered must apply to all products.

5.3. Sample categories (by topic):
5.3.1. Switches and routers – Core/Distribution/Access-switching (L2/L3), QoS, EVPN/VXLAN (if applicable), SD-WAN;
5.3.2. Firewalls and perimeter – NGFW, WAF, DDoS protection, segmentation, VPN/SSL;
5.3.3. Wireless Network (Wi-Fi) – Controllers, APs, Guest Network, 802.1X/NAC, RF Planning;
5.3.4. Servers – rack/blade platforms, RAID, drivers, and firmware;
5.3.5. HCI and clusters – compute+storage clusters, HA, quorum, replication;
5.3.6. Storage – SAN/NAS/object; FC/iSCSI; tiering; Deduplication and compression;
5.3.7. Backup & Restore – Backup Appliances & Software, Cataloging, DR Samples;
5.3.8. Virtualization – VMware/Hyper-V/Proxmox; Resource Management, vMotion/Live Migration, DRS/HA;
5.3.9. Container platform nodes – Kubernetes *workers*/registries, image scanning, and runtime protection (in cooperation with security solutions);

5.3.10. Remote access/PAM/bastion – private access management, session recording and audit;
5.3.11. IDS/IPS/NDR – sensors, TAP/SPAN, rule sets and signatures, integration with SIEM;
5.3.12. Loaders/Load Balancers – L4/L7 load balancing, health checks, SSL offload;
5.3.13. Timing and naming services – NTP/PTP, DNS/DHCP, Log and Synchronization Services;
5.3.14. Management and monitoring – NMS/APM, log and metric dashboards, alerts, CMDB binding;
5.3.15. Racking & power – Racks, UPS/PDU, Cabling/Optics, Labeling, Physical Security & Access;
5.3.16. Optics & media – SFP/SFP+/QSFP, DAC/AOC, FO terminators & patches.