



EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

European Union Agency for Cybersecurity (ENISA)

Call for tenders ENISA/2025/OP/0001 (F-OSA-25-T02)

**IMPLEMENTATION OF SINGLE REPORTING
PLATFORM**

Open procedure

**TENDER SPECIFICATIONS
Part 2: Technical specifications**

1 Contents

- 1 Contents 2
- 1. Introduction..... 4**
 - 1.1 General..... 4**
 - 1.2 Additional Information..... 4**
- 2 Technical Description 5**
 - 2.1 Purpose and Context of the Tender..... 5**
 - 2.1.1 Purpose..... 5**
 - 2.1.2 Services to be Provided..... 5**
 - 2.1.3 Minimum requirements of CRA SRP 9**
 - 2.1.4 Core Features 12**
 - 2.1.5 Implementation standards 14**
 - 2.1.6 Estimated Framework Contract Value and duration..... 15**
 - 2.1.7 Place of Delivery of Services and Intra-Muros Activities..... 15**
 - 2.2 Technical Requirements 16**
 - 2.2.1 Users 16**
 - 2.2.2 Users Roles and Access Control..... 16**
 - 2.2.3 Application Architecture 17**
 - 2.2.4 Security 19**
 - 2.2.5 Hosting 20**
 - 2.2.6 Performance 20**
 - 2.2.7 Availability and Reliability 20**
 - 2.2.8 Maintainability 21**
 - 2.2.9 User Interface (UI) and User Experience (UX) 21**
 - 2.2.10 Auditing and logging capabilities 22**
- 3 Technical documentation to be submitted 22**
- 4 Main use-cases 22**
 - 4.1 Manufacturer registration 22**
 - 4.2 Volunteer registration..... 23**
 - 4.3 Manufacturer registration validation 23**
 - 4.4 CSIRT re-assignment 23**
 - 4.5 Manufacturer initial report submission..... 24**

4.6	Volunteer initial report submission	25
4.7	Submission updates	25
4.8	Manufacturer user dashboard & profile	26
4.9	Voluntary reporting user dashboard & profile	26
4.10	CSIRT dashboard	27
4.11	ENISA dashboard	27
4.12	Report processing	27
4.13	Report dissemination	28
4.14	Automatic notifications	28
4.15	Analytics and reporting portal	29
4.16	ENISA admin portal	29
5	Scenarios	29
6	Financial Offer	30
7	Ordering and services modalities	30
7.1	Reporting and Deliverables	30
7.2	Contract Management	31
7.3	Other Requirements	31
7.3.1	Costs involved in preparing and submitting a tender	31
7.3.2	Use of Language	32
7.3.3	Remuneration and payment modalities	32
7.3.4	Payment Arrangements	32
7.3.5	Protection of personal data	32

1. Introduction

1.1 General

The European Union Agency for Cybersecurity (ENISA) was established by the European Parliament and the Council Regulation (EU) No 2019/881 of 17 April 2019 (OJ L 151/15, 07.06.2019). ENISA is actively contributing to European cybersecurity policy, in order to support Member States and European Union stakeholders to support a response to large-scale cyber incidents that take place across borders in cases where two or more EU Member States have been affected. This work also contributes to the proper functioning of the Digital Single Market. Further information about ENISA can be obtained on its website: www.enisa.europa.eu. In the context of the Cyber Resilience Act¹ (CRA), ENISA has received the responsibility of establishing a Single Reporting Platform (CRA SRP) to fulfil the reporting requirements described in articles 14 through 17 of the regulation. The day-to-day operations and maintenance of CRA SRP shall be also managed by ENISA.

1.2 Additional Information

The Cyber Resilience Act was published in the Official Journal of the EU on 20 November 2024 and entered into force on 10 December 2024. The Cyber Resilience Act introduces mandatory cybersecurity requirements for hardware and software products with digital elements, throughout their whole lifecycle. A key element of the Cyber Resilience Act is the development and operation of a single reporting platform (CRA SRP), which would allow manufacturers to securely report actively exploited cybersecurity vulnerabilities in their products and severe incidents having an impact on the security of those products, and thus contribute significantly to raising the level of security for anyone using such products, including critical infrastructures, industry, public administrations, and consumers. In addition to mandatory reporting, manufacturers as well as other natural or legal persons may notify any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements on a voluntary basis to a CSIRT designated as coordinator or ENISA using the CRA Single Reporting platform (CRA SRP). In the same vein, they may also notify any incident having an impact on the security of products with digital elements as well as near misses that could have resulted in such an incident. The architecture of the single reporting platform shall allow Member States and ENISA to put in place their own electronic notification end-points. In line with the Cyber Resilience Act, the reporting obligations for manufacturers will apply from 11 September 2026. The establishment, management, and maintenance of the day-to-day operations of the single reporting platform will be done by ENISA.

IMPORTANT: The final delivery date for the development and implementation of the Platform, in compliance with CRA's requirements, shall be no later than July 1st, 2026,

¹ <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>

unless otherwise specified by the contracting authority. All documentation submitted as part of the proposal must explicitly refer to the release of the fully operational Platform by the deadline specified above.

2 Technical Description

2.1 Purpose and Context of the Tender

2.1.1 Purpose

ENISA with this tender seeks the build-up of a turnkey solution to implement CRA SRP which must support all relevant functionality required by the CRA and respective (planned) delegated/implementing acts. The architecture and implementation of the platform, shall be future proof and support future integration with incident and vulnerability reporting systems and requirements in NIS2 Directive² and DORA³ regulations.

For the initial implementation, the CRA SRP must be able to support notifications as referred to Article 14(1) and (3) and Article 15(1) and (2) of CRA. The architecture of the CRA SRP shall allow Member States and ENISA to put in place their own electronic notification end-points. Establishment of the CRA SRP is referred in Article 16 of CRA.

CRA SRP might be implemented as a bespoke solution as well as adapting existing solution.

2.1.2 Services to be Provided

Realization and Implementation of CRA SRP. Under this framework contract ENISA may request support from the prospective contractor following groups of services:

- design and secure implementation of CRA SRP including analysis phase (validation and further development and detailing of use cases and requirements) complying with the minimum requirements to fulfill regulatory obligations of CRA;
- deployment (service transition) and operationalization (service operation) of the platform in production (including high availability requirements);
- implementation of additional features and capabilities not included in the initial requirements including for other systems related to overall incident and vulnerability reporting;
- provide operational maintenance of the code base as well of the infrastructure⁴

² <https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng>

³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554>

⁴ Operation and maintenance of the infrastructure depends on the deployment and hosting methodology and decision.

- other tasks related to implementation of CRA SRP (e.g., testing, implementing change requests)

The following chapters describe requirements, expected functionality and main use cases of CRA SRP.

To fulfil the services included in this framework contract, the contractor must make available the following indicative profiles depending on the requests in the specific contracts. Profiles should be available at the Mid-level (relevant education, at least 3 years of professional job experience in the specific profile) or Senior level (relevant education, at least 5 years of professional job experience in the specific profile, and project management or team lead skills). The expected contribution to service delivery throughout the entire project is 60% from Mid-level profiles and 40% from Senior-level profiles. The distribution of Senior and Mid-Level profiles, as well as the expected fraction of total service delivery planned for each individual profile as indicated in *Annex 6*, may vary in specific contracts depending on the needs of the Contracting Authority:

Profile	Responsibilities/Tasks	Education	Skills and Knowledge
Project manager	Plan and oversee project execution within scope, budget, and timeline.	Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Business Administration, Computer Science, Computer Engineering or equivalent	Leadership, Communication, Project Planning, Risk Management, Adaptability and flexibility, Team management, Budget management, Task assignment
Solution architect	Design and configuration of software for particular business process or task	Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Information Technology, Software Engineering or equivalent	Understanding of technologies (e.g. databases, networking, security), architecture patterns and design principles, provide technical solutions, resolve complex technical problems
Network or infrastructure architect	Design of the hosting and infrastructure environment	Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent	Understanding of network protocols, network topologies, and network security concepts. Ability to propose optimal network solutions, ability to understand, diagnose and troubleshoot network problems
Software architect	Design solution architecture for scalability,	Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications	Understanding of software design principles, proficiency in software development methodologies,

	reliability, and security. Define integration patterns for various technologies. Oversee system architecture compliance with industry best practices to ensure security, performance and scalability;	Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent	propose solutions on complex technical issues, draw cybersecurity architectural and functional specifications, Knowledge in event-driven architecture and API gateway design. Proficiency in database design and schemas. Knowledge of 3-tier architecture and microservices.
Business analyst	Elicit and document business and technical requirements. Analyze processes and propose IT solutions.	Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Business Administration, Computer Science, Computer Engineering or equivalent	Ability to gather and analyze business needs, model processes and develop use cases, understanding of business processes and industry best practices, formation of requirements (regulatory and business ones). Familiarity with user-centered design principles and technologies. Good knowledge of analysis/modelling tools and techniques. Knowledge of software development methodologies.
Software developer	Develop, deploy, and maintain application/software solution according to requirements	Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent	Proficiency in one or more programming languages and relevant frameworks, understanding of software development methodologies and secure development lifecycle, ability to develop, implement, maintain, upgrade, and test software solutions. Knowledge of secure development practices and frameworks (OWASP, NIST). Expertise in DevSecOps.
Software tester	Design, execute, and manage test cases for applications and systems. Validate software functionalities,	Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent	Understanding of various testing types (e.g. unit testing, integration testing, system testing, user acceptance testing), knowledge of test case design techniques and proficiency in test management tools, automation testing and

	<p>integrations, and performance.</p> <p>Perform regression, stress, and security testing on applications.</p> <p>Reporting of test results.</p>		<p>security testing. Capability to persevere in retesting solutions</p>
Security architect	<p>Designing and implementing secure solutions</p>	<p>Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent</p>	<p>Understanding of security concepts and technologies. Knowledge of security standards and regulations. Ability to analyze threat intelligence and identify potential security risks. Ability to draw cybersecurity architectural and functional specifications, develop security and privacy requirements, identify effective solutions, Understanding of security and privacy by design and by default. Strong understanding of security frameworks (e.g., ISO 27001, NIST).</p>
System administrator	<p>Installation, configuration, maintenance, hardening and patching activities of hardware and software components of the platform including DB configuration, maintenance and optimization.</p>	<p>Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering or equivalent</p>	<p>Knowledge of configuration, and maintenance of hardware and software components of IT solutions. Understanding of relevant technologies and best practices. Develop and implement strategies for data backup and recovery,</p>

IT Maintenance and Problem Management Services:

The contractor must ensure the all-time availability of the IT services necessary for the ongoing maintenance and management of a robust and user-friendly platform. The maintenance shall be provided during normal working hours on normal working days. The Contractor will also be responsible for managing the entire lifecycle of these IT services, ensuring the alignment of the

right processes, people, and technology so that the Contracting Authority can effectively meet its business goals and maintain business continuity of the platform across EU. The Contractor must ensure that the necessary resources are available for rapid implementation. The solution must be delivered on time to meet regulatory deadlines, ensuring that critical functionality is available as required while also guaranteeing iterative improvements. Additionally, the Contractor must be aware that after the launch of the CRA SRP, the platform must evolve based on user feedback, regulatory changes, and emerging business needs. For this reason, the contractor must have already in place the resources needed for incorporating additional functionalities. The Contractor must ensure that the necessary resources are in place to facilitate these adaptations, and no additional time prior to service delivery should be required to modify platform functionality once a change request has been required. The contractor must have a problem management strategy in place to systematically address bugs or any implementation issues that may arise during the realization of the building blocks as described in section 2.2.3, “Application Architecture”.

The following services are required in addition to the realization of the SRP platform:

- Investigating and diagnosing potential issues and bugs during the platform's development and subsequent maintenance phases.
- Identifying workarounds and determining the root causes of problems.
- Implementing solutions or fixes to eliminate known errors.
- Documenting applied workarounds or resolutions and communicating them with the Contracting Authority.
- Testing identified workarounds to ensure their suitability in resolving related incidents and or bugs.
- Proactive measures should be taken to improve the availability of services whenever it is cost-effective to do so.

For maintenance, the Contractor will conduct performance tuning activities to ensure the most efficient use of existing infrastructure. If the Contractor is unable to resolve the problem or identify a suitable workaround, or if the issue is found to be linked to another system, it should be escalated to the Contracting Authority's point of contact without delay. The contractor is responsible for assessing the need for maintenance services independently when a bug, error, or problem is identified, or upon the contracting authority's request.

2.1.3 Minimum requirements of CRA SRP

Language and Localization. English as the Primary Language: All platform interfaces, notifications, and communications must be provided in English. On a case-by-case basis, support for other languages will be based on user needs in particular on the end-points.

Geographic coverage: CRA SRP should be available to all EU Member States

The platform shall:

- 1) Enable manufacturers to notify actively exploited vulnerabilities contained in the product with digital elements simultaneously to the Computer Security Incident Response Team (CSIRT) designated as coordinator⁵ and to ENISA, based on the following requirements:
 - a) an early warning notification within 24 hours:
 - i) indicating the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;
 - ii) a vulnerability notification within 72 hours (*unless the relevant information has already been provided*), containing:
 - (1) general information about the product with digital elements concerned;
 - (2) general nature of the exploit and of the vulnerability concerned;
 - (3) corrective or mitigating measures taken;
 - (4) corrective or mitigating measures that users can take;
 - (5) level of sensitivity of the notified information;
 - iii) a final report, no later than 14 days after a corrective or mitigating measure is available (*unless the relevant information has already been provided*), containing:
 - (1) description of the vulnerability, including its severity and impact;
 - (2) information concerning any malicious actor that has exploited or that is exploiting the vulnerability;
 - (3) details about the security update or other corrective measures that have been made available to remedy the vulnerability.
 - 2) Enable manufacturers to notify severe incidents having an impact on the security of the product with digital elements simultaneously to the CSIRT designated as coordinator and to ENISA, based on the following requirements:
 - a) an early warning notification within 24 hours:
 - i) whether the incident is suspected of being caused by unlawful or malicious acts;
 - ii) indicating the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;
 - b) an incident notification within 72 hours (unless the relevant information has already been provided) containing:
 - i) general information about the nature of the incident;
 - ii) an initial assessment of the incident;
 - iii) corrective or mitigating measures taken;
 - iv) corrective or mitigating measures that users can take;
 - v) level of sensitivity of the notified information;
 - c) a final report within one month after the submission of the incident notification (*unless the relevant information has already been provided*) containing:
 - i) a detailed description of the incident, including its severity and impact;
 - ii) the type of threat or root cause that is likely to have triggered the incident;

⁵ Pursuant to Article 12(1) of Directive (EU) 2022/2555.

iii) applied and ongoing mitigation measures.

- 3) Enable the CSIRT designated as coordinator initially receiving the notification to request manufacturers to provide an intermediate report on relevant status updates about the actively exploited vulnerability or severe incident having an impact on the security of the product with digital elements.
- 4) Enable the CSIRT designated as coordinator initially receiving the notification to disseminate it via the single reporting platform to the CSIRTs designated as coordinators on the territory of which the manufacturer has indicated that the product with digital elements has been made available.
- 5) Enable, in exceptional circumstances and, in particular, upon request by the manufacturer and in light of the level of sensitivity of the notified information under Art 14(2), point (a), the CSIRT designated as coordinator initially receiving the notification to delay its dissemination for a period of time that is strictly necessary, based on justified cybersecurity-related grounds, including where a vulnerability is subject to a coordinated vulnerability disclosure procedure. The platform shall include functionality for the CSIRT to approve the delay of the dissemination and to inform ENISA about the decision to delay the dissemination and provide both a justification for withholding the notification as well as an indication of when it will disseminate the notification.
- 6) Enable manufacturers, in particularly exceptional circumstances, to indicate in the notification referred to in Article 14(2), point (b) of the CRA:
 - a) that the notified vulnerability has been actively exploited by a malicious actor and, according to the information available, it has been exploited in no other Member State than the one of the CSIRT designated as coordinator to which the manufacturer has notified the vulnerability;
 - b) that any immediate further dissemination of the notified vulnerability would likely result in the supply of information the disclosure of which would be contrary to the essential interests of that Member State; or
 - c) that the notified vulnerability poses an imminent high cybersecurity risk stemming from the further dissemination;

in such cases, the platform must make it possible that only the information that has been submitted by the manufacturer, the general information about the product, the information on the general nature of the exploit and the information that security related grounds were raised are made available simultaneously to ENISA until the full notification is disseminated to the CSIRTs concerned and ENISA itself.

The platform must enable ENISA, when it considers that there is a systemic risk affecting security in the internal market, to recommend to the initial recipient CSIRT that it disseminate the full notification to the other CSIRTs designated as coordinators and to ENISA itself.

- 7) Enable manufacturers as well as other natural or legal persons to notify on a voluntary basis any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements to a CSIRT designated as coordinator or ENISA.
- 8) Enable manufacturers as well as other natural or legal persons to notify on a voluntary basis any incident having an impact on the security of the product with digital elements as well as near misses that could have resulted in such an incident.
- 9) The architecture of the single reporting platform shall allow Member States and ENISA to put in place their own electronic notification end-points.
- 10) Enable the CSIRT designated as coordinator to prioritize the processing of mandatory notifications over voluntary notifications.

2.1.4 Core Features

The following section summarizes the core features of the platform. Additional information about service delivery and guidance for implementation will be provided following the awarding of the tender.

Regulatory Compliance

Regulation compliance: The platform must comply with the CRA and where available, its implementing and delegated acts, ensuring it meets the obligations set by the legislation.

Timely Handling of Submissions: The platform must ensure that reports and notifications are submitted and processed in accordance with the strict timeframes imposed by the regulation.

Non-Disclosure Requests: The platform must support manufacturers' ability to request non-disclosure of information for a specified period, which must be approved by the receiving CSIRT.

Ease of Use

Simplified Submission Process: The platform must allow manufacturers and voluntary reporters to submit reports easily, even if they are not pre-registered, without discouraging them from participating.

User-Friendly Interface: The platform must provide an intuitive and easy-to-use web-based interface for all users using best practices and recognized standards

Guidance for Voluntary Reporters: Voluntary reporters must be guided to select the appropriate CSIRT and submit their reports in a way that ensures relevant stakeholders receive the necessary information.

Efficiency in Report Handling

Efficient Case Management: The platform must support the creation of cases for each notification report, which can be tracked and managed by stakeholders, with appropriate notifications and case updates.

Automatic Notifications: Stakeholders must be automatically notified about significant events, such as the submission of new reports, updates to existing cases, and approaching or missed deadlines.

Re-assignment of Cases: If necessary, the platform must allow for the re-assignment of cases to a different CSIRT, either directly or via a broadcast request, to ensure the right CSIRT handles each case.

Data Integrity and Accuracy

Validation: CRA SRP will prioritize quick submission and basic validation (e.g., ensuring required fields are filled).

Reliable Data Submission: Manufacturers must be able to submit data in a structured format (based on Common Security Advisory Framework (CSAF) or software bill of materials (SBOM)), ensuring that the data submitted is accurate and complete to the best of their knowledge.

Duplication Handling: The system must handle potential duplication of submitted reports and identify cases where the same vulnerability is reported multiple times by different manufacturers or vendors.

Security and Data Privacy

Confidentiality: The platform must ensure that sensitive information, such as details about reported notifications, is securely stored and protected against unauthorized access or disclosure.

Data Retention Policies: The platform must adhere to data retention requirements, keeping relevant records for the mandated time periods while ensuring compliance with regulations.

Audit Trail: A comprehensive audit trail of all actions performed within the system must be maintained, ensuring that any changes to the reports, cases, or other relevant information are traceable.

Separation of environments: Test and production shall be separated and must not share any cryptographic material.

Open source and code auditing: The system should be available as Open Source (e.g., Apache 2.0 License) to allow the Member States to build trust and check the system for vulnerabilities.

Communication and Collaboration

External Communication: While direct communication between manufacturers and CSIRTs, or CSIRTs and impacted product users, will occur outside of the platform, the platform must allow for recording the fact that communication has occurred and enabling relevant stakeholders to change case statuses or send secure and authenticated notifications as necessary.

Transparency: The platform must provide clear visibility into the status of report cases and any actions taken, ensuring transparency for manufacturers, computer security incident response teams

(CSIRTs), and ENISA. Each party that is able to see a report is also able to retrieve that report in a structure, machine-processable format.

Notifications for Non-Disclosure Decisions: Manufacturers must be notified of the decision regarding their non-disclosure request, and the platform must track and record such decisions.

Support for Data Feeds and External Integrations

Data Feeds: The platform must provide feeds that allow subscribed CSIRTs to retrieve relevant data for further processing or integration with their own systems respecting access control and authorization rules

System-to-System (S2S) Integration: The platform must support S2S integrations for efficient communication and coordination between the platform and other systems used by stakeholders, (such as CSIRTs' ticketing and other systems) through well-defined API endpoints.

Scalability and Future Evolution

Scalability for Large-Scale Incidents: The platform must be able to scale quickly and handle increased workloads during large-scale incidents, ensuring it can handle high volumes of data and concurrent users.

Flexibility for Future Enhancements: The system must be designed to accommodate future enhancements, such as more sophisticated workflows, integration with case management systems, or additional validation rules, as requirements evolve over time.

Stakeholder and User Dashboards

Role-Specific Dashboards: Each actor must have access to a customized dashboard that presents the most relevant information and tasks for their role.

Data Search and Reporting: Users must be able to search, filter, and report on submitted data based on predefined criteria or through custom queries, enabling efficient data management and reporting.

Backup and Recovery and High Availability

Disaster Recovery: The platform must provide full backup and recovery mechanisms, ensuring that data can be restored within the required timeframes (RTO and RPO) in case of failure.

High Availability: The platform must ensure high availability through appropriate redundancy for all its components.

2.1.5 Implementation standards

The platform must be based on open standards and established methodologies. Examples of standards/methodology foreseen are listed below.

- Vulnerability Handling: Utilize the Vultron protocol as a guide for data handling and state management.
- Data Exchange Standard: Primarily use CSAF (Common Security Advisory Framework) in JSON format for data exchange.
- SBOM Support: Support SBOMs (Software Bill of Materials) but avoid becoming a manufacturer's primary SBOM repository.
- Identity Management: Implement robust identity management based on standards like OpenID Connect, SAML, and OAuth 2.0.
- Development: Adhere to DevSecOps practices, iterative development approach, and ENISA's architectural principles.
- Standardized reporting (e.g., STIX/TAXII)

The Contractor must guarantee that the platform delivered will not fail to execute its programming instructions due to defects in workmanship when properly installed. It shall be free from any deliberate mechanisms that leave it under the Contractor's control after being supplied to the contracting authority. It must meet the operating requirements, specifications, and characteristics specified in the Contractor's documents or outlined in the Framework contract. Throughout the entire implementation of the contract, the Contractor must ensure compliance with and full respect for the “Quality Assurance Management” documentation specified in Section 3.

2.1.6 Estimated Framework Contract Value and duration

The total budget is estimated at **€ 11 000 000 (Eleven Million Euros)** over the period of **4 (Four) years**.

2.1.7 Place of Delivery of Services and Intra-Muros Activities

The services shall be delivered either at the contractor's premises (extra muros) or at ENISA's offices and locations (Athens 70% or Brussels 30%) (intra muros). The contractor must be capable of providing services at ENISA's offices in Athens or Brussels, upon request of the Contracting Authority. Any tasks carried out by the contractor's personnel outside the contractor's premises will be considered intra-muros activities. As specified in **Annex 6**, In calculating the total price for price point determination, a weighted approach of 70% for extra muros and 30% for intra muros is applied. The intra muros rates, shall be inclusive of all subsistence expenses, including but not limited to meals, local transportation (such as transport to and from the airport or station within the place of performance), accommodation, sundry expenses and insurance.

Return trips (going to ENISA's offices and locations (Athens or Brussels and returning to contractor's premises) must not be included in the intra muros rates as presented in **Annex 6**, as such expenses are eligible for reimbursement. ENISA will reimburse travel costs in accordance

with Commission Decision C(2021)35 (as amended Commission Decision C(2024)5405)⁶ which defines the use of unit costs for the reimbursement of eligible travel costs under any action or programme financed by the Union budget during the 2021-2027 MFF period. For the purposes of declaring costs, the contractor is required to submit document (s) listing all profiles that performed intra muros activities outside the contractor's premises. The document(s) must be sent to the ENISA Project Manager within three weeks of the conclusion of the intra muros activity for which reimbursement is requested. The document must clearly specify the departure and return points for each profile, along with the corresponding distance (in kilometers).

For each profile, the ticket(s) or proof of actual travel must be attached. The document must be submitted in a PDF format and provide details for all team members involved in activities outside the contractor's premises. Only complete and accurate documentation will be considered for reimbursement. Any discrepancies or incomplete submissions may result in delays or rejection of the reimbursement request.

2.2 Technical Requirements

This section provides technical requirements and reference architecture foreseen for the implementation of the platform. Additional architectural and implementation details, if needed, will be provided during the implementation of the FWC and specified at the process for 'Request for Services' related to the execution of the specific contracts.

2.2.1 Users

Single Reporting Platform must support at least the following user groups:

- Representatives of Manufacturers and/or Vendors
- ENISA (Business users and administrative users)
- CSIRTs users
- Legal or natural persons reporting on a voluntary basis
- API clients

Additional user groups can be specified by ENISA in the course of implementation. The solution shall provide flexible implementation of user groups on a case-by-case situation. The solution must provide support for interfacing with existing systems of MS stakeholders.

2.2.2 Users Roles and Access Control

Users must be registered, authenticated and appropriately authorized before using the platform. The solution must support notification submissions for manufacturers or other legal or natural persons that have not been pre-registered but allow for quick registration at the time of the

⁶ [Calculate unit costs for eligible travel costs - European Commission](#)

submission. Manufacturer, ENISA and CSIRT registered users must utilize Multi-Factor Authentication for accessing the platform. The platform must support data-level authorization rules, ensuring that users only have access to information relevant to their role.

2.2.3 Application Architecture

The platform must be architected using a multi-tier architecture pattern with identifiable components/modules that handle the different aspects of the different concerns, allowing for future expansion (e.g hub-and-spoke or fully distributed approach).

Regarding data storage, the tenderer must be able to support diverse approaches and technologies, ensuring reliable data management and reduced complexities. Some building blocks might need to support a decentralized architecture according to the needs of Member States.

Tenderer must include their proposal of high- and low-level architecture of platform in their offer.

The identified building blocks of the platform are⁷:

- Identity management
- Web user interface (WebUI)
- CRA SRP backend
- Malware scanner engine
- Notification engine
- Scheduler engine
- Datastores
- Reports datastore
- Attachments/binary content datastore
- CRA SRP Administration server environment
- CRA SRP server environment

⁷ Additional building blocks can be proposed by the contractors as needed for correct implementation of the business and technical requirements to be agreed with ENISA once the contract is awarded

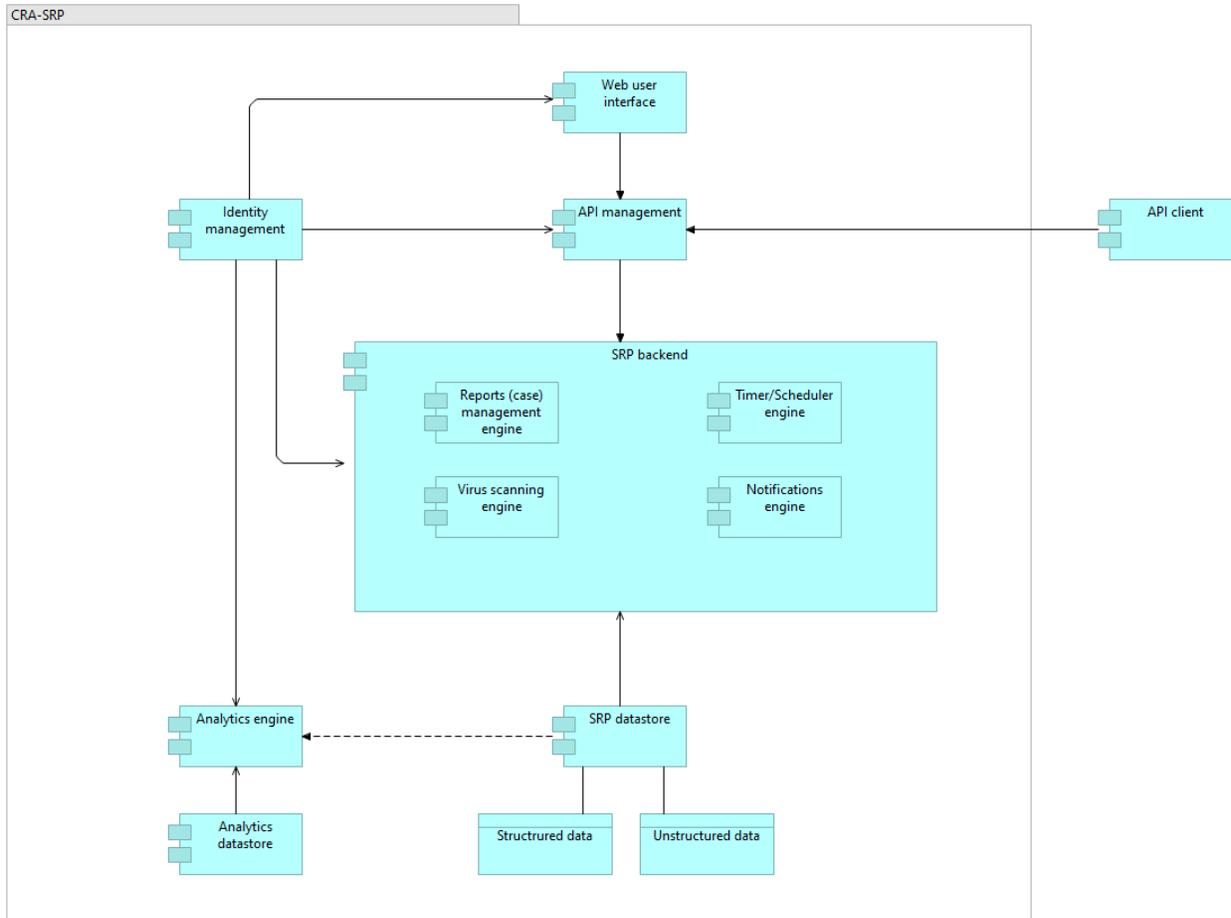


Figure 6: Indicative Solution architecture diagram (building blocks)

The interfaces/endpoints of the solution are the web user interface, available for all users of the platform with different functionalities based on the role of each user and the API management building block, through which the relevant API is exposed for CSIRT API clients to utilize. This functionality will implement the end-points capabilities as described in the CRA regulation.

The identity management building block is responsible for authentication of end-users and API clients and the provisioning of information relevant to authorization of operations in the platform. It must hold information about all types of users of the platform.

The API management building block is responsible for providing the exposed functionality of the system in the form of API for consumption by endpoints of the solution. It is also responsible for the validation of identity and application of authorization rules, so that requests to the system are allowed or blocked according to rules. It can also provide a first point of auditing traces.

The SRP backend is the core of the platform, providing all functionality necessary (apart from data analytics) exposed in the form of APIs that are consumed by the API management building block. The internal building blocks providing functionality can be listed as:

- Reports (case) management: This block provides the core functionality of report handling
- Timer/scheduler engine: Provides functionality related to time, e.g., trigger timers when a report is submitted to the platform, trigger notifications on predefined elapsed periods of time etc.
- Notification engine: Provides notifications functionality, either to human or system users

The SRP datastore is the building block for storing data, structured and unstructured, related to the platform. It serves the SRP backend through which it is accessed to ensure that any information entered via the interfaces is persistent.

Analytics engine & datastore: Building blocks responsible for further analysis of data stored in the main SRP datastore.

The final propose architecture must take into account the requirements to implement delayed notification.

2.2.4 Security

Due to the sensitive nature of information that the platform manages, security standards must be applied across all components of the platform to their respective extent

Data encryption

- Application-level encryption of sensitive information is mandatory (at rest)
- Encryption across communication channels is mandatory (in transit)

Encryption must be implemented using common industry standards and specifications applying most recent versions and highest level practicable.

Secure coding practices must be adopted ensuring the resilience of the platform regarding input validation, authentication and authorization, data encryption, secure communications and error handling/logging etc.

Integration of security within CI/CD pipeline, secure code inspection and review are expected to be conducted frequently within the software development lifecycle. Penetration testing must be performed on regular basis as releases are provided and at least before the final candidate release.

Contractor must also identify and implement⁸ the necessary infrastructure security controls.

Contractor must be aware that ENISA has the right to perform penetration testing and code review by third parties as required.

The platform must be architected using a multi-tier architecture pattern with identifiable components/modules that handle the different aspects of the different concerns.

2.2.5 Hosting

The services included in the platform will be hosted as following:

- Central services (such as back-end of identity management): hosted by ENISA
- Front-end services (such as WebUI): can be hosted by ENISA or hosted within Member State environment

The platform services must be built such as to be as interoperable as possible with underlying infrastructure stack used by ENISA. Additionally, the platform should be built in a way to implement a different hosting schema (for example if the system is transitioned to a distributed architecture).

2.2.6 Performance

Contractor must propose optimal values of standard response times for page load and API calls. System Setup and Architecture must support scalability (either horizontal or vertical). Load must be continuously monitored and capacity must be automatically adjusted based on real-time usage requirements.

2.2.7 Availability and Reliability

The solution and infrastructure hosting must implement high availability, ensuring continuous access to the system without significant downtime and be able to identify and mitigate DoS or any other similar type service disruption events.

The solution must be scalable in order to handle load spikes, especially in the event of a large-scale incident resulting in mass submissions.

The system shall provide mechanisms for complete data backup and restoration, according to the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) set by ENISA.

⁸ Depending on the specific infrastructure decided to host the platform services

The platform must support load balancing to distribute traffic across servers and prevent bottlenecks during high demand periods.

The system design must be modular with a clear separation of concerns at the data storage, service and the API layer. The adoption of open standards shall work towards the singular goal of interoperability.

The system must be highly configurable to accommodate changing business rules.

There must be no single point of failure including redundant hardware components, load balancing, support for failover.

Availability of at least 99.75% (or less than 22 hours of unavailability per year). Unless the system is non-operational, the system shall present the user with a notification informing them that the system is unavailable.

2.2.8 Maintainability

Software Code with version control must always be pushed to ENISA GitHub. User manuals, technical documentation (installation, configuration and maintenance guidelines) including code analysis reports are required deliverables .

2.2.9 User Interface (UI) and User Experience (UX)

Submission process interface must be intuitive and user-friendly.

The platform must provide dashboards, tailored to the role of each end-user, through which the functionalities can be provided in a simple and efficient manner. The dashboards must allow either for actioning of information (e.g., submitting a new report, appending information on an existing case, changing the status of a case, manual notifications etc.) or for providing access to information either through searching or through selecting predefined criteria thus allowing for information retrieval and reporting.

Overall, the look and feel of the application must ensure easy navigation and consistency. Standard design patterns using bars, side bars and breadcrumbs must be followed. Search functionality with filtering upon various elements must be provisioned. User needs must be addressed ensuring efficiency and minimal friction. Compatibility with well-known and commonly used browsers is required.

2.2.10 Auditing and logging capabilities

The platform must provide appropriate logging and auditing of both system and business operations. The information kept must be protected against unwanted disclosure and modification, ensuring that access to this information occurs through a controlled and centralized manner based on end-user roles. Auditing and logging agents must ensure full visibility in all user interaction and system events monitoring. The platform must maintain detailed logs for all operations, with secure access control to prevent unauthorized access to sensitive audit information.

All logs of all components must be centrally stored to enable easy analysis.

3 Technical documentation to be submitted

- Project Charter (purpose, scope, timeline, roles and responsibilities)
- WBS (work breakdown structure)
- Project Plan with key milestones (tenderer should assume that the contract award by July 2025 and implementation to be finalized by July 2026)
- Description of working method and working arrangements of the FWC and specific contracts
- Change Management
- Project Risk Management
- Project Team structure (roles and responsibilities, profiles (describing capacity and capabilities of personnel involved in project))
- Hosting and Deployment Strategy
- Software Development Plan
- Quality Assurance Management
- Stakeholder Communication Management
- Service Level Requirements proposal
- Description of scenarios as indicated in section 5

The documentation related to the above bullet points should not exceed 60 pages.

4 Main use-cases

Below are the indicative primary use cases for the platform, identified based on the initial assessment performed.

4.1 Manufacturer registration

Actors: The primary representative of the manufacturer.

Main Flow: The representative inputs the manufacturer's details in the registration form. During the form submission, it is mandatory to specify (or assign) the CSIRT designated as coordinator of the manufacturer.

Postconditions: The registration form is ready for validation by CSIRT.

Decisions: Platform will support multiple representatives (recommended minimum 2 users) for each manufacturer. One account will be the main submitter, while another will be used as a back-up.

4.2 Volunteer registration

Actors: A Volunteer (Legal or natural person)

Main Flow: The Volunteer completes the registration form. During the form submission, it is mandatory to specify the CSIRT designated as coordinator or ENISA to be the recipient of the report.

Postconditions: The registration form is ready for validation by the CSIRT or ENISA, when relevant.

4.3 Manufacturer registration validation

Actors: CSIRT authorized user

Precondition: An unverified registration form is completed in the system and assigned to CSIRT designated as coordinator, making it "owned" by that specific CSIRT.

Main Flow: The CSIRT user reviews and validates the vendor registration form. If the provided information is sufficient to validate the vendor, they “confirm” the manufacturer registration to the system. Otherwise, they reach out to the manufacturer outside the system (e.g., via email or phone) to request additional details or clarifications.

Postconditions: The manufacturer is either flagged as valid or the registration form is rejected.

4.4 CSIRT re-assignment

Actors: CSIRT authorized users

Precondition: An unverified registration form is completed in the system

Main Flow: The CSIRT user reviews the Manufacturer/Volunteer registration form and, if they determine it must be managed by a different competent authority a reassessment happens in the system, and a notification is sent to the newly designated CSIRT. This notification refers to the non-validated registration and invites the other CSIRT to take assignment of the submission. If the invited CSIRT accepts the reassignment, the manufacturer is allocated to the new CSIRT.

Solution must support:

- Direct re-assignment, in case the CSIRT received the report is aware of the relevant CSIRT to handle it
- Broadcasting of need to re-assign, in case the CSIRT received the report is not aware of the relevant CSIRT to handle it
- Self-re-assignment, after being notified by the broadcasting function

Postconditions: The non-verified registration form is assigned to a new CSIRT. The manufacturer is notified about the re-assignment.

4.5 Manufacturer initial report submission

Actors: Representative of the manufacturer

Precondition: The representative of the manufacturer may already be registered; otherwise, a wizard-like UI flow must guide the user through the registration process before submitting the report.

Main Flow: The system supports two types of reports:

- Actively Exploited Vulnerabilities (AEV)
- Incidents impacting the security of the product with digital elements (INC)

The user fills out the report after selecting the report type. They may save a draft version before submitting the report to the system. The report is automatically assigned to the CSIRT designated as coordinator as appointed by the submitter and, as a rule, simultaneously to ENISA, as per Article 14(1) of the CRA.

Depending on the report type, different fields are displayed. The user may attach accompanying files.

User may flag the report for non-disclosure for a specified period of time (“embargo”). The form will allow uploading of attachments.

The manufacturer must be able to select the countries which the manufacturer is aware that the affected product has been made available.

Postconditions: A report with the status "Received" is recorded in the system. An identifier is assigned and reported back to the submitter. The user is able to download that report.

4.6 Volunteer initial report submission

Actors: Volunteer (Legal or natural person)

Precondition: The volunteer may already be registered; otherwise, a wizard-like UI flow must guide the user through the registration process before submitting the report.

Main Flow: The system supports the following types of reports:

- Any vulnerability contained in a product that could affect the risk profile of it
- Any cyber threats that could affect the risk profile of a product
- Any incident or any near misses that could have resulted in an incident having an impact on the security of a product

The user fills out the report after selecting the report type. They may save a draft version before submitting the report to the system. The report is automatically assigned to the CSIRT designated as coordinator as appointed by the submitter.

Depending on the report type, different fields are displayed. User may attach accompanying files

Postconditions: A report with the status "Received" is recorded in the system. An identifier is assigned and reported back to the submitter. The user is able to download that report.

4.7 Submission updates

Actors: Representative of the manufacturer

Precondition: The manufacturer's representative registered on the platform must have already submitted an initial report and received the relevant identifier.

Main Flow: The user selects the identifier of the previously submitted initial report and selects the option of submitting an update. The update could be of the different types per initial report type, as stated in the reporting obligations of the manufacturer.

The user fills out the necessary information and may save a draft version before submitting to the system. Depending on the report type, different fields are displayed. User may attach accompanying files.

Information that can be retrieved by the initial report is pre-filled.

The user can additionally provide comments addressing requests originating from the assigned CSIRT.

Postconditions: A new submission report is created and linked with the initial report submitted (under the same identifier). A notification is sent to the designated CSIRT and ENISA for the new submission. The user is able to download that report.

4.8 Manufacturer user dashboard & profile

Actors: Representative of the Manufacturer

Precondition: The manufacturer representative must be registered in the system.

Main Flow: Once the user logs into the system, a dashboard-like page is displayed along with the user profile. This page serves as the main entry point to the reporting system, allowing users to query, view, create new reports, and check notifications.

The dashboard includes the following panels:

- Reports
- Notifications
- Manufacturer Profile

Users can apply filters and sorting to these panels, navigate to detailed reports, update comments, and view notifications. When a comment is added, a notification is sent to the assigned CSIRT.

Manufacturer representatives have access to reports associated with their respective manufacturers. Any modifications made to reports must be validated by the assigned CSIRT and ENISA. As part of this process, the two users allocated per manufacturer can view/edit the submission. The dashboard must highlight time left for next update and explicitly indicate a potential delay.

4.9 Voluntary reporting user dashboard & profile

Actors: Volunteer (Legal or natural person)

Precondition: The volunteer must be registered in the system.

Main Flow: Once the user logs into the system, a dashboard-like page is displayed along with the user profile. This page serves as the main entry point to the reporting system, allowing users to query, view, create new reports.

The dashboard includes the following panels:

- Reports
- Volunteer profile

Users can apply filters and sorting to these panels, navigate to submitted reports and potentially provide comments. When a comment is added, a notification is sent to the assigned CSIRT or, as the case may be, ENISA.

4.10 CSIRT dashboard

Actors: Authorized CSIRT users

Main Flow: After a CSIRT user logs into the system, a dashboard page is displayed. The dashboard includes the following panels:

- Reports
- Notifications
- Manufacturers

Users can apply filters and sorting to the panels, as well as navigate to view report details, make updates, and manage notifications. Reports that have not been disseminated are accessible exclusively to users belonging to the assigned CSIRT.

4.11 ENISA dashboard

Actors: ENISA authorized users

Main Flow: After ENISA user logs-in a dashboard page appears. Dashboard panels include - Reports User can apply filter to panels and navigate to report details and notifications. ENISA users will have read only access to disseminated reports.

A differentiation between disseminated and reports under embargo is applied, with different level of information for each type.

4.12 Report processing

Actors: Authorized CSIRT user, where the report is assigned to.

Precondition: A report has been recorded.

Main Flow: The CSIRT user processes the report based on its status. Depending on the situation, the user may contact the manufacturer by adding comments within the system or outside the system (e.g., via email or phone) to request additional information. If a report has been flagged for non-

disclosure for a specified period of time (“embargo”), the CSIRT user must receive a justification from manufacturer for further processing.

After processing the report, a status transition must be submitted. Indicative statuses include:

- R: Received
- V: Valid
- A: Accepted
- I: Invalid
- D: Deferred
- C: Closed

Indicative sub-statuses include:

- R: Request for information
- P: In progress
- U: Unassigned
- S: Disseminated

Postconditions: The status transition is recorded.

After each transition or comment, a notification is sent to the manufacturer.

4.13 Report dissemination

Actors: Authorized CSIRT user.

Precondition: A report has been received and validated.

Main Flow: The CSIRT user, unless embargo is requested, proceeds in selecting dissemination of the report to the CSIRTs of Member States to the territory of which the manufacturer has indicated that the product has been made available.

Postconditions: All designated CSIRTs receive notifications about the new report and the report becomes accessible to them. If the report was previously under embargo, ENISA now also receives the full content of the report.

4.14 Automatic notifications

Actors: CRA SRP service account/daemon

Main flow: Based on the defined obligations, the CRA SRP will emit notifications to stakeholders. Notifications will be sent in the following forms:

- Emails (PGP)
- Entries in the dashboard's notification panel

4.15 Analytics and reporting portal

Actors: ENISA users

Main Flow: Reporting

4.16 ENISA admin portal

Actors: ENISA admins

Main Flow

- Maintain ENISA Users
- Maintain CSIRT network users

5 Scenarios

Scenarios must comply with requirements and use cases listed in the specifications. For the purposes of developing the scenario, the tenderer must assume an implementation time for the platform of **no more than 1 year from the start of service delivery**.

There are two necessary Scenarios to be represented. **For the implementation of the Scenarios below, it is necessary to take into account the building blocks specified in Section 2.2.3: Application Architecture:**

- Scenario 1 - Implementation of identity management block
- Scenario 2 - Implementation of SRP backend block

Scenarios must be assessed, and a technical description of how you would implement and deliver the required building block must be provided. Scenarios are required as part of your technical offer and will be assessed exclusively as a qualitative award criterion.

The actual projects to be awarded to the successful contractor will have a much more detailed level of technical specifications. Please note that:

- Failure to provide a technical description for scenarios will lead to rejection of the tender
- Scenarios are provided solely as examples of services and do not constitute an exhaustive representation of all services required under the FWC
- The proposal must take into account all the requirements listed in the tender specifications and support authentication for all kinds of CRA SRP users. Block must ensure at least:
 - implementing or robust authentication mechanisms,

- enable granular control over access to the system
- support identity management
- support integration with existing identity providers
- adhere to relevant security standards and regulations

6 Financial Offer

Throughout the entire FWC duration and its implementation via the respective SCs, the estimated workload, measured in 'person-days' per profile, is outlined as percentages. The tenderer must indicate the rates per profile (mid-level and senior profiles, Extra and Intra Muros (Athens & Brussels)).

Furthermore throughout the entire project the involvement estimated to be :

- 60% from Mid-level profiles and 40% from Senior-level profiles
- 70% for extra muros and 30% for intra muros
- 70% Athens and 30% Brussels for intra muros

The final price will be calculated as the cost of the above as specified in **Annex 6**. As the figures are percentages, a reference point of 1000 person-days (indicative number of days) will be used to facilitate their conversion into euro amounts reflecting the estimated work required throughout the 4-year FWC.

7 Ordering and services modalities

After the signature of the FWC the contracting authority will send a 'Request for Services' on a specific subject matter to the 1st in cascade Framework contractor. The 'Request for Services' offer will contain all the details regarding the technical content of the request.

The Framework contractor will be required to respond within 7-14 working days with a detailed technical proposal, depending on the complexity of the project.

ENISA will evaluate the offer received. A Specific Contract will be concluded if the proposal is compliant with the specifications set in the Request for services.

7.1 Reporting and Deliverables

For all of the abovementioned services, the contractor must be able to:

- Deliver comprehensive reports including a Summary, Objective, Scope, Methodology, Findings and Recommendations.
- Deliver intermediate reports and presentations as required.

- Follow ENISA recommendations, guidelines and requirements regarding the abovementioned services.

7.2 Contract Management

The contractor is required to designate a contact person as the contract manager and provide their contact details to ENISA, along with a backup contact for correspondence related to services.

The contact person must be responsible for the overall management and administration of the framework contract. The contractor must provide an e-mail address and phone number through which all communication must be directed.

The contractor must ensure continuous service availability in Greece and Brussels (Monday to Friday, 09:00-17:00) by providing sufficient staff coverage to account for all holidays and absences.

The Contract Manager and the backup must be able to communicate fluently in the English language and will be responsible for all administrative aspects related to the contract execution, such as invoicing, payments and reporting. His/her main responsibilities will be to:

- Liaise with of ENISA;
- Receive and acknowledge ENISA requests for services in a timely manner and dispatch such requests appropriately;
- Ensure that ENISA's requests regarding the contract execution are performed within the deadlines indicated in the Framework Contract- Specific contract on implementation modalities;
- Coordinate service execution at all levels within contractor's remits;
- Act as first line support to all ENISA staff;
- Provide the necessary follow up to all inquiries;
- Manage all the matters relating to invoices and payments;
- Be responsible for solving any arising issues / delays regarding the provision of services;
- The presence of the Contract Manager or his/her backup is compulsory during working hours from Monday to Friday (from 09.00 to 17.00).

7.3 Other Requirements

7.3.1 Costs involved in preparing and submitting a tender

ENISA will not reimburse any costs incurred in the preparation and submission of a tender. Any such costs must be paid by the tenderer.

7.3.2 Use of Language

All communication during the implementation of the framework contract and the specific contracts must be carried out in English.

7.3.3 Remuneration and payment modalities

One or more invoices must be issued on completion of the services as described above. The invoice(s) must indicate the reference number of the FWC, the reference number of the Specific Contract, the service provided, period of reference and amount requested.

7.3.4 Payment Arrangements

Payments shall be carried out only upon completion services listed in the Specific Contract and according to the provisions of article I.6 of the FWC. The Intra-muros and Extra-muros rates shall be interpreted as daily rates, with one working day corresponding to eight (8) hours. The contractor's personnel is required to track their working hours using a timesheet. Upon completion of each assignment, the completed timesheet must be submitted to ENISA's Project Manager for prior approval before invoicing. ENISA shall only process payments for time that has been effectively worked and accurately recorded by the contractor.

7.3.5 Protection of personal data

Details on the protection of personal data are expressly set forth in the provisions of the Framework Contract.