FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

Frontex/OP/300/2019/SB

Multiple Framework Contract with reopening of competition for the provision of Software Development services

Annex II
Terms of Reference v.2

1. Terms and Definitions

The terms in the table below, appearing either in a complete or in an abbreviated form, when used in this document and its appendices, relating to the Technical Proposal, Financial Proposal and Draft Contract, shall be understood to have the following meaning. The part *General Terms and Conditions for Information Technologies Contracts* provides additional terms and definitions applicable to the mentioned documents.

Term	Abbreviation	Meaning
24/7/365	24/7	Used for defining services to be provided around the clock every day of a year when the differentiation of Normal and Extended Working Hours is not applied.
Azure DevOps	ADO	Frontex might use Microsoft Azure DevOps services for development environments and artefacts repository (DAR). These are cloud-based software development services which provide development collaboration tools including high-performance pipelines, free private Git repositories, configurable Kanban boards, and extensive automated and cloud-based load testing. For the on-premises platform, Azure DevOps Server (previously named Visual Studio Team Foundation Server) can be used. These services cover: - Boards (backlogs, sprints, work items) - Repos (git code repository) - Pipelines (builds, releases, environments) - Test Plans (cases, runs, reports) - Artefacts (packages, shared code)
Custom-developed software	CDS	Bespoke or custom-developed software is software which is commissioned, designed and developed specifically for Frontex.
Commercial Off-The-Shelf Software	COTS	A non-developmental and pre-built software that is both commercial and sold in substantial quantities in the commercial marketplace. It can be purchased, leased or licensed to the general public.
Customisation	customization	Tailoring of the out-of-the-box application using configuration and scripting that does not change the application's code, preserving at the same time the possibility to apply standard updates and new releases of the software.
Development artefacts repository	DAR	Central repository for code management, builds, automated test and other artefacts of software development as a back end to individual developers' environments. Frontex uses on-premises Microsoft TFS or ADO.
Development environment	LABS	Technical environment (network, systems, applications and related services, policies and practices) used by developers for development of the Main Product. It is composed of developers'

		individual local environments (virtual or physical) and central DAR.
Duration of the Assignment	ST LT	ST - Short Term, for 30 man-days or less in total LT - Long Term for efforts estimated for more than 30 man-days in total.
Extended Working Hours	EWH	Any working hours other than *Normal Working Hours*.
Fixed Price	FP	Fixed Price assignments as defined in the GTCITC.
Framework Contract	FWC	This Contract.
Frontex	FX	European Border and Coast Guard Agency
Frontex Headquarters	FX HQ	Frontex premises located in Warsaw, Poland.
Functional Requirements	FR	Requirements for the product which specify its behaviour and functions
General Terms and Conditions for Information Technologies Contracts	GTCITC	Contractual provisions applicable to this Contract.
Man-day	md	8 hours of work by one person. Typically, md is performed in the hours agreed with Project Manager and must include 30 minutes break that does not count towards the 8 hours of work.
Member State	MS	The European Union member state. This may include the Schengen Associated Countries as well.
Non-functional Requirements	NFR	Requirements for the product which reflect criteria that can be used to judge the operation of a system, rather than specific behaviours.
Normal Working Day	NWD	From Mondays to Fridays inclusive, excluding Frontex holidays. Frontex holidays usually cover Easter Break, 1-3 May, 9 May, Corpus Christi in June, Assumption Day in August 1 and 11 of November, last week of December and 1 day of January. Detailed list will be provided to the Contractor at the end of each calendar year.
Normal Working Hours	NWH	From 08:00 to 20:00 on normal working days
On-call duty	On-call	Defined period of readiness of the selected personnel on duty to undertake specific actions with regard to technical system in

		order to assure its continuity in business activities according to agreed service levels.
Open Source Software	OSS	Computer software that is available in source code form and is provided under a software license that permits users to study, change, and improve the software. Open source software is very often developed by communities in a public, collaborative manner where programmers create a program and make it available for others to use as well as modify the source code and to redistribute the modifications to the software user/developer community.
Out of the Box Software	OOTB	A ready-made software that meets a requirement that works right after installation without a special software development effort.
Personal Data		Shall have the same meaning as set out in the Regulation (EC) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC
Production environment	PROD	Technical environment (network, systems, applications and related services, policies and practices) used by end users for operational use for business purposes. PROD shall not be used for other purposes unless it is specifically accepted as an exception (e.g. for performance tests, penetration test).
Quoted Times and Means	QT&M	Quoted Times and Means assignments as defined in the GTCITC.
Quoted Unit of Work	QUW	Measure of work used by Frontex in software development organized in scrum in a particular SC. It is composed off all activities and efforts required for production of the product (Main Product and all other required deliverables and services) in scope of a defined sprint and all requirements and constraints set in this Specific Contract. QUW is measured in a defined number of User Story Points.
Scrum, Sprint, Sprint Review meeting, Sprint Planning meeting, Stand-up meeting, Sprint Retrospective meeting, Product Owner, Scrum Master, Scrum Development Team, Product Backlog, Sprint Backlog, Definition of Done,	Scrum	All the terms in this FWC follow the meaning commonly applied in Scrum Framework, as documented in the following reference: https://www.scrumguides.org/scrum-guide.html

Burn-down Chart, Velocity		
Schengen Associated Country	SAC	Countries which are associated members of the Schengen Area
Specific Contract	SC	Specific Contract as defined in the GTCITC.
Times and Means	T&M	Times and Means assignments as defined in the GTCITC
Training environment	TRN	Technical environment (network, systems, applications and related services, policies and practices) used to provide trainings to users. TRN shall not contain real PROD data.
User acceptance environment	UAT	Technical environment (network, systems, applications and related services, policies and practices) used for testing and acceptance of the Main Product.

2. Objectives

The objective of this Framework Contract is to provide Frontex with a capability for developing, integrating and supporting software applications for Frontex operational and administrative processes. The deliveries of services under this FWC will support Frontex in achieving goals and objectives set for Frontex in related Frontex Programmes of Work.

Frontex is seeking long term cooperation with maximum six Contractors who offer professional capability for software development in terms of professional resources, organized teams experience in delivering software, proven software development methodology and tooling at the highest possible maturity level as well as company experience in successful development of software in Fixed Price and Quoted Time and Means contracts.

Each individual Specific Contract will be related to one or more Frontex activities and will be covered by a project. That correspondence between the Specific Contract and the Frontex activity, and the project will be defined in the course of individual SCs.

3. Background

3.1. Frontex Tasks

Frontex, the European Border and Coast Guard Agency, promotes, coordinates and develops European border management in line with the EU fundamental rights charter and the concept of Integrated Border Management.

To help identify migratory patterns as well as trends in cross-border criminal activities, Frontex analyses data related to the situation at and beyond EU's external borders. It monitors the situation at the borders and helps border authorities to share information with Member States. The agency also carries out vulnerability assessments to evaluate the capacity and readiness of each Member State to face challenges at its external borders, including migratory pressure.

Frontex coordinates and organises joint operations and rapid border interventions to assist Member States at the external borders, including in humanitarian emergencies and rescue at sea. The agency deploys European Border and Coast Guard teams, including a pool of at least 1 500 border guards and other relevant staff to be deployed in rapid interventions. The members of the rapid reaction pool must be provided by Member States upon request by the agency. It also deploys vessels, aircraft, vehicles and other technical equipment provided by Member States in its operations. In addition, Frontex may carry out operations on the territory of non-EU countries neighbouring at least one Member State, in case of migratory pressure at a non-EU country's border.

Frontex, the European Border and Coast Guard, supports Member States with screening, debriefing, identification and fingerprinting of migrants. Officers deployed by the agency refer and provide initial information to people who need, or wish to apply for, international protection, cooperating with the European Asylum Support Office (EASO) and national authorities. It is the national authorities, not Frontex, who decide which person is entitled to international protection.

The agency assists EU Member States in forced returns of people who have exhausted all legal avenues to legitimise their stay within the EU. This help includes obtaining travel documents for the returnees by working closely with consular authorities of the relevant non-EU countries. It can also organise voluntary departures of nationals of non-EU countries who were issued return decisions by Member State authorities. Frontex also organises return operations on its own initiative and "collecting return operations", where returnees are returned with escort officers and transportation provided by their countries of origin. It has created several pools of return experts to be deployed in Member States when needed.

Frontex supports the cooperation between law enforcement authorities, EU agencies and customs at sea borders. Vessels and aircraft deployed in its operations also collect and share information relevant to fisheries control, detection of pollution and compliance with maritime regulations. The agency works closely with European Fisheries Control Agency (EFCA) and European Maritime Safety Agency (EMSA) to implement multipurpose operations. In these operations, vessels and aircraft deployed for border surveillance can also be used for fishing and environmental monitoring.

Frontex focuses on preventing smuggling, human trafficking and terrorism as well as many other cross-border crimes. It shares any relevant intelligence gathered during its operations with relevant national authorities and Europol.

The agency is the centre of expertise in the area of border control. It develops training curricula and specialised courses in a variety of areas to guarantee the highest levels of professional knowledge among border guards across Europe. It also supports search and rescue operations that arise during border surveillance operations at sea.

3.2. Frontex Origin

The ideas that led to the creation of Frontex have a deep history in the European project. Fostering the free movement of people has been an important objective of European integration. In 1957, free movement of goods, persons, services and capital were identified as foundations of the Community in the Treaty of Rome. During the 1980s, five Member States (Belgium, France, Germany, Luxembourg and the Netherlands) decided to create a common area of free movement – a territory without internal borders. In 1985, they signed the first agreement in a small town in Luxembourg called Schengen – an agreement that was followed in1990 by a Convention implementing the Schengen Agreement.

When the "Schengen area" – a territory in which the free movement of persons - entered into force in 1995, checks at the internal borders were abolished and a single external border was created. Slowly, border control, as well as the rules governing visas and the right to asylum, became common for all Schengen countries.

In order to keep a balance between freedom and security, participating Member States agreed to introduce additional measures focusing on cooperation and coordination of the work of the police and judicial authorities. Because organised crime networks do not respect borders, this cooperation became key to safeguarding internal security.

In 1999, with the signing of the Treaty of Amsterdam, this intergovernmental cooperation was incorporated into the EU framework. Since 1999 the European Council on Justice and Home Affairs has taken several steps towards further strengthening cooperation in the area of migration, asylum and security.

In the border management field, this led to the creation of the External Border Practitioners Common Unit - a group composed of members of the Strategic Committee on Immigration, Frontiers and Asylum (SCIFA) and heads of national border control services.

The Common Unit coordinated national projects of Ad-Hoc Centres on Border Control. Their task was to oversee EU-wide pilot projects and to implement common operations related to border management.

Two years after the establishment of "ad-hoc" centres the European Council decided to go a step further. With the objective of improving procedures and working methods of the Common Unit, Council Regulation (EC) 2007/2004 of 26 October 2004 led to the establishment of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex).

This Regulation was repealed by Regulation (EU) 2016/1624 of 14 September 2016, establishing Frontex, the European Border and Coast Guard Agency.

3.3. Frontex Organization

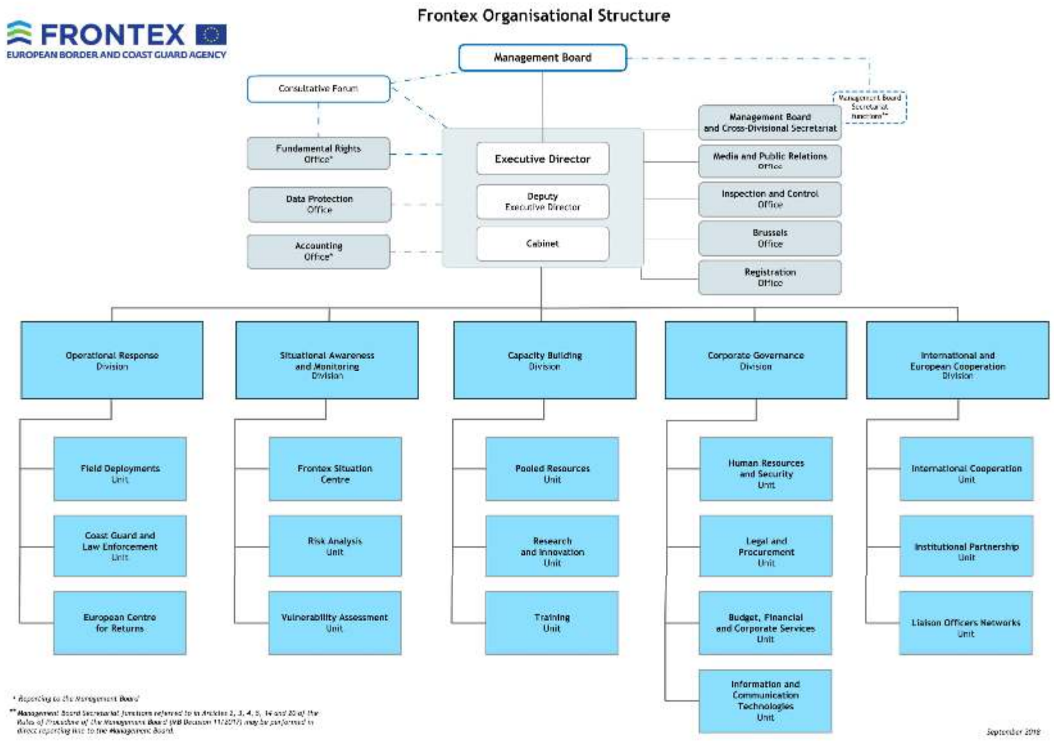
The agency is managed by an Executive Director whose functions and powers are defined in Article 68 of Regulation (EU) No 2016/1624. The Executive Director is assisted by a Deputy Executive Director and supported by five Divisions, a Cabinet, Offices (Data Protection, Accounting, Registration, Brussels) and Teams (Media and Public Relations, Inspection and Control, Management Board and Cross-Divisional Secretariat).

The Divisions are following:

- Operational Response Division
  (Field Deployments Unit; Coast Guard and Law Enforcement Unit; European Centre for Returns)
- Situational Awareness and Monitoring Division
  (Frontex Situation Centre; Risk Analysis Unit; Vulnerability Assessment Unit, Information Fusion Centre)
- Capacity Building Division
  (Pooled Resources Unit; Research and Innovation Unit; Training Unit)
- International and European Cooperation

- Corporate Governance Division
  (Human Resources and Security Unit; Legal and Procurement Unit; Budget, Financial and Corporate Services Unit; Information and Communication Technology Unit)

An independent Fundamental Right Officer reports directly to the Management Board and cooperates with the Consultative Forum which assists the Executive Director and the Management Board with independent advice in fundamental rights matters.



Frontex Organisational Structure

FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY
Management Board
Consultative Forum
Fundamental Rights Office*
Data Protection Office
Accounting Office*
Executive Director
Deputy Executive Director
Cabinet
Management Board Secretariat functions**
Management Board and Cross-Divisional Secretariat
Media and Public Relations Office
Inspection and Control Office
Brussels Office
Registration Office
Operational Response Division
Situational Awareness and Monitoring Division
Capacity Building Division
Corporate Governance Division
International and European Cooperation Division
Field Deployments Unit
Coast Guard and Law Enforcement Unit
European Centre for Returns
Frontex Situation Centre
Risk Analysis Unit
Vulnerability Assessment Unit
Pooled Resources Unit
Research and Innovation Unit
Training Unit
Human Resources and Security Unit
Legal and Procurement Unit
Budget, Financial and Corporate Services Unit
Information and Communication Technologies Unit
International Cooperation Unit
Institutional Partnership Unit
Liaison Officers Networks Unit

* Reporting to the Management Board

** Management Board Secretariat functions referred to in Articles 2, 3, 4, 5, 14 and 20 of the Rules of Procedure of the Management Board (MB Decision 11/2017) may be performed in direct reporting line to the Management Board.

September 2018

3.4. ICT Unit

Frontex ICT Unit architects and delivers organization-wide ICT capabilities, supports business units in delivery of specific business domain capabilities, controls ICT security, controls IT technologies used in Frontex, manages all IT services deployed for operational use, provides all levels of technical support to IT users and systems.
With reference to this contract, it is important to know that ICT delivers software applications made “in-house” by mixed teams of internal ICT resources and contractors, as well as by managing delivery of software applications fully made by the Contractor under fixed price contracts. Frontex practices also other delivery scenario, in which the project is managed by the actual business unit with support of Frontex ICT acting as internal supplier. Every software application, which is a subject of deployment to operational use, regardless the model of its delivery, must pass business acceptance (focus on functional requirements), ICT acceptance (focus on non-functional acceptance) and must be handed over to operational use and maintenance according to a defined ICT Change Management process. Maintenance and administration of the application becomes then the responsibility of Frontex ICT while product ownership and management (including the functional evolution of the application) remains with the business unit.

3.5. Related contracts

Due to the limited resources and capabilities, the delivery of new systems as well as part of operational maintenance services are performed with the support of external contractors awarded in various tender procedures. Despite other numerous individual contracts, the most related to this FWC is the framework contract referenced as FWC/OP/500/2014 Lot 1 for Software Development Services.

The below list presents others framework contracts runs by Frontex which include software development or related services:

i. FWC-OP/500/2014 Lot 1 – 4 years long contract with 4 contractors for software development services
ii. FWC-OP/500/2014 Lot 2 – 4 years long contract with 2 contractors for system, storage and helpdesk support services
iii. FWC/OP/131/2016-AH – 4 years long contract with 3 contractors for delivery of software development service for SharePoint technology
iv. Frontex/RP/159/2017/AH - 4 years long contract with a single contractor for delivery of, among others, software development services for Eurosur application
v. Frontex/2018/63/SB - 4 years long contract with a single contractor for delivery of software development services for Opera application
vi. FWC/OP/726/2016/AH Lot 3 - 2 years long framework contract with 3 contractors for delivery of ESRI GIS related services
vii. FWC/OP/726/2016/AH Lot 1 - 2 years long framework contract with a single contractor for delivery of SAS related services
viii. FWC/OP/726/2016/AH Lot 2 - 2 years long framework contract with 3 contractors for delivery of Microsoft BI related services

Scope of each of the above contracts is defined in the pertinent contract’s documentation. In case of overlapping in services and competencies, the above listed, already signed contracts will be used for contracting these services as long as they are available.

In parallel to this framework contract, Frontex intends to sign another framework contract for software development, limited to Time & Means services. Although, in addition to other areas included in its cope, it will be used for developing software, the capabilities expected from the contractors as well as the model of cooperation is substantially different from this framework contract. Both framework contracts can be considered as continuation of the mentioned FWC/OP/500/2014.

As it is described further in this document, this framework contracts will be used for development of defined software solutions by organized teams. By default, execution of any Specific Contract will be managed under properly established internal project in Frontex. Conversely, the abovementioned other T&M framework contact for software development services shall be considered as a sourcing mechanism for T&M services of individual consultants. Although its scope is broader, with regard to software development it will be used mainly for developing early versions of new software systems (where the scope and shape of the product is not yet fully defined), for services focused on corrective and perfective maintenance of existing systems, for specific consultancy (e.g. analysis, testing) or support to ongoing activities.

4. Stakeholders

From the point of view of this FWC there are 4 primary stakeholders who will be directly affected by the implementation of the FWC or could be affected in the course of its implementation. These are:

- Frontex business units which shall be considered as users and who may also manage the projects by executing SCs under this FWC.
- Frontex ICT unit which shall be considered as the internal supplier in the projects related to the SCs under this FWC, as well as administrator of the systems to whom the solution shall be handed over for operational maintenance and who shall be supported in maintenance of the systems. Specifically, ICT unit is responsible for assuring systems security from ICT perspective.
- Frontex Corporate Governance Division that is responsible for administering the FWC including financial and procurement matters.
- Contractors acting under various contracts with Frontex for designing, implementing or supporting other related systems.

Other stakeholders who play important roles in the scope of this FWC in its broader sense are: the European Commission, other EU Agencies and Member States who may participate directly or indirectly in the projects related to this FWC and use the services and products delivered under this FWC.

The detailed identification of the stakeholders shall be performed for each individual SC.

5. Description of the current and target states

5.1. Current Situation

In the recent years Frontex has deployed a number of software applications which are currently in operational use and in further evolution. They were developed mainly by use of external contractors while operational maintenance is performed partially by external contractors and partially by Frontex ICT staff. These applications were delivered in projects lead by either business units or ICT staff, under technical control of ICT staff, and handed over for 1st and 2nd lines of maintenance to ICT Unit. The software accepted in operational baseline is included in the official ICT Service Catalogue and supported within the service levels agreed in specific service agreements or indicated in the catalogue. Software development itself was performed in a defined process following best practices in that discipline however not in one unified way for all systems and at different levels of maturity in different areas. By default, Frontex holds the source code of the software applications, users and administrators' manuals, business requirements documents, technical design documents and standard operating procedures. Applications were tested and formally accepted for usage. Most of the applications underwent independent security penetration tests or other health checks recommended by technology vendors. Software applications are frequently updated with new releases providing corrective updates to the bugs discovered and evolutionary new features.

Most of the internally hosted applications have been developed in Microsoft technology stack as transactional, web and service-oriented applications. Nevertheless, it is still the fact that many applications operate independently with little integration. There is no single integration model or bus, so various interfacing techniques (mainly web services and database level replications) are applied between various systems. The technologies and components used in development of applications are listed in *Appendix no 2 Current ICT Baseline*.

The following applications shall be recognized as important capabilities which have been recently developed or are under development:

- JEVO (successor of former JORA) for reporting incidents in joint operations and surveillance of the situation at the borders
- MyFX (MS SharePoint based) for Frontex intranet, document management system, records management, case management, collaboration platform, knowledge database, recruitment system, contracts management, automated workflows
- Frontex Application for Returns to facilitate return operations and management of charter flights for returns
- Vulnerability Assessment EU Restricted platform (Java based applications, MS SharePoint case management and PowerBI based) which facilitates vulnerability assessment function vested to Frontex
- TRU Platform (MS SharePoint and K2 Workflows based) for managing training activities delivered by Frontex to Member States
- Operations AnTools (custom .net based application integrated with MS SSRS) for business intelligence on combined Eurosur and Jora data
- Esign solution for server-side qualified and advanced electronic signature and seal for documents.

Although many new applications have been contracted as Fixed Price contracts (MyFX, TRU Platform, AnTools, eSign etc.) still large fraction of software developments have been continued in Time & Means model.

5.2. Target Situation

Frontex intends to continue sourcing of software development service from external companies which specialize in this area. The internal software development resources, although growing, will not be built to cover any substantial part of the internal demands for application development services. Furthermore, Frontex would like to change the proportion of types of contracts used for software delivery from extreme intensive use of Time & Means contracts toward the use of Quoted Times & Means and Fixed Price software developments. Frontex intends to limit Time & Means software delivery mainly to early developments of new applications (especially for new business capabilities) which are not sufficiently mature to define their scope and requirements, and to perfective evolution of existing applications.

The maintenance model will be sustained. The 1st and 2nd lines support will be handed over to Frontex ICT with T&M support from the external contractors while the 3rd line of support will be by default fully sourced from external contractors preferably under fixed price.

Frontex will continue its technology focus on Microsoft technology stack in developing new applications. However, the full homogeneity will not be enforced, mainly due to the need for further evolution of EUROSUR Application, further evolution of SAS related platforms, handover of IRMA platform and its integration with other Frontex systems.

Due to extreme growth of Frontex, which follows changes in Frontex mandate, the development of applications will face the following challenges. The terms and conditions of this contract are specifically decided to assure availability of proper tools and resources to manage the challenges. These are:

- Extreme increase in number of internal and external users of Frontex applications
- Assurance of compliancy to the actual GDPR rules, especially with regards to “by design” and “by default” protection of personal data in applications
- Need to take over and continue evolution of existing applications developed by other parties
- Progressing need for using in-cloud hosting models for software applications including a need for conducting Security Risk Assessments
- Integration and reuse of components especially regarding authentication and authorization mechanisms, use of metadata and dictionaries, mapping and BI services, search and document storing, logging, generating records, business workflows, electronic signature
- Unification of graphical user interfaces for Frontex applications
- Increasing role of mobile applications
- Increased requirements regarding continuity of services, including 24/7 operations of applications
- Increased role of Frontex restricted network and various types (BI, GIS, SP and others) of applications hosted there, not referring to Eurosur application itself

Recently Frontex started using Microsoft DEVOPS environment to foster extra-muros developments, yet assuring full control over development artefacts to Frontex and a continuous build processes. This framework, although not limited to, will be largely following this model of cooperation.

Recently, Frontex initiated development of Enterprise Architecture. The initiative, if accepted and effectively executed, will continue along execution of this contract. The software development artefacts required in this FWC will contribute to development of EA, especially the Target Architecture and its data model. In the reverse direction, the EA (especially the TA and the data model) will affect the architectures and design of the solutions to be contracted under this framework.

The following list presents non exhaustive enumeration of the new capabilities planned for the coming years. Although the list is not exhaustive, these items will change the landscape of Frontex applications:

- Opera Evolution for planning and management of operational resources
- Frontex extranet which will replace the existing FOSS system and offer more functionalities for collaboration with authorized external partners
- New version of IRMA platform for return operations
- New personnel management suite SYSPER
- Document Handling System in the EU-Restricted network for document-based collaboration
- Target version of the Vulnerability Assessment platform
- SIS II access for deployed Frontex officers
- Tools to support ETIAS capability
- Tracking system for Frontex deployed assets
- JEVO / JORA 2
- Risk Analysis Unit Platform

6. Scope

6.1. Scope Statement

This framework contract shall be considered as the source for contracting software development services mainly under Quoted Times & Means and Fixed Price assignments.

Use of Time & Means may take only under the following conditions:

- Shall not exceed 7% of the total value of the FWC

And

- Shall be limited to Short Term assignments

And one of the following:

- Can be established as supportive means in case of a need to use resources already engaged into development or maintenance of existing systems due to need to assure continuity of services or effective use of their knowledge about specific applications.

Or

- Shall be limited to development of urgent requirements, or prototypes and changes for which upfront definition of requirements is not possible, or assistance in the handover of application to operational use.

Software Development Services shall be understood in broad meaning with reference to all phases of software life cycle and technical domains of software engineering. Therefore, it may cover typical software development as well as maintenance of existing software, refactoring, tuning etc. The technological scope of the services covers the technologies presented in Appendix 2 Current ICT Baseline.

6.2. Work Breakdown

The following services are envisaged to be ordered under this FWC:

a. Business processes modelling and requirements engineering

b. Security risk analysis and other security related consultancy

c. Software architecting and design

d. Software development

e. Software testing

f. Software integration

g. Software deployment and transition to operational maintenance

h. Training and training materials

i. Project management

j. Guarantee

k. Maintenance

l. Software related consultancy

These services will be used to deliver the following products:

m. Software systems

n. Computer Based Training for the delivered software

o. Software Development process deliverables

p. Project Management deliverables

q. Security Risk Assessments

r. Documentation

6.3. Indicative Implementation plan for the FWC

The list below presents the indicative plan for implementation of the Framework Contract; it is not binding on Frontex and may be adapted during the contractual period. The composition of the plan presents the intended flexibility in ordering and delivering various work items. The same work item may be ordered under different types of contracts according to the actual needs of Frontex. In addition, one SC may cover more than one work item.

- Evolution of Frontex applications for operations monitoring and management - JORA 2 and Eurosur Fusion Services
- Evolution of IRMA[1] platform
- SIS II[2] access application for deployed Frontex officers
- Integration with European Search Portal[3] for persons identity recognition
- Integration of application with central identity and access management system
- Development of mobile applications supporting return operations
- Implementation of time registration system
- Development of extensions and integration services for new HR system
- Delivery of application testbeds
- Evolutionary maintenance for already developed applications in .net technology
- Development of MS SharePoint workflows for internal administrative processes
- Implementation of vehicle tracking systems for the operation-deployed assets
- Evolution of Vulnerability Assessment platform
- Development of document management and collaboration DHS system in Frontex Restricted environment
- Automation platform for Risk Analysis Unit
- Other products and services

6.4. Key Competencies

Performance of this FWC requires from the Contractors their professional capacities, expertise, experience and availability of workforce in the following professional domains (not exhaustively listed):

- Microsoft technology stack and Microsoft best practices in software development
- Development of multitier, web-based, enterprise level systems in .net framework
- Development of RIA[4] in Angular and HTML5 with intensive use of ArcGIS
- Development of MS SharePoint, MS Graph, MS Flow and PowerBI

[1] *IRMA - https://ec.europa.eu/home-affairs/content/irregular-migration-management-application-irma_en*

[2] *SIS II - https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Sis-Ii*

[3] *ESP - https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171212_proposal_regulation_on_establishing_framework_for_interoperability_between_eu_information_systems_police_judicial_cooperation_asylum_migration_en.pdf*

[4] *RIA – Rich Internet Application*

- Development in Java J2EE and JBoss environment
- Development in Drupal environment
- Development of mobile application for iOS
- Software security
- Software Engineering and Software Development Lifecycle Management
- Software Testing and development of automated test
- Business Analysis and Requirements Management
- Software GUI design
- Training users of software applications
- Project management

7. General Requirements

The following requirements apply to any work item of the FWC. Adherence to these requirements shall be explicitly confirmed by the Tenderer in his Offer.

7.1. Application of GTCITC

General Terms and Conditions for Information Technologies Contracts, as included in Appendix 1, apply to this FWC according to the order of precedence defined in the FWC. Any definition of a term used in this document, if not included in chapter 1, shall be identified in the GTCITC. When consulting the General Terms and Conditions for Information Technologies Contracts please observe that all references to 'the Commission' shall be read as 'Frontex' and all references to 'Brussels' and 'Luxembourg' shall be read as 'Warsaw'.

7.2. Duration

The Framework Contract is expected to have an initial duration of 2 years, starting from the date of its signature by the last contract party, framework contract shall be automatically renewed no more than two times, each time for a period of one (1) year and on the same conditions, unless one of the parties informs the other of its intention not to extend the framework contract and such notification is received by the party to which it is addressed, no later than three months before the contract expires. The overall duration of the framework contract may in no event exceed four (4) years

7.3. Venue

The actual venue for each Specific Contract will be defined in the Request for Services.
The following categorization of place of performance shall be applied:

- For Quoted Time and Means – extra muros assignments to be performed at the Contractor's premises
- For Fixed Price - extra muros assignments to be performed at the Contractor's premises
- For limited amount and restricted scope of Time & Means - intra muros assignments to be performed at the Frontex premises
- Other Location - for assignments to be performed at geographical locations other than listed above. Other Location shall be explicitly indicated by Frontex in the Request for Service. Reimbursement incurred for travel and subsistence expenses shall be authorized only in case of Other Locations.

The venue for performance of T&M Specific Contract shall be predominantly Frontex Headquarters and will be specified in a Request for Service.

7.4. Guarantee

The guarantee for the Products acquired via this FWC is for minimum 2 years. The guarantee price shall be included in the Service purchase price. No maintenance fee shall be included in the Service purchase price.
In derogation to Article II.1.2 of the General Conditions and Article 3.4, Article 4.2 and Article 5.3.4 of the General Terms and Conditions for Information Technologies Contracts, the two-year guarantee starts from the date of signature by Frontex of the Certificate of Conformity described in Article 3.3 of the General Terms and Conditions for Information Technologies Contracts.

7.5. Security

Frontex does not require from the Tenders any personal or facility security clearance, neither at the stage of the tender procedure nor for the signing of the FWC. Performance of some of the Specific Contracts may require valid Facility Security Clearance at CONFIDENTIEL UE level for the Contractor's company and valid Personal Security Clearance at the CONFIDENTIEL UE level for the personnel performing the Specific Contract. In such a case the mandatory requirement for security clearances will be addressed in the Request for Services during the Reopening of Competition and only the proposals meeting the security requirements can be perceived as eligible.

The Contractor shall respect Frontex Security Rules and the related policies and procedures. Frontex Security Rules and the relevant policies and procedures will be made available to the involved employees of the Contractor at the beginning of each Specific Contract; any updates, and changes in these documents or any publication of new documents will be communicated during the execution of the contracts.

The Contractor's personnel involved in the execution of the Contract will be asked to sign a Declaration of Confidentiality (see chapter 3 of Annex VI Technical Proposal) prior to the start date of their direct involvement in the Contract.

If the Contractor or his personnel and, where applicable, subcontractors fail to comply with the Frontex security rules or with instructions from the Frontex Security Manual, Frontex may, without prejudice to any indemnity due by the Contractor to Frontex, terminate the Contract with immediate effect by giving notice in writing to the Contractor. In these circumstances, no costs or compensation relating to such termination shall be due by Frontex to the Contractor.

Any EU security classified Information shall be handled and protected by the Contractor as described in the Security Aspect Letter.

In addition, Frontex reserves the right to require the Contractor to initiate security screening for his personnel directly involved in the execution of the FWC to obtain the security clearance at RESTREINT UE, CONFIDENTIEL UE or SECRET UE level in order to provide specific services planned for the course of this FWC.

7.6. Working environment and conditions

For intra muros assignments, Frontex will provide to the Contractor the following resources:

- Office space for the Contractor's staff performing intra muros assignments.
- Access to all premises and elements of infrastructure necessary to conduct the tasks.
- Access to all necessary documentation and information in Frontex possession that are necessary to conduct the tasks of the Specific Contract.
- Computers, software licenses and other ICT tools for the duration of the SC; Frontex may require exclusive use of it.

All software necessary for the accomplishment of the tasks of any intra muros assignments under this Framework Contract will be installed on Frontex hardware and will remain within Frontex without deletion, change, or deletion of configuration at the end of the Specific Contract and of the FWC.

Contractor's staff may bring their company or own PC in order to perform some tasks not related to the FWC. In line with Frontex security policies, these devices will not be authorised to connect to the Frontex Network. They will get a wireless access to the internet provided by Frontex.

7.7. Methodologies, best practices and standards

The Contractor shall perform in accordance with technical norms, standards and procedures based on best professional practice in the informatics and/or telecommunications field.

The Contractor shall reference the norms and standards that he is applying for works performed under this FWC.

Frontex requires compliancy with the following methodologies, best practices and standards by default where applicable: PRINCE2[5] or PM2@EC[6], ITIL[7] and Agile[8], OGC[9] standards, INSPIRE directive[10], OWASP[11], OSSTMM[12], ISO/IEC 12207 and ISO/IEC 25000. Additional requirements regarding applicable methodologies, best practices and standards shall follow the Specific Requirements or will be laid in the Request for Services.

7.8. Subcontractors

Technical assistance to Frontex under this FWC would normally cover geographic areas within the European Union and the Schengen Area, and occasionally some activities implemented outside these areas. The Framework Contractor may be supported by associated partners providing local expertise and logistical support. If such local support is perceived by the Contractor as needed for the interest of Frontex in the scope of a SC, a prior authorisation from Frontex must be received and reflected in the SC. The FWC Contractor remains the sole party which is contractually liable.

7.9. Exclusivity

The conclusion of the FWC does not confer on the Contractor any exclusive rights in relation to the provision of services or supply of goods specified therein.

7.10. Exclusions

No exclusions have been identified of the FWC. In case any specific exclusions are identified they can be applied on the level of Specific Contract and will be demonstrated in the related Request for SC.

7.11. Transparency and handover

Frontex requires transparency from the Contractor in the provision of services under the Specific Contracts, specifically regarding the organisation and staff engaged, processes and standards used, information and documentation produced in these processes (i.e. bugs repository), and in the methods and tools used in delivering *Services* and *Products*. Frontex reserves the right to use third party professional companies to support the verification and validation of *Services* and *Products* delivered by the Contractor under this FWC.

At the request of Frontex the Contractor must hand his tasks over to Frontex staff or other indicated third party contractor by the defined date. The handover shall be planned and the plan shall be submitted to Frontex for acceptance. The handover shall enable the taking-over party to continue the tasks of the Contractor at the levels defined in the respective Specific Contract and to provide further maintenance and evolution of the solution with no additional costs for reengineering, redevelopment of documentation or reimplementation of administrative tools. The Contractor is required to train the taking-over party, present his recommendation for how to continue his tasks,

[5] *PRICE 2 - http://www.prince-officialsite.com*

[6] *PM@EC - project management methodology adopted by EC that may be made available to the Contractors after signature of the FWC*

[7] *ITIL - http://www.itil-officialsite.com*

[8] *Agile - here the iterative and incremental scrum based software development methodology*

[9] *OGC - http://www.opengeospatial.org/standards/is*

[10] *INSPIRE - http://inspire.ec.europa.eu/*

[11] *OWASP - https://www.owasp.org/index.php/Main_Page*

[12] *OSSTMM - http://www.isecom.org/research/osstmm.html*

submit all pending reports, return all tools and documents used in the performance of works, archive and handover all information, credentials and documents that and might be needed for continuation of the tasks performed by the Contractor.

Such a handover takes place by default (without a request from Frontex) at the completion of the FWC.

By the end of the Specific Contract the Contractor is required to submit all relevant reports, return all tools and documents, handover all on-going tasks to Frontex staff, archive and handover to Frontex all information, credentials and documents that might be needed for the continuation of the tasks performed by the Contractor.

7.12. Language

All the communication and documentation, both in paper and electronic form and any other deliverables, including software, source codes with its naming conventions and comments, shall be in English (U.K.) and shall adhere to a high standard appropriate for technical documentation, with no ambiguities and no mistakes in grammar or spelling. All members of the Contractor’s staff allocated to this contract shall speak and write in English at B2 level. Higher levels are required for certain profiles as indicated in Appendix 3 Staff Profiles chapter 2. The language levels are according to the Common European Framework of Reference for Languages[13].

7.13. Documentation

Technical documentation, whenever applicable, shall apply UML and automated tools for document generation. All applicable tools and standards and the standard Frontex document template shall be mutually agreed between Frontex and the Contractor. The Contractor shall adopt Microsoft Writing Style Guide[14] for the purpose of producing technical documentation under this FWC.

Frontex requires that all the documents created in the course of the project maintain a high quality. The following criteria shall be adopted when producing the necessary documentation:

- A clear and appropriate document structure, i.e. the document must be organised into chapters, sections, subsections etc. in a clear and logical way.
- Compliance with a writing style that supports a consistent structure, form and style of documents.
- Completeness of documents, i.e. the complete presentation of the entire scope of the described issue without any omission.
- Consistency and coherence of documents, i.e. ensuring mutual accordance of all types of information and lack of logical contradictions of information between the submitted documents or between parts of the same document.
- Proper identification of its title, scope, authors, reviewers, related dates, status, versions, history log, audience, quality or acceptance criteria (if the document is subject to acceptance).
- Adoption of the right format and writing style considering the content to convey and the audience.
- Reference list of bibliography if other sources are used.

The documentation shall be delivered in searchable PDF version and in editable electronic versions preferably in MS Office formats (including all tables, drawings, mockups, pictures and snapshots contained therein shall be delivered).

The Contractor shall implement and maintain in perfect order an electronic repository of the technical and project management documentation produced during the course of the FWC. This documentation shall be well organised, identified, kept up-to-date, and marked with its actual status (draft, rejected, approved). The repository shall be hosted at Frontex, accessible from Frontex and the access privileges shall be given to users approved by Frontex.

[13] *http://www.coe.int/t/dg4/linguistic/Manuel1_EN.asp*

[14] *https://docs.microsoft.com/en-gb/style-guide/welcome/*

8. Specific Requirements

The following specific requirements shall be obligatory for the Tenderer when delivering the related *Products* and *Services,* unless it is marked as optional. The Tenderer is required to declare compliancy to these requirements in his Offer.

Each requirement is marked as applicable to all types of SC or limited to specific types which are listed in the square brackets in column Title.

8.1. Product delivery

No	Title	Description
1	Main Product [QT&M, FP]	In case the SC is for delivery of a Product, it will be clearly identified and defined in the Request with FR, NFR, and if applicable, also with its vision and mock-ups. It shall meet all the functional and non-functional requirements, be fit for the purpose presented in the request, and realize its vision. The attached mock-ups and pilots shall be used to interpret the requirements. Any interfaces to external systems, reuse of components as well as standard integration with other systems defined in Current ICT Baseline shall be considered as integral part of the Main Product.
2	Delivery [all types]	All the deliverables shall be submitted to Frontex in accordance with the project Schedule. The official submission shall be confirmed by Frontex representative in form of a Consignment Note. Each deliverable shall be submitted to Frontex in: • regarding software deliverables, a complete copy of all source code including the related data files, scripts and other files needed for building the executable and operational Solution, the executable software, administrative scripts and the related release notes - all delivered in a form of an installable release package and an archived copy of the code repository. • regarding document deliverables, an electronic copy in both searchable PDF and editable formats in line with chapter 7.15 • a complete copy of the project repositories in an installable form.
3	Acceptance [QT&M, FP]	The Main Product shall be free of defects and deficiencies. Frontex decides about eligibility for acceptance testing based on the reported results of the tests performed by the Contractor. The acceptance of the Main Product shall be granted based on the positive results of the Acceptance Tests. In case of discovering minor bugs in the acceptance tests, Frontex may decide to grant provisional Acceptance and qualify the Main Product, or its part, to deployment. Such provisional acceptance may be granted only if the methods and deadlines for fixing bugs are agreed by both parties and must be followed by subsequent acceptance testing prior granting Acceptance. The scenarios, test cases, pass criteria and tools for the Acceptance Tests shall be delivered by the Contractor for Frontex acceptance prior testing. Frontex may extend the scope of the acceptance testing. The Acceptance Tests shall be performed in the environment simulating the final production environment, preferably in the UAT Environment. No tacit approval of any deliverable without a written consent of Frontex authorised representative can be recognised as binding.
4	Initial contents, directories, templates and processes [QT&M, FP]	The Main Product in a SC shall be delivered with the minimum content defined in the Request. Verification of the content shall be included in the acceptance testing. Frontex shall deliver the content in raw format as exported from other systems while the role of the Contract is to transform the content to the form necessary for upload to the Main Product. Frontex requires automated upload of the initial content and provision of the tools used for the upload or documentation which is sufficient to repeat the process by Frontex or upload other similar data.

5	Configuration Management [all types]	All project artefacts should be consistently named and marked, stored, interrelated and versioned in an electronic repository accompanied by history log fully available to Frontex.
6	Identification of Deliverables [all types]	All deliverables shall be identified and marked as configuration items (CI). Each deliverable submitted for acceptance shall carry the CI identification number, versions, and versions history log. The deliverables submitted for acceptance shall correspond to each other by allocation to the same configuration baseline. Each deliverable shall be subject of quality check by the Contractor. The deliverable shall carry information on when and who personally performed the quality check prior its submission. For each document type of deliverable there shall be an evidence of all Frontex comments collected in working level reviews and how they are addressed. For each software type of deliverable there shall be an evidence of all defects discovered to them by Frontex and the Contractor and how they are addressed.
7	Delivery Packages [all types]	Each release of software (COTS, OSS, 3rd Party Components and custom developed software) shall be handed over to Frontex in the form of installation packages and media accompanied by appropriate release notes, an installation manual, configuration data and other elements needed for successful installation.
8	User Manual [QT&M, FP]	The User Manual shall include all the information needed to learn the application. Basic computer knowledge (Windows, Office and Internet Explorer) shall be sufficient to understand the manual. The User Manual should be delivered at least in form of a searchable and structured electronic content page that can be made available on Intranet.
9	Administrator Documentation [QT&M, FP]	Main Product Administrator Documentation shall be at the minimum composed of: • Description of the environment configuration (hardware and software). • Description of the deployment of new versions including how to switch the application into and out of the maintenance mode. • Description of the application configuration (setting up the application configurable parameters). • Information about backup/restore procedures preserving transactional integrity of data (what, who, when, how, etc.). • Contractor's recommendation regarding configuration management. • Description of troubleshooting procedures in general and for specific, most frequent incidents. • Description of important parameters to monitor, the thresholds to observe and actions to take • Description of basic tests to be performed by the system administrators in order to check if the application is up, running and behaving properly after system shutdown and re-launch. • Description of the application log management procedure (when, how often and how the application log files shall be managed).
10	Security [QT&M, FP]	The software deliverables must pass the attack vectors defined in the OSSTMM (Open Source Security Testing Methodology Manual) in its current version. If the deliverables include web-applications or other web-based technologies, they need to pass all the vulnerability tests defined in the OWASP standard (Open Web Application Security Project). The most current OWASP version, at the time of signing the Specific Contract, should be used as the reference. At least the following must be covered: i. SQL injection to ensure that the SQL queries are parameterised and that any input used in a SQL query is validated. ii. Cross-site request forgery. iii. Data access to look for improper storage of database connection strings and proper use of authentication to the database. iv. Input/data validation to ensure all client-side validation is backed by server-side validation, to avoid poor validation techniques such as reliance on file names or other insecure mechanisms, and to make security decisions and output that is based on user input encoded using appropriate library v. Authentication to ensure that minimum error information is returned in the event of authentication failure and to ensure that credentials accepted from users are securely stored (hashed with a key) and check if authentication attempts are audited vi. Authorisation to limit database access and to separate privileges

		vii. Sensitive data to avoid mismanagement of sensitive data by disclosing secrets in error messages, code, memory, files, or the network. viii. Auditing and logging to ensure the application is generating logs for sensitive actions and has a process (and log viewer application in case of complex logs) in place for auditing log files periodically. ix. Code that uses cryptography to check for a failure to clear secrets and improper use of the cryptography APIs themselves. x. Threading problems to check for race conditions and deadlocks, especially in static methods and constructors. xi. There is a process in place for extracting and sharing logs, heap dumps etc. among the Frontex teams and the Contractor
11	Penetration Test [QT&M, FP]	Frontex may perform on their own, or by use of a third party, a security penetration test. In case the results indicate obvious security gaps or vulnerabilities or failures in the implementation and compliancy to the required standards and practices, the Contractor will be required to correct the system immediately at his own cost.
12	Health Checks [QT&M, FP]	Frontex may perform checks on the system's health as recommended by vendors of the applied technology. In case the results indicate failures in the implementation and compliance to the required standards and practices, the Contractor will be required to correct the system immediately at his cost.

8.2. Personnel

No	**Title**	**Description**
13	Profiles [all types]	All Contractor's staff who take part in the performance of this FWC, related Specific Contracts and the candidates offered for it, shall be assigned to one of the profiles specified in Appendix 3 Staff Profiles and shall fulfil the criteria set out in there.
14	Capacity check [all types]	The Contractor company shall evidence appropriate personnel capacity in terms of quantity of available compliant candidates as well as managerial processes and practices put in place to retain and improve professional knowledge at the company while sustaining the motivation to work. In specific: a. The number of available candidates who are fully compliant with the corresponding profiles shall be not fewer than numbers presented in Annex VI Technical Proposal, chapter 1.2.2. *Required number of the eligible personnel*. b. The Contractor shall have provided professional training in the domain of competency appropriate to the profile to personnel offered for the FWC at min of 5 training days per year on average during the recent 2 years. c. Fluctuation (turnover) of the Contractor's engineering personnel cannot be higher than 30% in the recent 2 years.
15	Named Candidates [all types]	The Contractor shall prove the availability of its personnel by submitting a list of named candidates who fulfil the requirements set for the profiles as in Appendix 3 and are made available for execution of this contract. a. The Contractor shall provide a list of candidates meeting or exceeding the numbers presented for each profile in Annex VI Technical Proposal, chapter 1.2.2. *Required number of the eligible personnel* for two domains where .net domain is one of them. b. The Contractor shall provide duly filled Form for the Named Personnel Available for the FWC per each person declared in bullet a) above accompanied by a copy of diploma and professional certificate(CV's of personnel not required and are applicable only in reopening of competition for SC). c. One individual shall be assigned to only one profile. d. A Statement of Intent and Statement of Compliancy shall be duly signed by each member of the proposed team. The personnel shall be evaluated only on the basis of the information clearly stated in the forms indicated above. Frontex reserves the right to verify the declared qualifications and experience at source.
16	Candidates proposed in Reopening of Competition [all types]	a. In the Request for Services, Frontex may require submission of a list of named candidates for a specific SC or may request submission of fully-fledged CV's of the offered personnel. b. Frontex may score the technical proposals based on the degree of how the candidate capabilities fit the tasks planned for the SC, especially regarding specific technology or technical component planned for the SC which fits to the generic profile but is not reflected in the generic profile. In such a case the Request for Services will define the scoring method. In no case will the scoring refer to any new requirements not included in the profiles conveyed in Appendix 3.
17	Interviewing candidates	As a part of competition for SC, Frontex reserves the right to interview the candidates for the SC before they take up the duties under the FWC. Such interview may take place in form of video conference or physical meeting.

	[T&M, QT&M]	
18	Replacement of personnel [T&M, QT&M]	a. When a person proposed by the Contractor in reply to Request for Services is no longer available before the start of the contract, the Contractor is obliged to inform Frontex immediately. b. In case of replacement of person in the course of the SC, the Contractor shall give one month's notice to Frontex and get Frontex acceptance for the replacement. c. In case of replacement, the Contractor will provide Frontex with the CVs of the proposed substitutes, their CV Compliancy Declaration Forms and Statements of Intent. The Contractor should propose two replacement persons with the required qualifications and experience for the profile and they must have at least the same level of qualifications/education and experience as the person proposed in the original offer. d. In case of replacement acceptance by Frontex, the replacing person can assume the work at identical financial conditions, the Contractor ensures the transition of service between the replaced person and the substitute. The handover period for service transition must be at least 5 working days of both persons, free of charge to Frontex. If no handover is possible, and additional training is needed for the replacement person, at least 10 working days (free of charge to Frontex) must be performed by the substitute. e. In case the continuity of service under SC is not sustained due to the change of personnel, Frontex may terminate the SC.
19	Underperformance and incapability of personnel to perform tasks [T&M, QT&M SC]	a. In case the Contractor does not fulfil the contractual requirements, specifically regarding the registration of time and reporting on tasks or applying work standards defined in a specific project he participates, or is not available for tasks, or breaches security or safety rules, or the reported task are consistently considered not satisfactory to Frontex, or does not communicate or cooperate with the co-working team lowering quality or slowing down work of the team – Frontex may consider such a Contractor as not capable of carrying out the specified tasks. b. At Frontex' demand, a person reported by Frontex as not capable for performing tasks, must be replaced. c. The replacement person will be given sufficient training during an adequate handover period, so that he/she becomes immediately operational when the original expert is withdrawn. Any such replacement and training, if required, will be carried out by the Contractor at no additional cost to Frontex.
20	Planned and unplanned absence of personnel [T&M, QT&M]	a. At Frontex' demand, during holidays or other periods of absence of the person involved, the Contractor will be required to provide an adequate replacement. b. The replacement person will be given sufficient training and provided with all information necessary to guarantee continuity of the service provided to Frontex. c. All such training and handover work will be carried out at no additional cost to Frontex. d. Any planned absence shall be agreed by Frontex at least two weeks prior the absence. e. Frontex shall be informed about any unplanned absence (e.g. sickness) immediately.
21	Place of work [all types]	a. The primary place of performance for T&M SCs is the Frontex Headquarters. b. The individuals performing the T&M SCs may be tasked to perform their duties in other, primarily European locations for a short period of time. d. If the nature of the tasks or service requires regular or long term visits to other locations, it shall be clearly indicated in the *Request for Services*. e. The place of performance for QT&M SC is: • intra muros for Sprint Review Meetings and presentation of deliverables, requirements elicitation and modelling meetings, acceptance testing, trainings, deployment assistance, data migration, service management interventions, project management meetings, • extra muros for all other activities in scope of the contract except those listed for intra muros, specifically software development and testing The performing team shall sit together where high quality continuously available video conferencing capability from the place of performance to Frontex shall be delivered and maintained by the Contractor. f. The primary place of performance for FP SC is Contractor's premises. However, workshops, project meetings, testing, training and deployment tasks shall be performed on Frontex premises.
22	Dedication [T&M, QT&M]	a. If not decided differently in the Request, personnel working on T&M and QT&M assignment shall be dedicated to this assignment with no engagement to any other tasks in their company except for participation in professional training programme. Frontex may terminate the SC in case of any departure from this requirement.
23	Colocation and communication [QT&M]	Contractor shall: a. Collocate all team members appointed for its execution in a single office. b. Establish and maintain a broadband on-demand video conference connectivity to the collocated team office and for every Stand-up meeting and any other meeting on demand. c. Enable participation of Frontex staff in person in the Stand-up meeting and free access to the Contractor's team members on demand.
24	Normal working hours	a. Frontex requires that the T&M services are provided in *Normal Working Hours*.

	[all types]	b.	At Frontex' demand, in exceptional circumstances or when indicated in the related Request for Services, the person involved might be asked to work in *Extended Working Hours*.
25	24/7 [T&M or QT&M]		Frontex may require, by clear indication in the *Request for Services*, that the services are provided according to the agreed timetable in the 24/7 mode and in total cover 8 hours a day per person on average, counted in one-month periods excluding lunch breaks.
26	Duration of the Assignment [all types]		Frontex may require that a person is assigned for:
		a.	ST - Short Term, for 30 man-days or less in total.
		b.	LT - Long Term for efforts estimated for more than 30 man-days in total.
27	On-call duty [all types		Frontex may require all the personnel assigned to T&M and QT&M Specific Contracts to stay in readiness for work and in case of such a need to take up tasks at the place of the performance of the Specific Contract no longer that 1 hour from the notification by telephone call or sms. The on-call shifts shall last 14 hours whether in normal or extended working hours. The Contractor shall provide the necessary phones to all its personnel subject to on-call duty.
28	Registering time [T&M, QT&M]	a.	Each individual performing services under the T&M and QT&M Specific Contracts is obliged to register the time of work by registering the exact time of every entry to, and leave of the place of work in an Attendance Sheet presented in the Annex VI Technical Proposal, or in an application provided by Frontex for time registration.
		b.	The actual attendance sheets shall be continuously available to Frontex for verification.
		c.	The Contractor is required to submit monthly attendance sheets duly completed and signed by the performing person for acceptance by Frontex.
		d.	All the time evidenced in the Attendance Sheets shall be attributed to the tasks contracted.
29	Reporting for T&M and QT&M	a.	The Contractor is required to maintain a list of all atomic tasks in electronic format in the repository provided by Frontex or, if agreed, provided by the Contractor. The tasks of different nature may be stored in more than a single repository e.g. ticketing system, tasking system, requests, DEVOPS, sprint backlog etc.
		b.	The Contractor is required to report regularly, not less frequently than once a month, on the status of all tasks assigned to each specific person in the reporting period, the tasks assigned earlier but not yet reported as completed, and the related issue log. During the course of a SC, depending on the current needs of the project or service, Frontex may require to report in higher frequency which will be communicated to the performing Contractor.
		c.	The report on tasks shall be submitted for Frontex acceptance. For each atomic task it shall present at least: a short description, reference to the tasks or service of the SC, the time planned, actual time spent, and the indication of completion.
		d.	The issue log shall present an explanation of the issues linked to the tasks, proposals for dealing with the issues and tracks of the history of each issue.
30	Kick off and inception [all types]	a.	Frontex may require that contracted staff attend a kick-off meeting before starting the delivery of services under a Specific Contract.
		b.	For T&M and QT&M SCs, Frontex may indicate in the Request for Services the duration of the inception phase in which the contracted personnel is required to familiarise with the work environment, methods and tools, and to achieve normal effectiveness in performing the tasks. In case of not achieving the normal effectiveness in the inception time Frontex may demand from the Contractor to exchange personnel assigned or terminate the SC.
31	Escalation [T&M, QT&M]	a.	Frontex requires that any irregularities, vulnerabilities or risks observed by the personnel performing the contract are immediately reported to Frontex in writing by means of the issue log, and in the cases requiring immediate action, also by telephone to Frontex 24/7 helpdesk.
		b.	Frontex requires that, in relation to the activities performed in direct relation to this FWC, the Contractor implements in his own organisation an effective internal escalation mechanism in order to control and manage risks related to the Specific Contract and the underperformance of its personnel.
		c.	In case of non-acceptance and rejection of the report on tasks in T&M and QT&M SCs the Contractor shall initiate his internal escalation procedure.
		d.	In case of rejection of the report on tasks for a person, the management staff of the Contractor shall propose improvements.
		e.	In case of two rejections of report on tasks Frontex and rejection of the proposed improvements, Frontex may demand the replacement of the person or terminate the Specific Contract.
32	Closure of a Specific Contract [all types]	a.	By the end of each Specific Contract or the engagement of a specific person in the Specific Contract the Contractor is required to submit all pending reports, return all tools and documents, handover all on-going tasks to Frontex staff, archive and hand over to Frontex all information, credentials and documents that are not in possession of Frontex staff and might be needed for the continuation of the tasks performed by the Contractor.

		b. Frontex may task the Contractor, within the scope and duration of the Specific Contract, to hand over his duties and transfer all knowledge acquired in performing the task to Frontex personnel or another third-party contractor, irrespective of whether the handover tasks were explicitly indicated in the Request for Services or not.
33	Criminal Record [all types]	Contractor shall demonstrate a valid excerpt of the criminal record of the Contractor staff members planned to participate in the execution of a Specific Contract. Frontex may refuse participation to any person that has been: convicted of an offence concerning their professional conduct by a judgment, which has the force of res judicata; guilty of grave professional misconduct, the subject of a judgment, which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests.
34	Declaration of Confidentiality [all types]	The Contractor’s personnel involved in the execution of any Specific Contracts shall sign a Declaration of Confidentiality before the commencement of work.
35	Related services and processes [T&M, QT&M]	The T&M and QT&M Specific Contracts will be performed in the scope of tasks described in the appropriate Request for Service. Frontex may ask the Contractor to perform these tasks for technical components that are not directly included in this particular FWC but which are composing its context, are integrated with it or are managed by the same team or standard process implemented in Frontex ICT.

8.3. Project Management

No	**Title**	**Description**
36	Deliverables [FP]	The following deliverables are required: a. Project management deliverables: • Project Management Plan (PMP) • Stage/Iteration Plan (S/IP) • Minutes of Meetings (MoM) • Project Reports (RE) • Project Logs (LOG)
37	PMP [FP]	The Project Management Plan should cover the following: • Project Objectives and Tasks • Project Product Description • Project Deliverables (definition, quality criteria) • Stakeholders and Communication Management • Configuration Management and Change Control • Product Delivery Management • Project Tolerances • Quality Management • Scope Management • Project Organisation Structure, Role Assignment and Composition of the Team • Project Master Schedule (including resource allocation, dependencies and effort) • Risk Management • Project Management templates By default, the PMP must meet Frontex acceptance within 1 month from project start date.
38	MoM [all types]	The Contractor shall be responsible for drafting and disseminating minutes of the meetings within 3 working days from the end of the meeting. Minutes must be a tangible record of the meeting for its participants and a source of information for people who were unable to attend. They must capture in a clear, unbiased and concise way the essence of the meeting, its agenda, motions and contrasting positions presented during the meeting, decisions taken, action items set and reviewed. Capturing the minutes live during the meeting and visible to all participants on the screen is a preferred method of drafting.
39	RE [FP]	Regular monthly (or bi-weekly if required by Frontex at any stage of running project) Highlight Reports as well as: end stage/project, exception reports are required. The reports shall be mainly composed of a narrative description of the overall situation, the progress in delivery of products in the reported period, plans for the next period as well as decisions needed and excerpt from the LOGs (including risks and issues). The update on tasks and deadlines shall be referred to the baseline schedule. Reports shall not be used to interpret requirements. Contractor shall correct the reports based on Frontex feedback.

40	LOG [QT&M, FP]	The Contractor shall maintain continuously the following registers: Risk Log, Issue Log, Quality Log, Daily Log and Configuration Item Record.
41	Product Descriptions [QT&M, FP]	Product Descriptions shall be prepared by the Contractor and agreed with Frontex prior to the development of the Product.
42	Escalation [all types]	Frontex recognizes the need for escalation when issues need senior-level’s awareness or intervention, especially if there is a risk of going beyond the project tolerances, or there is a risk or event of breaching the terms and conditions of the contract, security or safety rules, or the decisions cannot be taken in a timely manner according to standard project management procedures. In such cases the Contractor must immediately escalate the issue, in the first instance, to the Frontex Project Manager, in the second instance to the Project Board. The escalation shall be accompanied by unbiased and clear documentation and recommendations.
43	Conciseness of plans [FP]	PMP shall convey the content which is specific for the project. No voluminous presentation of standards is allowed. Static parts (methodology) shall be separated from dynamic parts (schedule).
44	Compliancy of the PM methodology [FP]	a. The project management methodology applied by the Contractor shall be compliant with: Prince2 or PM2@EC Project Management Methodology developed by DIGIT. b. Frontex may require the Contractor to apply processes and templates specified by Frontex.
45	Frontex staff availability [all types]	The Contractor shall precisely address his requirements for contributions from Frontex staff by definition, level of details and deadlines while respecting the time limitations of staff due to missions and other assignments.
46	Role of SC Contract Board [QT&M, FP]	FP and most of the QT&M SCs are concluded in correspondence to Frontex IT Enabled Projects. In these cases, the SC covers a part of the scope of the Frontex IT Enabled Project. For these projects Frontex establishes project management structure according to his internal policies. The following roles are established: Project Executive (Owner), Senior User, Senior Supplier, Project Manager and optionally support of Contract Officer, PMO and ICT Support to PM. a. A SC Contract Board shall be established for each such SC for effective sponsorship at both sites, for surveillance of the progress and quality of SC, communication between Frontex and the Contractor at managerial level, consultations regarding management of the contractual changes and for dealing with issues escalated from project managers or users. b. The SC Contract Board shall be composed of Senior Supplier and optionally Project Executive from Frontex and SC Contractor’s Manager from the Contractor site. c. The SC Contract Board shall be supported by Contracting Officers from both sites. d. The SC Contract Board shall be supported by Project Managers from both sites.
47	Role of SC Contractor’s Manager [QT&M, FP]	a. The Contractor shall nominate SC Contactor’s Manager who will be ultimately representing the Contractor’s company and subcontractors vis a vis Frontex for the supervision of the SCs, overall performance of the Contractor, change management and escalation of issues not solved at the level of the individual contracts. b. The role of SC Contractor’s Manager may be played by the FWC Executive. c. The SC Contractor’s Manager shall assure sponsorship for Contractor resources. d. The SC Contractor’s Manager shall be available for meetings of SC Contract Board meetings on short notice (the same calendar week) when requested by Frontex.
48	Role of PM [QT&M, FP]	a. The Contractor shall nominate his Project Manager. PM is considered as a member of key personnel and shall not be changed during the complete duration of the QT&M and FP SC. Frontex may terminate SC in case of not agreed unilateral change of PM. b. PM coordinates and manages for the Contractor the execution of Specific Contracts, Contractor’s resources. PM is responsible for delivery of the all contractual deliverables and work packages in the conditions of the SC. c. The nominated PM shall take the responsibilities described for this profile defined in this FWC. d. PM shall be entitled to represent the Contractor in daily cooperation with Frontex and to decide the allocation and tasks of the Contractor project team members. e. The Contractor PM shall work in close cooperation with the Frontex PM, report, advise, assist and support him in favour of the Frontex project that the Specific Contract is contribution to. f. The Contractor PM shall work with the project team at Frontex premises or, if the project is performed at other locations, he should work at that location with regular frequent visits to Frontex Headquarters.

		g. The Contractor PM may be required to provide planned or ad hoc presentations of the projects that he is managing to Frontex and MS stakeholders.
49	Synchronization and Harmonization [QT&M, FP]	a. Projects under this FWC will be performed in the context of other projects and service delivery processes. Therefore, the Contractor shall define and maintain relations with other projects, synchronise the related activities and harmonise the processes to the greatest possible extent. The Contractor shall foresee the synchronisation and harmonisation efforts in planning and reporting. b. It is required that all the projects performed by the FWC Contractor are managed in a unified way. It is required that the Contractor periodically presents to Frontex the unified portfolio level reports on the ongoing and planned projects, their status, dependencies, shared risks and issues, resources used, projected benefits delivery plan and plan of new releases and roadmaps of already operational systems.
50	Dedication of resources [all types]	The Contractor shall present in the project plan the resources allocated to the project. A situation where the same key project resources are assigned to more than one project should be avoided.
51	Configuration audit [QT&M, FP]	The Contractor shall perform regular configuration audits and the audit report shall be presented to Frontex.
52	Quality reviews and docs [QT&M, FP]	The Contractor shall perform internal quality reviews and the related documentation shall be accessible to Frontex.
53	Project repository [QT&M, FP]	All project management documentation shall be handled in electronic format in project repository fully accessible to Frontex. The recoverable copy of the repository shall be handed over to Frontex by end of the SC and any time on request.

8.4. Implementations

The following requirements are applicable for implementation of the delivered applications composed of OSS, COTS, custom software, separately or jointly.

No	**Title**	**Description**
54	Branding (BRAND) [QT&M, FP]	The BRAND shall at least cover the fully fledged, final resolution, colourful, OOTB compliant and aligned to the OSS/COTS: navigation, UI java scripts, master pages, pages layouts, styles, skins/themes, graphics, composed looks, icons and user snippets. Branding shall be managed centrally in the Main Product and delivered as installation files. Branding shall fully foresee the specifics of mobile platforms.
55	UX/GUI [QT&M, FP]	User Experience of application (ergonomics, graphical user interface, navigation, interface behaviours and dialogs etc.) shall be designed in professional manner. Unless Frontex decides on the use of software OOTB, the UX/GUI shall be built based on analysis of the requirements, modelling with users and documented with the most possible reuse of it from other Frontex systems. Frontex may impose the use of its standard for UX/GUI under any SC under this FWC, as well as the use of a single central UX/GUI design tool. Currently Frontex uses Axure software for this purpose. Mobile application User Experience design shall respect platform guidelines e.g.: • Human Interface Guidelines for Apple devices • Material Design Guidelines for Android devices
56	Customizations [QT&M, FP]	All the configuration, metadata and customisations (where custom development is not required) shall be delivered with the documentation of: configuration settings, SQL and search queries, power shell scripts and Java scripts etc. The customisations shall be delivered as templates or scripts.
57	Information Architecture (IA) [QT&M, FP]	The IA Information Architecture shall be delivered as the recommended design covering at least: • functional modules structure • definition of the taxonomies used with the related taxonomy management rules and draft metadata management policy document • definition of actual nodes in navigation and visualisation of navigation means implemented in the Solution • definition of the content types and related policies

	• communication channels • search configurations • possible ways of personalisation • values for labelling user interface and the hints for mouse hoover • definition of the landing pages • dictionaries and stores structures • views, listing and sorting • definition of personas for the solutions and user roles • definitions of roles, groups and access/privileges schemas • contribution to Frontex policies and procedures concluding from the IA

8.5. Software development artefacts

No	Title	Description
58	Artefacts in Software Development [QT&M, FP]	The following artefacts are required in software development: a. Project management deliverables as described in the Project Management requirements b. Software Development Process and Practices (SDPP) c. Architecture deliverables ○ Architecture (ARCH) d. Requirements deliverables ○ Business Requirements Document (BRD) ○ System Requirements Document (SRD) ○ ICT Security Risk Assessment (SRA) e. Design deliverables ○ Technical Design Document (TDD) f. Development deliverables ○ Source code (CODE) including data files, scripts and other files needed for executable system ○ Executable software (EXE) ○ Unit Tests (UT) ○ Automated Tests (AT) ○ Technical Documentation (TD) ○ Administrator Documentation (AD) ○ User Manual (UM) g. Testing deliverables ○ Test Plan (TP) including testing traceability matrix ○ Test Cases and Test Scenarios (TC/S) ○ Test Log (TL) ○ Test Summary Report (TSR) h. Deployment deliverables ○ Application deployment (DEP) The artefacts are considered as contractual deliverables.
59	PMP [FP]	As described in the Project Management requirements.
60	SDPP [QT&M, FP]	Software Development Process and Practices shall document the organization of development process in this specific project and its tooling. It shall cover: • Organization of work in development teams, lifecycle of development artefacts, relation and treatability of development artefacts, roles and tasking • Progress tracking and reporting • All practices in software development to be applied for assuring quality in the process e.g. code reviews, walkthroughs and others with specific parameters e.g. coverage, frequency and thresholds • Configuration of tooling in scope of backlogs, tasks, builds, releases • Definition and configuration of repository for development artefacts • Configuration and use of tooling for testing • Overall design and topology of the environment related to delivery of the Main Product including development, UAT, training and production environment • Description of dependencies and synchronizing of the environments in their lifecycle

		• Configuration of the ICT environments and its services • Description of the development-testing-deployment workflow including timing, conditions, tools, roles and responsibilities
61	ARCH [QT&M, FP]	Architecture documents shall convey at the minimum the following information: • Vision of the system • Architectural goals • Architecturally significant requirements and constraints • Key abstractions • Architectural decisions (with related rationale) and options • Architectural mechanisms and patterns • Operational model and deployment approach • Architecturally significant design elements • Critical system interfaces • Capacity, performance and scaling • Security • Assets to be reused • Guidance for developers
62	BRD [QT&M, FP]	The Business Requirements Document shall convey at the minimum the following information: • Vision of the system • Reference to Business-Case including risk analysis, value delivery timetable, success indicators • Business Architecture including value chains, business processes (BPMN), roles, actors, capabilities, business rules • Business domain model and taxonomies • Scope definition (inclusions, exclusions) • Requirements register, or user stories and storyboards (including priorities, dependences and sourcing) • Non-functional requirements • Quantitative analysis
63	SRD [QT&M, FP]	The System Requirements Document shall convey at the minimum the following information: • References to the Business Requirements Document and Technical Design Document. • Application Architecture including system roles, use cases specifications, system rules (UML). • Data Architecture including logical data model and data life cycles (UML). • Mock-ups, navigations, UI or functional prototype • Document templates and data scopes. • Acceptance criteria for users stories (if it is required) • Traceability matrix for use cases and requirements
64	SRA [FP]	ICT Security Risk Assessment shall cover the following substantial elements: • Scope definition - the scope of the information system and of the risk management process must be defined prior to starting and related to the business context under consideration. • Asset identification - essential information handled and the services provided must be identified as well as subordinate system components - applications (software), equipment (hardware), communications, media, facilities, and personnel. • Dependencies between assets. • Asset classification (process to identify the classification levels by determining the possible business impacts resulting from incidents for each of the confidentiality, integrity and availability categories). • Potential Impact and Risk Determination - calculated for an asset considering its accumulated value, threats and the likelihood of occurrence. • Safeguard selection - it is necessary to go through all of the potential safeguards and retain only those which are relevant for protecting the asset. • Safeguard valuation – effectiveness and maturity level of each safeguard shall be estimated using Capability Maturity Model. • Residual Impact and Risk Determination (for both on premise and cloud computing model) - This is calculated for an asset considering series of safeguards in place, asset accumulated value, threats and the likelihood of occurrence. • Conclusions of risk assessment for current and target computing model

65	TDD [QT&M, FP]	Technical Design Document shall be composed of: • Technology prototypes or technology evaluation report • Application Architecture including ○ System component model ○ Internal interfaces description ○ External interfaces control documents ○ Deployment model and connectivity • Security, authentication and authorisation model • Description of how the security and compliancy requirements will be fulfilled • Data migration • HW sizing, capacity and performance model • Assumptions and constraints • Design risks and planned mitigations • Requirements - design components traceability matrix
66	TD [QT&M, FP]	Technical Documentation shall be at the minimum composed of: • Source code structure and description • Low level design documents if used (e.g. state machine diagrams, sequence diagrams, deployment diagrams) • Standards used • Detailed physical data models • API documentation and guidance for integration with other systems • Deployment manual and configuration • Release notes • Reports on unit tests • Specification of Open Source software or any third-party software used and its configuration • Updates to TDD reflecting "as implemented" status with clear indications on the departure from the approved TDD and the reasons therefore

8.6. Software development process

No	**Title**	**Description**
67	Model for Software Development Lifecycle	a. Software development shall be primarily conducted in accordance with SCRUM framework. b. The Contractor shall propose his recommendation for software development process in compliance with Frontex requirements. Frontex and the Contractor will adjust the proposed methodology to the actual needs and constraints on the commencement of the Contract. c. For a SC, the Contractor may be required to apply a specific implementation of SCRUM named Agile@EC that is used for internal development in the Commission and to apply the related templates.
68	Software developments in scrum-based [QT&M]	All requirements set in the chapter Specific Requirements are applicable to SC for software development in scrum-based QT&M unless specific items are excluded in the Request for SC. The following parameters will be defined by Frontex for scrum-based software development in QT&M SC: a. Frontex will define sprint duration (preferably 3 weeks). b. Frontex will provide the **definition of done** (by default covering: the stories of the sprint backlog are developed, tested and documented, all tasks are registered with status and time spent, burndown and velocity is captured and transparent, code and configuration data is registered and stored in code repository, software is tested against defined test cases covering user stories and integration tests, it is deployed to UAT environment and integrated with the existing version of the application, it is demonstrated to and approved by the Product Owner, the TDD document is updated. c. Frontex will provide Request for SC with a defined sprint backlog for assessment of volume of work for the initial sprint and then assume the same volume of work in other sprints. The work volume, named Quoted Unit of Work, will be sustained in all sprints so all sprints are equal in volume of work. Future sprints will be composed from the live product backlog to correspond to business priorities and keep the scale of sprint constant. d. Estimation of work will be performed by Contractor per each backlog item and approved by Frontex. Method of estimation will be defined, transparent to Frontex and applied to any future sprints.

		e. Contractor will assign a team sized to cover all services and scope elements for the QUW and keep the team dedicated and unchanged for the SC. Stability of the team is considered as a key requirement. Frontex may terminate the SC in case of changes to the scrum team. f. User stories shall be sized to be expressed in User Story Points (or other agreed unit) according to the Sizing method agreed in the Specific Contract. The Contractor shall break down the provided Epics, Features, User Stories, Use Cases or Requirements down to Work Items. g. Every sprint shall finish with the working Product demonstrated to Product Owner. Frontex will have indicated in the SC how often the Product of the sprint shall be deployment to PROD (e.g. every second sprint). h. Frontex will nominate the Product Owner. i. Contractor will nominate the Scrum Master who is considered a member of key personnel and must not change in the course of SC. j. Frontex will establish an inception period (usually first 2 weeks of work) which shall be devoted to inception, elicitation of the requirements, building product backlog, development of TDD design, building development and testing environment and procedures, building project repositories so the first sprint work goes smoothly in full sense of scrum and for meeting the Definition of Done. k. Frontex will establish completion period (most often final 2 weeks of the Contract) for review of all pending stories and issues discovered, creation of Lessons Learned report by the Contractor and handing it over to Frontex, handing over complete project artefacts repository for all product documents, scrum registers, source and compiled code and configuration data to Frontex, performing configuration management audit, performing complete integration tests, handing over technical documentation for all software developed in the Contract and complete maintenance documentation, delivery of training materials in the entire scope of functionalities, performing data migration. l. Sprint Review, Planning and Retrospective meetings shall be documented by Contractor and Frontex will participate in them. m. Product backlog shall be validated and prioritized by the Product Owner. Its entries are validated and sized by the team under Scrum Master's facilitation. Allocation of items to Sprint backlog shall end in the Sprint Planning meeting following the priorities and up to the Sprint QUW. n. All other principles, values, roles, events, artefacts of Scrum shall be respected. o. Scrum management tools, especially Product backlog, Sprint backlog, tasks, Burndown charts shall be maintained electronically and remain accessible at any time to team members and Frontex using the agreed DAR. p. In case of departure from the above requirements or unapproved deviation from scrum principles, after 2 consecutive written complaints from Frontex, Frontex may terminate the SC at the failure of the Contractor. q. A successful acceptance of any Sprint Review based on the Sprint backlog in reference to the Definition of Done by the Product Owner is a condition pre-requisite to acceptance of the contractual QT&M SC. r. Delivery of all artefacts and successful acceptance of the Completion Period are the prerequisites to the final acceptance of the SC.
69	Software development in [FP]	All requirements set in the chapter Specific Requirements are applicable to SC for software development in FP unless specific items are excluded in the Request for SC. Conditions and expected organization of software development in Fixed Price SC will be constrained in Request for SC. In contrast to Scrum-based software development in QT&M the Contractor will provide price for delivery of the entire scope and Main Product and will offer his organization of work. In a Request for SC, Frontex may require to follow the same principles as set for QT&M.
70	Compulsory Reports from software development [all types]	The following reports shall be maintained continuously during the software development process at minimum: a. Product log b. Sprint log c. Burn down chart d. Quality log
71	Source Code Control [all types]	All development source code, along with relevant documentation and all software assets, including configuration data and scripts, shall be uploaded and stored in DAR with no delay. This can be done either by working directly in the source code repository

		or by uploading stable source code snapshots in the event that the supplier is working remotely. All check-ins must have a clear English description of the modifications in the form of (where XXXX stands for unique identification): • bug XXXX: description - if the check-in is related to a bug fix • story XXXX: description - if the check-in is associated with a user story • other: description - if the check-in is not related to a bug or a story number
72	Integration [all types]	Contractor is responsible for integration of the custom developed code, new releases and patches to the Main Product. The integration includes a merge with other changes (including those performed in T&M or QT&M assignments), integration and regression tests.
73	Installation Packages [all types]	Each release of software shall be handed over to Frontex in the form of source code in the project repository with the proper build scripts and configuration accompanied by appropriate release notes, an installation manual, configuration data and other elements needed for successful installation. Updates to manuals and self-explanatory power point presentation of the changes and the new features together with screenshots shall be delivered prior the release.
74	Defects DB [all types]	a. Any issues, bugs or defects identified in the system under development shall be recorded in the Defects DB. b. The Contractor shall implement Defects DB. It shall be hosted at Frontex or at the site provided by Frontex. c. Any issues, bugs or defects identified in operational use of the system shall be recorded in the Defects DB. d. The Defects DB must provide reporting capability to reflect the status of the issues as well as to provide statistical data on bugs and the tempo of resolving them. e. Any resolved issue, bug or defect registered in the Defects DB must be accompanied by the reference to the version, versions, release in which the issue is resolved. f. Frontex shall have full and unhindered access to the Defects DB.
75	Development Artefacts Repository [all types]	a. Each incremental build that is of release quality and contains new functionality must be archived into an Artefact Repository tagged with build number. b. SC shall define hosting model of DAR: Frontex on-prem TFS or ADO, or another defined DAR. c. By default, DAR is managed by Frontex.
76	Release Notes [all types]	Any new releases of software shall be accompanied by Release Notes that provide clear reference to the implemented stories, change requests, issues, bugs and defects corrected in it.
77	UML [all types]	a. UML v.2 shall be used for analysis, design and documenting the software. b. Additional narrative descriptions of the models may be necessary when communicating with the users.
78	Process Audit [QT&M, FP]	a. Frontex may require an audit of the actual software development processes executed by the Contractor against the plans, applicable standards and requirements. b. Any such audit shall last no longer than 2 working days in 6 months for a Specific Contract. c. Any observed deviations from the plans, applicable standards and requirements shall be rectified or, if justified for Frontex interest, can be waived by Frontex.
79	Testing Scope [QT&M, FP]	a. Automated tests delivered by the Contractor covers: • Agreed unit tests • Agreed user story tests • System test (testing the whole system via UI) • Sanity tests (after recovery, deployment or restart) • Agreed Load and Performance tests b. A user story will not be considered complete unless there is a full suite of passing tests against it. Each user story has to be covered by related Test Case. c. The following tests apply for the solution as a whole and shall be performed by the Contractor: • Regression testing • Security testing • Load and Performance testing • Automated deployment testing d. Frontex may require to perform: • Usability test • Other non-functional tests

		e. All the tests shall be documented by the Contractor. The documentation of the tests, including the results, shall be handed over to Frontex
80	Acceptance Tests	See chapter 8.1
81	Unit Tests [all types]	The minimum required unit test coverage for business or other operational logic (e.g. web services, UI Logic) shall be agreed by Frontex in the project plan, however by default it shall not be less than 70%.
82	Security Testing [QT&M, FP]	a. Security Test shall cover at least the following: i. SQL injection to ensure that the SQL queries are parameterised and that any input used in a SQL query is validated. ii. Cross-site scripting. iii. Cross-site request forgery. iv. Data access to look for improper storage of database connection strings and proper use of authentication to the database. v. Input/data validation to ensure all client-side validation is backed by server-side validation, to avoid poor validation techniques such as reliance on file names or other insecure mechanisms, and to make security decisions and output that is based on user input encoded using appropriate library vi. Authentication to ensure that minimum error information is returned in the event of authentication failure and to ensure that credentials accepted from users are securely stored (hashed with a key) and check if authentication attempts are audited vii. Authorisation to limit database access and to separation privileges viii. Sensitive data to avoid mismanagement of sensitive data by disclosing secrets in error messages, code, memory, files, or the network. ix. Auditing and logging to ensure the application is generating logs for sensitive actions and has a process (and log viewer application in case of complex logs) in place for auditing log files periodically. x. Code that uses cryptography to check for a failure to clear secrets and improper use of the cryptography APIs themselves. xi. Threading problems to check for race conditions and deadlocks, especially in static methods and constructors. xii. There is a process in place for extracting and sharing logs, heap dumps etc. among the Frontex teams and the Contractor
83	Effort Estimation [QT&M, FP]	It is required to provide an effort estimate for each software development assignment based on QT&M and FP and to decompose the estimate down to deliverables, split into profiles and provide traceability to requirements or group of requirements. The decomposition shall not be considered as any type of limit of efforts.
84	Development Team [QT&M, FP]	a. The team engaged in software development shall be composed of professionals who are accepted and who meet the requirements set for the profiles. b. The composition of the team, profiles, roles and planned level of engagement shall be indicated in the response to the Request for Services and reflected in the Project Management Plan.
85	Configuration Management [all types]	a. The Contractor is responsible for harmonised management of the configuration for all configuration items related to all activities related to the FWC. b. The Contractor is responsible for maintaining the consistency of the source code across all software development activities under various assignments of the FWC and merging all simultaneous or overlapping versions and branches.

8.7. Compliancy, security and data protection

No	Title	Description
86	Contractor vulnerability testing [QT&M, FP]	Contractor is required to run application vulnerability test with globally recognised vulnerability testing tools or service and handover the resulting documentation of the test to Frontex through secured channels accepted by Frontex.
87	Penetration Test [QT&M, FP]	Frontex may at any time perform on their own, or by use of a third party, a security penetration test. In case the results indicate obvious security gaps or vulnerabilities or failures in the implementation and compliancy to the required standards and practices, the Contractor will be required to correct the system immediately at his own cost.
88	Software security references [QT&M, FP]	a. All web-based software architectures, design, development and deployment shall meet the IT Security Standard Web Application Security Standard, C(2018) 7283 Final (https://ec.europa.eu/transparency/regdoc/rep/3/2018/EN/C-2018-7283-F1-EN-MAIN-PART-1.PDF)

		b. and web Applications Secure Development Guidelines by EC DIGIT SECURITY ASSURANCE https://webgate.ec.europa.eu/fpfis/wikis/display/SecurityAssurance/EC+DIGIT+SECURITY+ASSURANCE+Documents c. The software deliverables need to pass the attack vectors defined in the OSSTMM (Open Source Security Testing Methodology Manual) in its current version. If the deliverables include web-applications or other web-based technologies, they need to pass all the vulnerability tests defined in the latest version of OWASP Application Security Verification standard ASVS 4.0 d. Mobile applications design, development and deployment shall meet the requirements and recommendations set in the latest version of Mobile AppSec Verification published by OWASP https://www.owasp.org e. All software products shall comply with Frontex cryptography policy as covered by Security Notice no. 18_2016 f. All software products shall comply with Frontex ICT Systems Assess Management covered by Security Notice no. 13-2016 g. The above-mentioned security notices will be made available upon initiation of the framework contract
89	Cryptography and Access [all types]	a. All software products shall comply with Frontex cryptography policy as covered by Security Notice no. 18_2016 b. All software products shall comply with Frontex ICT Systems Assess Management covered by Security Notice no. 13-2016 c. The above-mentioned security notices will be made available upon initiation of the framework contract
90	Personal Data Protection [QT&M, FP]	a. Any personal data shall be handled in line with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), personal data protection rules and practices and additional requirements to be identified at the start of the project. b. Software shall assure protection of any Personal Data to be processed in it "by design" and "by default" (Article 25 and Recital 78 of the GDPR). All measures and mechanisms for protection of Personal Data shall be included in all software development artefacts especially in TDD, documentation and tests. c. The developed software shall implement, where applicable, the guidance provided by European Data Protection Supervisor published in https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en d. System design (software, technical environment, operating procedures) shall follow Security Risk Assessment and Data Protection Impact Assessment DPIA (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236). e. The following not exhaustive list of specific features need to be designed, implemented and tested: - information notes and consent for processing personal data pushed to user - separation of personal data from other data wherever possible - user access to his personal data with possibility to differentiate access to its attributes - non-disclosure of personal data between users except attributes foreseen for sharing - configurable and defined access to personal data - reports on consent for processing personal data - anonymization and pseudonymization feature of data on request of subject - deletion (right to be forgotten) feature of data on request of subject - audit trail for access and changes to personal data - management of personal data lifecycle with defined retention actions and periods
91	Readiness for RESTREINT UE [all types]	Frontex may require that the software development artefacts are compliant and ready for accreditation at RESTREINT UE/EU REESTRICTED level.

8.8. Maintenance

No	Title	Description
92	Role [all types]	The primary role of the Maintenance is ensuring that the target system, within the scope of its software *Products* and software components, remains in perfect working order or can be restored to perfect working order under the defined conditions and service level requirements. The service shall also keep the system aligned with technological changes of its environment. Maintenance covers Preventive Maintenance, Corrective Maintenance and Evolutionary Maintenance. It may cover Adaptive Maintenance if ordered.
93	Scope [all types]	Maintenance shall be provided for all software components including server and client software, all layers including business and middleware, the bespoke custom application, COTS and OSS of the delivered systems or being a subject of this service and the entire solution. Maintenance covers components separately and jointly (integration and compatibility).
94	OSS and COTS Maintenance [all types]	Maintenance Service is limited to distribution of new versions, updates, patches, access to standard training materials and knowledge-base as being offered and provided by the Vendor of the OSS and COTS to wide commercial market in a standard way.
95	Solution Third Level Support [all types]	Maintenance Service shall be provided by the Contractor to Frontex for custom developed software as well as the entire solution which integrates various components including OSS and COTS elements and covers Preventive Maintenance, Corrective Maintenance and Adaptive Maintenance in the defined Service Window at the defined Service Levels for Incident and Problem Management Processes
96	Hotline Support [all types]	Maintenance Service shall be provided in form of interactive hot-line assistance in English to authorised Frontex users in solving urgent functional requests and sharing knowledge about how to best use the software (may cover OSS and COTS, custom code and the entire solution).
97	Guarantee [FP, QT&M]	a. The guarantee for newly delivered Products is provided at the price of the SC with no additional cost to Frontex. is included in the price of the SC. b. The guarantee covers Corrective and Evolutionary Maintenance. c. Frontex may order Third Level Support of any type (Basic, Standard or Critical).
98	External access [all types]	a. External access to the target system will not be granted by default to the Contractor. b. Frontex may decide, if in his interest, to grant temporary remote access in justified cases and define mandatory security requirements that have to be met by the Contractor. c. In exceptional situations, when solving an urgent incident which cannot be replicated in other environments, an assisted remote session to the Production Environment can be established for the Contractor's named staff. The named staff accessing the Production Environment must be previously authorised by Frontex and it is Contractors responsibility to ensure that no unauthorised personnel shall access the Production Environment. Such an exception may be applied temporally and under full control of Frontex. Contractor may access and manipulate merely the minimum of data for diagnostic and repair. The Contractor must not copy, must not delete and must not alter any data or logs. Any operation performed by the personnel accessing the Production Environment remotely, including view of data, must be logged for auditing.
99	Place of work [QT&M, FP]	Primarily the services shall be provided extra muros, however all on-site interventions shall be done at Frontex Headquarters.
100	Preventive Maintenance [all types]	The Contractor shall carry out regularly corrective maintenance tasks on his initiative to lower the risk of failures or to mitigate security vulnerabilities. That shall include, but is not limited to: distribution of patches, performing health checks, reconfiguration.
101	Evolutionary Maintenance [all types]	The Contractor shall implement all necessary modifications to the released software that are necessary for sustaining its full operational capability due to the modifications of underlying software products such as the upgrade of operating system, database or other infrastructure software.
102	Corrective Maintenance [all types]	The Contractor shall repair all failures (including degradation of performance below thresholds), vulnerabilities and bugs of the delivered Product and software components in order to restore it and keep in perfect working order.

103	Adaptive (Perfective) Maintenance [all types]	The Contractor shall implement changes to the current version of the delivered Products and software components or implement new features that improve the systems.
104	Diligent examination and diagnosing [all types]	a. The Contractor shall maintain the environment necessary for reproducing faults at his own premises. No transfer or use of production data in that environment shall be done without written express authorisation of Frontex. b. If the fault has to be diagnosed in the Frontex environment the Contractor has to be assisted by Frontex staff. c. The Contractor will not be allowed to make changes directly to the production environment. d. Contractor is obliged to examine the incident and problem in professional manner with diligent examination and possessing the knowledge of the Product in maintenance as well as the Frontex context. In case the Contractor can diagnose the incident or the problem with his environment and based on his knowledge of the Product and Frontex context, the request shall not be rejected, put on hold or set in pending mode even if more detailed information is to be provided by Frontex.
105	Work around [all types]	Any work-around shall be promptly exchanged for the final systemic solution that should be delivered as a regular release or patch.
106	New Versions [all types]	Any new release shall be compliant with the requirements set for software development, including the scope of testing, assisting documentation, and the sequence of deployment to specific environments.
107	Distribution [all types]	Distribution of patches, documentation, media and other related goods shall be included in the price of the *Service*.
108	Documentation [all types]	Any solution provided by Third Level Support shall be duly documented and reflected in the regular user, administrator and technical documentation.
109	Service window [all types]	Third Level Support shall be available in 3 options: • Basic available in Normal Working Hours • Standard available in the Normal Working Hours and Extended Working Hours on Normal Working Days • Critical available 24/7
110	Single Point of Contact (SPoC) [all types]	The Contractor shall nominate and inform Frontex about his Single Point of Contact for addressing all communications regarding Third Level Support. This person will be responsible for the coordination of all related activities (including prioritization, escalation and managing contract with third party vendors, monitoring thresholds) and reporting.
111	Incident management process [all types]	a. On T1, if needed, Frontex will escalate and send a Request for Intervention to the Contractor SPoC e-mail. Within T2 hours, the Contractor shall send a Request for Intervention Acknowledgement back to Frontex. The Contractor shall confirm that the incident description was received, communicate the unique incident number (ticket number) and indicate T3. b. If On-Site-Intervention is required then per a request from Frontex: Within T5 hours, the Contractor shall arrive in Frontex with proper tools for solving the specific incident. Within T4 the incident shall be resolved by the Contractor and verified by Frontex; Frontex will send a message to the Contractor SPoC e-mail stating the incident's closure. The Contractor shall send a message to Frontex clearly specifying the T1, T2, T3, T4, T5, the problem diagnosis and the actions carried out by the Contractor to solve the incident. **c.** If Remote Assistance is required and permitted by Frontex, then: Within T6 hours, the Contractor shall be available by phone for Frontex with the relevant information needed for solving the specific incident. Within T3 the incident shall be resolved by the Contractor and verified by Frontex; Frontex will send a message to the Contractor SPoC e-mail stating the incident's closure. The Contractor shall send a message to Frontex by e-mail clearly specifying the T1, T2, T3, T4, T5 (if exists), problem diagnosis and actions carried out by the Contractor to solve the incident.
112	Service level requirements for incidents [all types]	Definitions: T1: incident reporting time, times count from this moment in time T2: Incident-Notification-Acknowledgement-Time T3: Incident-Planned-Resolution-Time T4: Incident-Actual-Resolution-Time T5: On-Site-Intervention-Time

		Requirements: T2 must be less than 4 working hour T3 must be less than 24 working hours T4 must be less than 40 working hours T5 must be less than 40 working hours Temporary solution shall be considered as meeting the required threshold of T4 if the technical solution is coordinated and technically accepted by Frontex, it is implemented in T4 with no degradation in functionality and performance of the Solution and the deadline for delivering the permanent solution is agreed.
113	Problem management process [all types]	a. Frontex may organise an ad-hoc meeting notifying the SPoC via e-mail, in order to acknowledge the problem's existence and assess its impact. b. Within T1, the Contractor shall establish a register containing all incidents (and/or all devices impacted) associated with the problem. c. Within the T2 timeframe, the Contractor shall send to Frontex an action plan to solve the problem. The outcome of the action plan must be guaranteed by the Contractor who is supposed to have tested it before delivering the plan to Frontex. The relevant Test Reports shall be delivered to Frontex in advance, as the Contractor responsibility. d. Frontex may approve or refuse the action plan and the solution. e. If approved, then: Frontex shall send to the Contractor an e-mail of approval and within the T3 timeframe, while monitoring the implementation, the problem shall be solved by the Contractor. f. The progress on the action plan shall be monitored daily and reported weekly by the Contractor to Frontex. g. If refused, then: The Contractor shall propose a new solution with the additional help of manufacturers, or shall provide evidence proving that there is no acceptable solution to the problem.
114	Service level requirements for problems [all types]	Definitions: • T1: problem reporting time, request for preparing a file related to the problem • T2: days allowed for delivering an action plan to solve the problem • T3: days allowed for solving the problem Requirements (times count from T1): a. T2 must be less than 5 days **b.** T3 must be less than 10 days
115	Reporting [all types]	The Contractor shall monthly report to Frontex: a. Outstanding problems and incidents with related statistics and tracked history b. Detailed statistics of service level requirements showing all departures from the targets
116	Penalties [QT&M, FP]	In case the Contractor does not meet the required Service Levels requirements the Contractor is due the penalties equal to the fraction of the value of the yearly maintenance fee for the target system or the complete suite of OSS or COTS software as indicated below: i. 0.2% for a day of delay of T4 in case of delays for software of the production system that stops delivery of the services indicated in Appendix 4 ii. 0.1% for a day of delay of T4 in case of delays for software of the production system that does not stop business services iii. 0.02% for a day of delay of repair in the case of other delays. The penalties described here do not limit Frontex from applying the measures indicated in the GTCITC.

9. Implementation of FWC

9.1. Types of assignments

The work items performed under this FWC, following the definition provided in the GTCITC, may be contracted on the basis of Specific Contracts of the following types:

- Fixed Price (FP)
- Quoted Times and Means (QT&M)
- Limited Times and Means (T&M)

Each assignment of T&M or QT&M type under the FWC will be classified as:

- *Short Term* for for 30 man-days or less in total;
- *Long Term* for efforts estimated for more than 30 man-days in total;

By default, services shall be provided during Normal Working Hours, however Frontex may request the Contractor to perform in Extended Working Hours or on a 24/7 basis. The type of assignment shall be indicated in each Request for Services.

The Financial Proposal shall reflect the above differentiation of the types of assignments.

9.2. Ordering process

9.2.1. Reopening of Competition

Each time the competition is reopened, all framework Contractors will be invited to submit their proposals for the specific assignment described by Frontex in the Request for Services.

Frontex shall establish and communicate to the framework Contractors the deadline for submitting the specific proposals and the relevant award criteria for their evaluation.

In case of the Reopening of Competition for QT&M Specific Contract, the indicative criteria for the evaluation will be similar to the ones for the for the Hypothetical Scenario and are presented in chapter 4 of Annex VI Technical Proposal.

In case of the Reopening of Competition for a FP Specific Contract, the indicative criteria for the evaluation are presented in chapter 4 of Annex VI Technical Proposal.

In general, each Specific Contract shall be awarded on the basis of the most economically advantageous specific proposal, with the price/quality ratio corresponding to that used for awarding the framework contract

9.2.2. Specific Contracts

Whenever a new Specific Contract is required, Frontex will release to the framework Contractors a *Request for Services (RfS)*, which will define:

- In case of T&M services – the profiles of expert(s) requested, the volume, tasks to be performed, duration of the assignment, acceptance criteria, reporting requirements, venue of the assignment and other relevant conditions. The request will provide detailed evaluation criteria, i.e. the technical score (suitability of the proposed candidates: 60%) and the total price (40%).
- In case of QT&M services – description of services and products to be developed, service criteria and performance levels, definition of done, duration of sprint, set of requirements sufficient for calculation of

QUW and other characteristics as listed in 8.56 Software development for scrum-based software development The request will provide detailed evaluation criteria, i.e. the technical score (e.g. the suitability of the proposed architecture and design of the product, proposed team, its organization and competences for execution of the SC, the method of work of the team and effort estimation method: 60%) and the total price (40%).

- In case of FP *Services* or *Products, the Request for Services* shall specify the requirements for those services and products, objectives, deliverables, acceptance criteria, schedule, place of performance and other conditions. The request will provide detailed evaluation criteria, i.e. the technical score (e.g. suitability of the proposed solution design, method of work, project plan: 60%) and the total price (40%).

The actual evaluation criteria will be defined in each Request for Service at Reopening of Competition. The RfS might furthermore define a minimum threshold for technical score that must be met for the proposal to be eligible. If, after the receipt of Frontex Request for Services, the Contractor requires clarifications, these clarifications shall be prepared without delay and distributed to all Contractors. Such requests for clarifications shall not be admissible on the last five calendar days before the deadline for submitting the specific proposal. Unless the clarifications imply modification of the initial Request for Services, the deadline for submitting proposals shall not be extended.

Contractors shall submit their specific proposals in reply to the Request for Services within the deadline indicated in RfS by Frontex. The default deadline is 10 calendar days for T&M and QT&M contracts and 20 days for FP contracts. Frontex might establish a longer deadline if this is justified by the complexity of the assignment.

Each submitted proposals must be compliant with the Request for Services. It shall be valid for the duration indicated in the request but not less than 30 calendar days.

Each specific proposal will define:

- In case of T&M services - at least 1 compliant candidate for each required position at the prices not exceeding those defined in the FWC, together with the description of each candidate's tasks, reporting, quality assurance measures and other requested documentation (e.g. CVs, compliancy forms, diplomas etc.).
- In case of QT&M services – at least the proposed product architecture or description of the services to be provided in the defined levels, the description of the method of work in this SC including the tooling, description of the work estimation method and estimation of the effort needed for the fulfillment of the requirements in the Request for Services, the composition and organization of the team, description of team roles and competences, named list of team members or CVs of key members.
- In case of FP s*ervices* - offering delivery of the services and products according to the specification. The proposal shall provide: a project plan, organization structure, composition of the team, description of tasks, quality assurance measures, schedule, and technical description of the proposed solution. The price quoted shall not be higher than that calculated on the estimated effort per profile and the profile prices in the Contractor's Financial Proposal.

The proposals shall be evaluated and the results of this evaluation shall be communicated to the Contractors who have submitted the proposals.

In case of T&M services, the proposed candidates shall be available for video conference interviews during the validity of the proposal against the Request for Services. Frontex will propose 2 dates for interview of the candidates and at least one date shall be accepted. If none of the dates are accepted the proposal shall be considered as not valid.

The Contractor submitting the most economically advantageous offer will be awarded the Specific Contract, on the basis of the draft Specific Contract included in the Annex V Draft Service Contract.

The awarded Contractor must sign the Specific Contract within 5 working days of its receipt. Once the SC is signed by both parties the work shall start immediately unless the Contract specifies a later date of commencement. The implementation of the Specific Contract shall progress in coordination with Frontex without unjustified periods of inactivity.

9.3. Acceptance

The official acceptance of the work carried out, or of the goods delivered, will take place at pre-defined milestones during the implementation and at the completion of each Specific Contract. It shall be conducted against the quality or acceptance criteria set in the related specifications, Request for Services or in the related Product Description. In general, the acceptance process shall follow the terms and conditions of the GTCITC unless the Specific Contract has provided for different timings and steps for acceptance.

9.4. Obligation to perform

The conclusion of the FWC does not impose on the Contractor the obligation to submit a proposal in reply to each Request for Services; however, Frontex reserves the right to terminate the FWC with a specific Contractor in the following cases:

a) The Contractor does not submit the proposal for the Request for Services for the third time.
b) The submitted proposal for the Request for Services is evaluated to be below the minimum required levels for the fifth time.

9.5. Other costs

The prices included in the FWC and in the related SC are fully inclusive. No additional costs are eligible. This includes but is not limited to ordering, processing, logistics, communication, secretariat, customs, training, tooling and equipment used by the Contractor staff.

Reimbursements of incurred travel and subsistence expenses will be authorised only in case of SC with the place of performance being Other Locations and will be made in accordance with Annex V Draft Service Contract.

9.6. Payments

Payments for Specific Contracts will be executed based on Contractor's invoice and following the described below rules:

1) If the total amount of the Specific Contract does not exceed 100,000 EUR an invoice for the whole amount shall be issued at the completion of the work, based on a written Acceptance Form (Appendix 5) for all Specific Contract s and Attendance Sheet Form (Appendix 6) for T&M Specific Contracts, issued and signed by Frontex (to be attached to the invoice).
2) If the total amount of Specific Contract exceeds 100,000 EUR, the Contractor may claim may request to implement in the SC one of the listed below invoicing procedures followed by payment of the balance at the completion of the work
    a) a pre- financing payment of 30% of the total value of the Specific Contract on basis of the counter-signed Specific Contract;
    b) Interim payments on the basis of relevant progress report, stages, deliverable result or reference defined in the respective Specific Contract and approved Acceptance Form (Appendix 5).

If applicable, the chosen invoicing procedure shall be indicated by the Contractor in his financial proposal for Specific Contract and this preference shall be reflected in the Specific Contract, too.

Invoice may be issued upon completion of the related work and when the following applicable documents are duly completed and signed: Appendix 6 Attendance Sheet Form for the invoiced period. Every invoice shall be issued solely in relation to the single Specific Contract.

Invoices and the documents accompanying them are to be scanned and sent in pdf format (attached to an email) and addressed to invoices@frontex.europa.eu with the subject indicating the reference number of the FWC Contract and of the Specific Contract.

9.7. Framework Contract Management

The Contractor will nominate a FWC Contract Officer who shall act as a single contact point for vis a vis Frontex for the FWC matters for the duration of the FWC. That individual must be available for Frontex requests. All the contractual correspondence and related coordination will be addressed to that person.

The Contractor will nominate a Framework Contract Executive (henceforth referred as FWC Executive), who will be ultimately representing the Contractor's company and its subcontractors vis a vis Frontex for the performance management of the framework contract, as described in this tender. The FWC Executive may also performs the roles of SC Contractor's Manager for Specific Contracts.

The FWC Executive must be reachable during the Normal Working Hours. In case of absence, a back-up person has to be designated by the Contractor, informing in advance Frontex's Framework Contract Executive.

Framework contract management tasks include:

- Monitoring and proactive management of all Specific Contracts;
- Supervision of overall performance of the Contractor;
- Producing and presenting service reports;
- Participate in FWC management meetings with Frontex, either proposed by the Contractor or requested by Frontex;
- Managing sub-contractors (when applicable);
- FWC change management and escalation of issues not solved at the level of the SCs;
- Management of risks and issues;
- Communication with Frontex's Framework Contract Executive.

Regular FWC review meetings with individual Contractors will be organized by Frontex once per year (annual period counting starts at signature of FWC). These meetings will take place in Frontex's premises. Additional meetings may be organized upon request of Frontex or the Contractor, conducted on-site or using video conference systems.

Frontex will nominate a Project Manager who will be ultimately point of contact for Contractor for all issues related to execution of the Framework Contract. All the FWC's contractual correspondence and related coordination shall be addressed to the Frontex Project Manager.

9.8. Reporting and quality monitoring

Throughout the duration of the FWC, Frontex shall conduct accurate appraisal of Contractor's performance to determine whether the Contractor is executing the tasks assigned to him in accordance with the provisions of the FWC. To allow Frontex to regularly identify the progress made in execution of the tasks in accordance with the Tender Specifications and the TOR, the Contractor shall set up the appropriate monitoring, assessment and supervisory procedures. For these purposes, the Contractor shall propose all necessary details for the monitoring and reporting procedures, in particular the following:

- Schedule of interim and final reports
- Terms for approval, structure and content of each document
- Other consideration if addressed in best practices for monitoring this type of FWC

Frontex will monitor the quality of the service provided by the Contractor. The elements that will be monitored include:

- quality indicators as stated in the Service Level Agreement agreed with the Contractor
- Responsiveness to the released Requests for Specific Contracts
- effectiveness of providing staff with the appropriate skills as requested
- quality of the staff and the adherence to the profile requirements
- speed and agility of responding to tasks
- compliance of the proposals in response to Requests for Services
- adherence to deadlines
- quality of the programme/project management
- quality of the deliverables.

9.9. Underperformance

In case the Contractor:

- is not respecting its contractual obligations
- is not submitting compliant proposals against the Request for Services
- performs below the agreed levels
- his performance is frequently sub-standard
- his quotations for FP Specific Contracts repeatedly exceed market offers

it will be recognized as a breach of the Contractor's obligations under the FWC, in which case Frontex may consequently terminate the FWC in line with the provisions of the Contract.

9.10. Escalation

The Contractor shall continuously monitor the progress of work and the risks of underperformance. In case of registering an underperformance or assessing a risk of underperformance behind acceptable tolerances established in the project plan, the Contractor must report it to Frontex according to standard reporting procedures agreed for the Specific Contract. If the standard reporting procedure does not correspond to the urgency of the issue, or in the Contractor's perception the report does not reflect proportionally the reported underperformance or risk, the Contractor shall escalate it by *Means of Registered Communication* to Frontex.

In case of detecting a serious underperformance or a risk of underperformance of the Contractor, Frontex may escalate this observation to the Contractor by *Means of Registered Communication* and this requires that the Contractor's FWC Executive (at the level of the Board of Directors) will be available for Frontex to report on the issue and propose countermeasures at short notice.

10. Appendices

The following Appendices are included:

Appendix 1 General Terms and Conditions for Information Technology Contracts

Annex II Appendix 1 General Terms and Conditions for Information Technology Contracts in separate file

Appendix 2 Current ICT Baseline

Annex II Appendix 2 Current ICT Baseline in separate file

Appendix 3 Staff profiles

Annex II Appendix 3 Staff profiles in separate file

Appendix 4 Hypothetical Scenario

Appendix 4 Hypothetical Scenario in separate file

Appendix 5 Acceptance Form

Model of Task / Deliverable Acceptance Form

FOR SPECIFIC CONTRACT No ……… UNDER FWC No …………

Original document - duly signed - to be attached to the invoice

TASK / DELIVERABLE DESCRIPTION

Please give reference to the Terms of Reference and short description of the task or deliverable.

Please describe observations and reservations if any.

In case of Task/Deliverable rejection please detail reasons.

TASK / DELIVERABLE is ACCEPTED / REJECTED

To be filled in by Frontex:

Official responsible for acceptance (in block capitals):	
Date and signature	
Official responsible for final validation (in block capitals):	
Date and signature	

Appendix 6 Attendance Sheet Form

Warsaw, _____________

Year		
Month		
Specific Contract		
FWC Ref.No.		
Frontex Project Name		
Name of Contractor		
Name of Consultant		phone:
Frontex Project Manager		for approval

	Signature of Consultant	Date	1st Entry Time	1st Exit Time	2nd Entry Time	2nd Exit Time	Day (total working time)
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							
31							
Total Time worked for the whole Month							

Appendix 7 Declaration of Confidentiality

Tender procedure: Frontex/OP/300/2019/SB

Multiple Framework Contract with reopening of competition for the provision of Software Development services

Contractor's Personnel
Declaration of confidentiality

I, ____ (N*ame and Surname*)

in my function of _______________________________ *(full Function name),*

representing __________________________________ *(full Company name),*

hereby declare that I will treat the information and/or documents that are made available to me or generated in the context of the execution of the above mentioned contract with the strictest secrecy. No such information and/or documents will be divulged to any third parties.

I am aware that tasks carried out in view of the execution and/or performance of this contract also are governed by this principle of secrecy.

I am also aware of the fact that the principle of secrecy pointed out in the first paragraph will continue to apply after the completion of the above mentioned contract.

All information and documents received will be used solely for the execution and/or performance of this contract.

Name of the person: ______________________________

Signature: ______________________________

Place, date: ______________________________