Tender Specifications

for

IT Infrastructure services

Framework service contract

Publication Reference: OJ/2017/ICT/9196

December 2017

Table of Contents

Introduction to ECDC

The European Centre for Disease prevention and Control (ECDC or the Centre) is an agency of the European Union, established by the European Parliament and Council Regulation 851/2004 of 21 April 2004. Its purpose is to identify, assess and communicate current and emerging threats to human health from communicable disease. Within this broad mission statement, the main technical tasks of the Centre fall into the following four categories:

- The publication of independent scientific opinions, bringing together technical expertise in specific fields through its various EU-wide networks and via ad hoc scientific panels;
- The provision of technical assistance to EU member states, communication of the Centre's activities and results and dissemination of information tailored to different audiences;
- The development of epidemiological surveillance at the European level and the maintenance of networks of reference laboratories; and
- Early Warning and Response based on 'round the clock' availability of specialists in communicable diseases.

Further information about the Centre can be found on the ECDC website www.ecdc.europa.eu.

The tender process

The purpose of competitive tendering for awarding contracts is two-fold:

- to ensure the transparency of operations;
- to obtain the desired quality of services, supplies and works at the best possible price.

The applicable regulations, namely Directive 2014/24/EU and Regulation 966/2012, oblige the ECDC to guarantee the widest possible participation, on equal terms in tender procedures and contracts.

1 Overview of this tender

1.1 Description of the contract

The services required by ECDC are described in the terms of reference in **section 2** of the present tender specifications.

In drawing up a tender, tenderers should bear in mind the provisions of the draft contract in **Annex I**. In particular, the draft contract indicates the method and the conditions for payments to the contractor.

Tenderers are expected to examine carefully and respect all instructions and standard formats contained in these specifications and the invitation to tender. A tender which does not contain all the required information and documentation may be rejected.

1.2 Timetable

Activity	Date	Comments
Launching	05/12/2017	Dispatch of contract notice to the OJ
Site visit or clarification meeting (if any)	-	Not applicable to this tender
Deadline for request of clarifications	20/02/2018	Six working days before deadline
Deadline for submission of tenders	**28/02/2018**	At 16:00 CET
Interviews (if any)	-	Not applicable to this tender
Opening session	02/03/2018	
Date for evaluation of tenderss	Opening session date plus 1 week	Estimated
Notification of award to the tenderers	Evaluation date plus 1 month	Estimated
Contract signature	Notification date plus 1 month	Estimated

1.3 Participation in the tender procedure

This procurement procedure is open to the natural or legal person wishing to bid for the assignment and established in the European Union, European Economic Area and Stabilisation and Association Agreements countries.

Tenderers must not be in any situation of exclusion under the exclusion criteria indicated in section 3.1 of these tender specifications and must have the legal capacity to allow them to participate in this tender procedure (see section 3.2.1).

Please note that any attempt by a tenderer to obtain confidential information, enter into unlawful agreements with competitors or influence the evaluation committee or ECDC during the process of

examining, clarifying, evaluating and comparing tenders will lead to the rejection of his tender and may result in administrative penalties.

1.4 Participation of consortia

A consortium may submit a tender on condition that it complies with the rules of competition.

A consortium may be a permanent, legally-established grouping or a grouping which has been constituted informally for a specific tender procedure. Such grouping (or consortium) must specify the company or person heading the project (the leader) and must also submit a copy of the document authorising this company or person to submit a tender. All members of a consortium (i.e., the leader and all other members) are jointly and severally liable to ECDC.

In addition, each member of the consortium must have access to ECDC's procurement procedures as stated in section 1.3, and provide the required evidence for the exclusion and selection criteria (see section 3). Concerning the selection criteria, the evidence provided by each member of the consortium will be checked to ensure that the consortium **as a whole** fulfils the criteria.

The participation of an ineligible member of the consortium will result in the automatic exclusion of that member, and the whole consortium will be excluded.

1.5 Subcontracting

If subcontracting is envisaged, the tenderer must clearly indicate in the tender which parts of the work will be subcontracted. The total value of the subcontracted part of the services cannot represent the total value of the contract value.

If the identity of the subcontractor is not known at the time of submitting the tender, the tenderer who is awarded the contract will have to seek ECDC's prior written authorisation before entering into a subcontract.

Where no subcontractor is given, the work will be assumed to be carried out directly by the tenderer.

Security requirements (and all requirements in principle) applies to 3rd party of 3rd party (ie. any level of subcontractors).

1.6 Presentation of the tender

Tenders must be submitted through the electronic submission system (see point 3 in the Invitation to tender and Annex VII for further information).

Make sure you submit your tender on time: you are advised to start completing your tender early. To avoid any complications with regard to late receipt/non receipt of tenders within the deadline, please ensure that you submit your tender several hours before the deadline. A tender received after the deadline indicated in the procurement documents will be rejected.

Contact details for helpdesk can be found at the following link: https://webgate.ec.europa.eu/supplier_portal_toolbox/esubmissionFileProject/files/BT3/spotsHelpPage_en.html

See the e-Submission application testing to be done in advance under point 1.1 in Annex VII.

1.6.1 Language

Tenders must be submitted in one of the official languages of the European Union. ECDC prefers, however, to receive documentation in English. Nonetheless, the choice of language will not play any role in the consideration of the tender.

1.7 Contacts between ECDC and the tenderers

Contacts between ECDC and tenderers are prohibited throughout the procedure, except in the following circumstances:

1.7.1 Written clarification before the deadline for submission of tenders

Requests for clarification regarding this procurement procedure or the nature of the contract should be done **in writing only** through the eTendering website at https://etendering.ted.europa.eu in the "questions and answers" tab, by clicking "create a question".

Each request for clarification sent to ECDC should indicate the publication reference and the title of the tender.

The deadline for clarification requests is indicated in the timetable under section 1.2. Requests for clarification received after the deadline will not be processed.

At the request of the tenderer, ECDC may provide any additional information or clarification resulting from the request for a clarification on the eTendering website (see above).

ECDC may, on its own initiative, inform interested parties of any error, inaccuracy, omission or other clerical error in the text of the contract notice or in the tender specifications by publishing a corrigendum.

Tenderers should regularly check the eTendering website for updates.

1.7.2 After the closing date for submission of tenders

If, after the tenders have been opened, some clarification is required in connection with a tender, or if obvious clerical errors in the submitted tender must be corrected, the ECDC may contact the tenderer, although such contact may not lead to any alteration of the terms of the submitted tender.

1.7.3 Visits to ECDC premises

No site visits at ECDC's premises are deemed necessary for this procedure.

1.7.4 Interviews

The Evaluation Committee will not conduct interviews for this procedure.

1.8 Division into Lots

This tender is not divided into lots. The tenderer must be in a position to provide all the services requested.

1.9 Variants

Not applicable.

1.10 Confidentiality and public access to documents

All documents presented by the tenderer become the property of the ECDC and are deemed confidential.

In the general implementation of its activities and for the processing of tendering procedures in particular, ECDC observes the following EU regulations:

- Council Regulation (EC) No. 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents; and
- Council Regulation (EC) No. 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

The tender process will involve the recording and processing of personal data (such as a tenderer's name, address and CV). Such data will be processed pursuant to Regulation (EC) No. 45/2001.

Unless indicated otherwise, a tenderer's replies to questions and any personal data requested by ECDC are required to evaluate the tender in accordance with the tender specifications and will be processed solely for that purpose by ECDC. A tenderer is entitled to obtain access to their personal data on request and to rectify any such data that is inaccurate or incomplete.

If you have any queries concerning the processing of your personal data, you may address them to the ECDC Data Protection Officer dpo@ecdc.europa.eu. You also have the right of recourse at any time to the European Data Protection Supervisor for matters relating to the processing of your personal data.

1.11 Contractual details

The contract is a "cascade" multiple framework service contract *("the FWC"*) with the title: **ICT Infrastructure services.** As a derogation to the standard cascade multiple framework service contract only one provider will be active at a time, this type of cascade multiple framework service contract is called "sleeping cascade" framework contract.

As exact implementing conditions, quantities and/or delivery times cannot be indicated in advance, the ECDC intends to conclude a FWC, which shall establish the basic terms for a series of specific contracts (hereafter collectively referred to as *"orders"*) to be issued over its duration.

The FWC will be concluded in English. All formal communication related to the FWC and its implementation will be done in the language of the FWC.

The FWC shall be concluded in the form of separate but identical framework contracts with up to three (3) economic operators at most provided that there are enough economic operators who are not excluded (checked in the first stage of assessment), who satisfy the selection criteria (second stage of assessment) and satisfy the award criteria (third stage of assessment). Should only one tender be awarded, a single FWC will be signed.

After the evaluation the successful tenders will be ranked in the descending order with a view to establishing a list of contractors and a sequence in which they will be offered work when orders are placed. The second contractor in the order of the cascade will only be asked to provide the services foreseen in the contract if the contractor's framework contract first in the cascade has been terminated. The third contractor in the order of the cascade will only be asked to provide the services foreseen in the contract if the framework contracts with the first and the second contractor have been terminated. This proceeding is called "sleeping cascade".

The estimated maximum value of the FWCs is EUR 8.000.000 over a period of four (4) years.

A draft contract is attached to these technical specifications as **Annex I**.

Signature of the framework contract imposes no obligation on the Centre to order services. Only the implementation of the framework contract through specific contracts/order forms is binding for ECDC.

Each specific contract/order form will contain details of deliverables and timelines for particular services to be provided.

1.12 Electronic exchange of documents

Please refer to the draft contract attached to these technical specifications as Annex I. The related documentation can be found at: http://ec.europa.eu/dgs/informatics/supplier_portal/index_en.htm . Other applications currently under development may be implemented on a voluntary basis during the contract execution.

1.13 Additional information

By virtue of article 134(1)(e) and article 134(4) of the Rules of Application of the Financial Regulation, ECDC reserves the option to launch further negotiated procedure, with the contractor chosen as a result of the present call for tender, for new services consisting in the repetition of similar services during the four years following the signature of the original contract.

1.14 Type of contracts and contract execution

Services shall be provided on the basis of the below types of order:

- **Fixed-Price contracts**, which correspond to the order of a defined deliverables or to the order of application management services.
- **Quoted Time & Means contracts**, which correspond to the order of a number of person-days for defined sub-tasks.
- **Time & Means contracts**, which correspond to the order of a number of person-days of particular profiles performed inside or outside the Agency's premises.

In a Fixed-Price contract ECDC specifies the deliverables corresponding to the work to be delivered within an expected timeframe.

In a Quoted Time & Means contract (QTM) ECDC specifies in the service request the different services to be provided, namely the different sub-tasks to be executed in a project, as well as the duration of the specific contract. The agency may also specify the required profiles and the total maximum number of person days.

The agency specifies in the service request its needs for the profiles of the Framework Contract, the workload (e.g. person-days) per profile, the tasks to be carried out and the expected deliverables, as well as the place of performance. The service request can combine different profiles, with the requested individual workload.

The following table gives an overview which type of contracts are foreseen during the lifecycle of the framework contract

Scope of the contract	Contract type	Comment
Takeover of the current IT infrastructure services from ECDC / previous contractor	Fixed price	At the beginning of the FWC, 2 month duration
Regular standard service execution	Fixed price	Major part of the FWC in terms of duration and budget, from

		month 3 towards the end of the FWC
Outside office hours support	Quoted Times & Means	Addition to the regular standard service execution
Handover of the services to ECDC or follow-up contractor	Fixed price	At the end of the FWC, 2 month duration
Exceptional work in project mode	Times & Means	Only for exceptional projects or out of service activities

1.14.1 Fixed price contracts

Naturally at the beginning of the framework contract the takeover of the service will be contracted and at the termination of the framework contract the handover service each by a specific contract. In between, regular standard service delivery will be ordered for a defined period (fixed price service combined with outside office hours contingent). Usually this period will be for 12 months from February to February, but at the beginning and end of the FWC the duration might be different.

For the implementation of fixed-price contracts ECDC specifies in the service request the service type (contract phase) and delivery schedule. The Contractor must present an offer meeting the requirements as specified in the service request and associated annexes, such as the technical specifications, work packages, deliverables, and deadlines. The deliverables must be in line with the delivery schedule, and conform to the technical specifications of the framework contract.

Acceptance of the work under fixed-price contracts will be done by validation of the monthly service management reporting and a monthly work acceptance form. The invoicing shall be based on the acceptance of the deliverables by the Agency, independently of the workload that the Contractor has used to produce the deliverables.

The start of the contract based on a fixed-price order will be formalised by a kick-off meeting which shall take place within ten (10) working days following the signature of the order by both parties or as stipulated in the specific contract.

No later than three (3) working days before the kick-off meeting a detailed presentation of the team allocated to the execution of the order, a detailed version of the service delivery plan (or takeover or handover plan) shall be provided by the contractor for validation by ECDC.

ECDC shall have five (5) working days following the kick-off meeting to validate, or reject the team allocated to the execution of the order, the detailed version of the service plan or the takeover / handover plan. The contractor may be requested to provide additional information or introduce modifications to its proposal. In such situations an updated proposal shall be provided within two (2) working days following the reception of the request by the contractor.

1.14.2 Quoted times and means contracts

In addition to the fixed price service contract ECDC will contract a specific contract for requested work outside office hours that will be covered by Quoted Times and Means contracts. These quoted times and means acontracts will run in parallel (and in support to) the fixed price service contracts. The place of performance of the work can be either off-site or on-site (or both), depending on the needs of the Agency. ECDC will order a certain contingent of the work outside office hours and in case of need request the execution of this work throughout the contract period. The contractor will on monthly basis send an acceptance form for the of the work outside office hours and the approved version will be submitted in support to the invoice.

1.14.3 Times and means contracts

Outside the regular service ECDC might need additional consultancy services in exceptional and most likely rare cases. For this exceptional work in project mode ECDC would contract individual consultants of the contractor on the basis of Times and Means contracts.

For the implementation of Times and Means contracts ECDC specifies in the service request the needs for profiles of the Framework Contract, the workload (e.g. person-days) per profile, the tasks to be carried out and the expected services, as well as the place of performance. The service request can combine different profiles, with the requested individual workload.

The Contractor must present candidates that match the requested profile description as laid down in the service request and in line with these specifications. The Contractor shall provide the CVs (in Europass format) and/or certifications of the candidates, proposed for the implementation of the specific contract. The offer must also include the financial bid based on the unit prices of the Framework Contract. The prices must be all inclusive. Prior to the signature of the specific contract, ECDC will verify that the (team of) consultant(s) proposed by the Contractor meets the requirements of the service request of ECDC and of the profiles in the Framework Contract. Candidates proposed must be available for phone interviews (remotely or in person) and be available on the start date of the assignment defined in the service request.

The invoicing will be based on the number of person-days performed. In case of a Times and Means contract the Contractor can request payment only if accompanied by a work acceptance form and a time sheet signed by ECDC.

1.15 Currency of tender

The Financial Proposal Form in **Annex II** must be used to submit a tender.

The price for the tender must be quoted in euro. Tenderers from countries outside the euro zone have to quote their prices in euro. The price quoted may not be revised in line with exchange rate movements. It is for the tenderer to assume the risks or the benefits deriving from any variation.

Prices must be quoted free of all duties, taxes and other charges, including VAT, as the European Union is exempt from such charges under Articles 3 and 4 of the Protocol on the privileges and immunities of the European Union. The amount of VAT may be shown separately.

1.16 All-inclusive prices

Prices submitted in response to this tender must be inclusive of all costs involved in the performance of the contract (e.g. to include delivery, supply and installation, maintenance, travel, subsistence, etc). No expenses incurred in the performance of the services will be reimbursed separately by ECDC.

1.17 Price revision

Prices submitted in response to this tender shall be fixed and not subject to revision for Specific Contracts concluded during the first year of performance of the Framework Contract.

From the beginning of the second year of performance of the Framework Contract, prices may be revised upwards or downwards each year, where such revision is requested by one of the contracting parties by notice served no later than three months before the anniversary of the date on which the Framework Contract became effective.

Specific Contracts shall be concluded on the basis of the prices in force on the date on which they are signed. Such prices shall not be subject to revision.

See Article II.20 “Price revision” in Annex I – Draft contract for the formula used for the calculation of the price revision.

1.18 Costs involved in preparing and submitting a tender

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

1.19 Protocol on the Privileges and Immunities of the European Union

The Centre is, as a rule, exempt from all taxes and duties, and in certain circumstances is entitled to a refund for indirect tax incurred, such as value added tax (VAT), pursuant to the provisions of articles 3 and 4 of the Protocol on Privileges and Immunities of the European Union. Tenderers must therefore quote prices which are exclusive of any taxes and duties.

1.20 Payments

The distribution of payments and the mandatory reporting is detailed in Annex I – Draft Contract.

1.21 Financial guarantees

ECDC may require a pre-financing guarantee or a performance guarantee from the Contractor chosen as a result of this tendering procedure. When such guarantee is requested, the specific conditions related to the provision of a guarantee are included in the draft contract (Annex I). The costs for the guarantee shall be borne by the Contractor.

2 Terms of reference

The terms of reference will become an integral part of the contract that may be awarded as a result of this tender procedure.

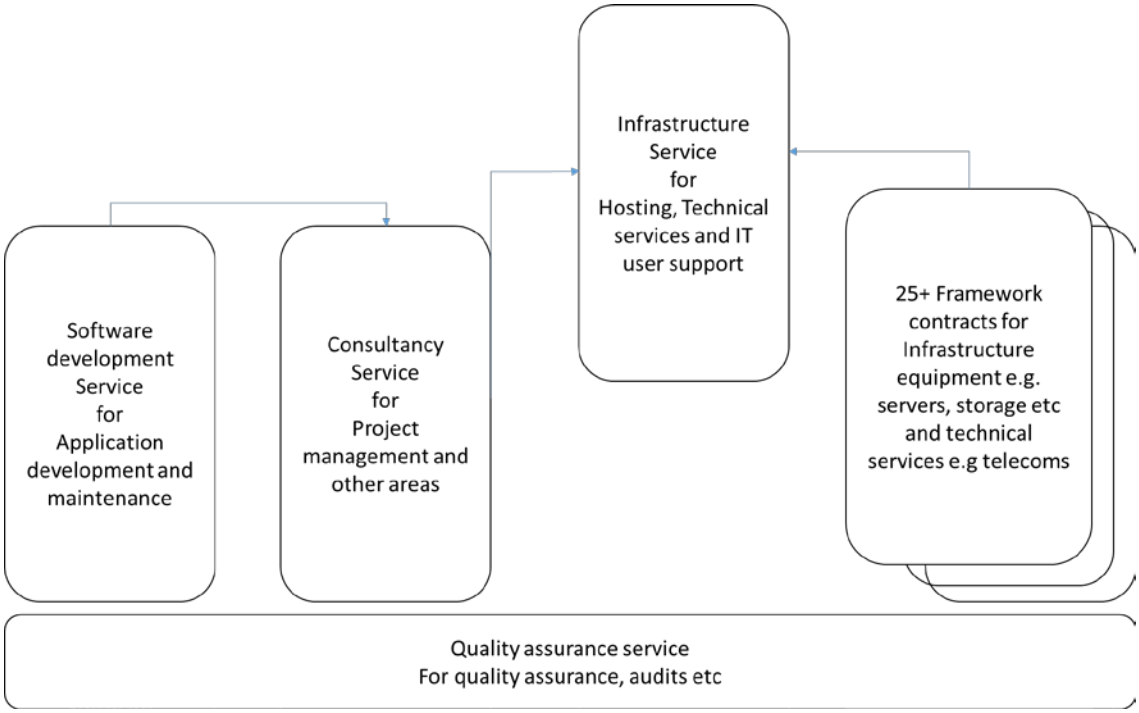
2.1 Introduction: Background to the invitation to tender

With high-level expertise in information and communication technologies, the Information and Communication Technologies (ICT) Unit at ECDC delivers studies, tools, application development and infrastructures to ECDC's operational and administrative stakeholders.

The work to achieve these aims is carried out by four sections:

1. Business Solutions (ICT-S): Being responsible for conducting studies and projects and maintaining IT products for all Units.
2. ICT-Quality (ICT-Q): Being responsible for ICT quality management including drafting of IT quality plan, IT quality policies and methodologies, overall coordination, planning and monitoring of the Unit resources.
3. (ICT-D): Development and maintenance of ECDC core business products.
4. (ICT-I): Providing front-end services, application hosting and enterprise infrastructure services.

ECDC is using a number of framework contracts to organise the overall IT projects and services rquired. Most of these contracts are already in place, while some will be launched later:



The scope of this tender is to support the infrastructure services for hosting, technical services and IT user support.

ECDC aims to migrate the current IT infrastructure services provided by several Times and Means framework contracts towards predominantly fixed price services.

ECDC Infrastructure services is currently provided by 3 different teams, provided by internal staff and consultants:

1. FrontOffice team – Provision of the end user services, support to the hosting services and end user related technical services.
2. ICT BackOffice – Provision of the hosting services and technical services.
3. Network, telecommunications and security - Technical services that are the foundation for hosting services and end user services.

FrontOffice and ICT BackOffice services are in scope of this tender and are described more in detail below.

2.2 Contract objectives and scope

The objective of this call for tender is the signature of framework contracts for predominantly the fixed price provision of FrontOffice and ICT BackOffice infrastructure services as well as for Quoted Times & Means contracts and Times & Means contracts as described in Section 1.14.

The high level objective of the framework contract is to:

1. Deliver outsourcing of services in scope (Frontoffice and ICT Backoffice).
2. Provide high quality of services – customer satisfaction is a key success factor and continuous improvement, innovation, increased efficiency etc
3. Provide secure and high availability access to all relevant resources necessary in supporting ECDC's activities for the relevant systems and services in scope.
4. Constantly improve the efficiencies and continuous improvement of the activities that fall under this framework contract.

The scope of the contract aims to cover the following elements:

1. Services to operate (see 2.2.1 and Technical Annex 2)
2. ECDC systems to operate under this framework contract (see 2.2.2 and Technical Annex 1 and Technical Annex 2)
3. Processes to operate for the execution of the service (see 2.2.3)
4. Work descriptions (see 2.2.4)
5. Requirements on the contractor's staff (see 2.2.5 and Technical Annex 3)
6. Security requirements (see 2.2.6and Annex VI of the Framework contract)
7. General requirements and conditions (see 2.2.7 and Technical Annex 6)
8. Contract phases to cover (see 2.2.8)
9. Framework contract governance (see 2.2.9 and Technical Annexes 4,7,8)
10. Exceptional work in projects mode (see Technical Annex 2.2.10 and Technical Annex 3)

Out of scope of this tender:

The network, telecommunications and perimeter security services are delivered fully by in-house staff and are thus not part of the framework contract.

The equipment (e.g. server, end user equipment) and technical services (e.g. cloud services) required for the Infrastructure services will be provided by other framework contracts and are for that reason out of the scope of this tender.

Minimum requirements

The follows aspects are essential for the offer as well throughout the contract execution:

1. All contractor's consultants working for ECDC need to have at minimum an ITIL foundation certification.
2. Compliance with the applicable environmental, social and labour laws.
3. Compliance with security controls as described in the section 2.2.6.2 and schedule of implementation should not exceed one month after signature of the relevant specific contract.

4. Fulfilment of all the mandatory Key Performance Indicators (KPI) as listed in the SLA Technical Annex 4.
5. All service delivery facilities must be located in the EU.

2.2.1 Regular standard Services in scope

The related services consist of end user services, hosting services and technical services. The list of services that will need to be provided in the export of the services is attached in the Technical Annex 2.

It is important to understand that the scope of the services will change over time by natural evolution and some services and systems will be retired or altered while new systems and services will be added during the execution of the contract. These changes will not be considered as a change to the framework contract.

2.2.2 ECDC systems to operate under this framework contract

2.2.2.1 Overview of systems

End user systems

End users at the ECDC premises use, with few exceptions, laptops with Windows OS. The Windows OS is usually on one main version (currently windows 7) and in parallel one new version that is deployed gradually (currently Windows 10). On these machines, users have standard office automation software and a number of small software applications that users are able to download themselves from the service portal and some software that can be requested. A full list of the current software in use for end users see Techncial annex 1 list of software. The list will evolve over time.

COTS systems

ECDC is using some COTS products for delivering business solution. One platform used in several cases is the product Microsoft SharePoint. It has been used for several bespoke systems as well for the ECDC Document management system.

Bespoke systems

Due to the nature of the agency, ECDC require a number of specialised systems for data collection and management, event management, alerting and planning. ECDC has developed around 30 mainly small bespoke systems, many of them on .NET, Sharepoint, ARC GIS and DRUPAL.

Audio visual systems

ECDC has large conference facilities and performs a lot of Video and Audio conferences. Video conferencing is based on CISCO hardware and software as well as Webex technologies.

2.2.2.2 ECDC IT environments to manage

The ECDC internal users are located at one physical location – the ECDC premises in Solna, Sweden. On a regular basis, ECDC users work remotely from home or on mission using VPN technology to reach all the ECDC systems. Currently, ECDC is in the process of introducing Bring your own device (BYOD) with mobile device management and several cloud based software services.

The majority of the external users using the external facing Web based services are located in Europe.

The main data centre is located at the ECDC premises, a backup data centre with mirrored services, currently in Cologne, Germany. Cloud services from different providers are always located in Europe (due to EUROPEAN DATA PROTECTION SUPERVISOR (EDPS) regulations).

Logically, ECDC has internal networks that are separated and secured against a Demilitarised zone (DMZ) network and the internet. Dedicated VPNs to key partners (e.g. the European Commission in Brussels, Belgium) or cloud providers extend the networks.

Printing/scanning facilities are offered by 14 Multi-Function Devices (MFD) distributed over all office floors and will include FollowMe Printing.

Most systems are maintained in production, UAT, test, development test and development environment.

2.2.2.3 User communities

On site users – ECDC has on its premises in Solna, Sweden about 300 users that require day to day support for the front end services and support for the hosted systems.

VPN users – Several of the ECDC users are performing regular missions, often within the EU, but sometimes worldwide. In addition, ECDC allows their users to telework from home. In these situations, the users use their laptop with VPN to reach ECDC systems and services. These users also require support via phone and remote desktop tools.

Nominated users – for most important external facing systems, the user communities are well defined and a clear process for their nomination is in place. The identity management system supports this process by linking the Customer Relationship Management (CRM) nominated users with propagation into the security directory. Via Single Sign-On (SSO), the users experience a single account and login. Many of the nominated user communities of the different external facing systems overlap with the core user community around 4000 users. ECDC has federated and aim to futher federate to some external identity management systems (e.g. to cloud provider).

Self-nominated users – Besides the core systems and the public website, ECDC has a few applications with low security / authentication needs, which require a low level of authentication, but are not open for everyone. For these systems users can create an account themselves and the only parameter validated will be the email address. There are currently around 3500 self-nominated users.

2.2.2.4 IT Service Management Tool

The contractor shall make use of the tool provided by ECDC, currently IVANTI Servicedesk. The contractor will be responsible to maintain and update the system, create, run or update the necessary reports, adjust the process implementation when necessary.

2.2.3 Processes to operate for the execution of the services

The following standard ITIL processes (with some adaptations) are currently used and expected to be provided by the future contractor. ECDC will have for each process a responsible staff member who will be the owner and supervisor for the process. The provider will be expected to execute, maintain and operate the processes. ECDC will coordinate and supervise the process execution. Several of the processes interface to other support groups e.g. to the ECDC network team for second level support or release deliverables from external providers.

2.2.3.1 Incident management

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimise the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.
ECDC's incident management process has some local adaptation from an ITIL aligned process.
Activities:

- Logging email, Service Portal and telephone initiated incidents
- Incident categorisation and prioritisation
- Initial investigation
- Technical escalation

- Further investigation/diagnosis
- Applying workarounds
- Resolution and recovery
- Closure
- Managing incident resolution clock
- Identify and notify related Problems
- Raising related Changes
- Escalating process and tool anomalies
- Attending incident review meetings
- Contributing to service improvement
- Monitoring incident queue and quality (Incident Manager)
- User communication

Excluded from this process is the management of the security incidents.

2.2.3.2 Request fulfilment

ICT Infrastructure aims to provide an excellent service to ECDC and our external users. The goal of the requests process is to fulfil all types of service requests in an efficient and timely manner with high user satisfaction.
The objectives of ECDC's Request fulfilment process are:

- To receive, log, validate, and fulfil service requests. Also monitor, measure, report, review and improve the services provided.
- Maintain user and customer satisfaction through efficient and professional handling of all service requests
- Provide a channel for users to request and receive standard services for which a predefined authorization and qualification process exists
- Provide information to users and customers about the availability of services and the procedure for obtaining them
- Source and deliver the components of requested standard services.
- Assist with general information, complaints or comments.

Activities to be performed are:

- Logging and categorisation of email, service portal, telephone and walk-in initiated requests
- Request prioritisation
- Request evaluation
- Request fulfilment (Deliver the requested service according to predefined process. See List of services, Technical Annex 2 -sheet Front End Services)
- Closure
- Proposing new request catalogue services

2.2.3.3 Change management

The purpose of the change management process is to control the lifecycle of changes of production systems, enabling beneficial changes to be made with minimum disruption to IT services.
Normally the change management is a post-project activity, but in ECDC it is combined with the Release and Deployment Management. Releases will be provided by ECDC development team or external providers.
Change Analyst Activities:

- Recording/capturing requests for change
- Describing the change instructions (Where appropriate)
- Preparing and testing rollback procedures
- Contributing to the definition and agreement of release and deployment management plans in line with business priorities
- Creating and testing release packages
- Integration testing (Where appropriate) (Performed by Tester Profile)
- Deploying release packages
- Performing post change data validation (Where required)
- Attending Change Advisory Boards (CAB) (Where necessary)

- Attending change reviews (Where appropriate)
- Rolling back changes
- Escalating process and tool anomalies
- Notifying Configuration Management of CI changes

Change Manager Activities:

- Accepting/rejecting/abandoning change requests
- Identifying change related stakeholders
- Organising and chairing Change Advisory Boards (CAB)
- Prioritisation and initial scheduling (estimate) of change activities
- Managing change resources
- Managing change reviews

In 2015 ECDC had performed a total of 263 changes and 147 deployments while during 2016 - 277 changes were performed and 160 releases deployed.

2.2.3.4 Service level management

Independent from the Service level management of the framework contract, the end user services and the hosting services are agreed with the business users with an internal SLA. Requirements of these SLA are reflected in the Key performance indicators of Technical Annex 4.

Service Level Management Activities:

- Gathering business requirements
- Advising on Data Controller compliance
- Drafting, negotiating and agreeing SLA's
- Set up service monitoring and reporting
- Service management tool and service catalogue maintenance
- Periodic, annual and ad-hoc service review meetings with the business including follow up activities and minutes
- Preparing and implementing service improvement plans

2.2.3.5 Service catalogue management

ECDC ICT infrastructure is offering to the internal users an online service catalogue. Here the users can see and request end user services and see the details for the hosting services. On the backend the service catalogue contains the technical services and for the analyst work, work-instructions or the request fulfilment instructions.

An export of the services is attached in the Technical Annex 2.

The service catalogue needs to be reviewed regularly to update the backend work instructions. Also retired or changed services need to be removed and updated. The work instructions for services helping the analysts to fulfil requests and perform successful troubleshooting need to be updated according to the evolution of technology

Per analysis of the unclassified requests the contractor should recognise if there are regular requests that are not yet defined in the service catalogue. This might also occur on specific request of an end user or IT manager. In these cases new services need to be created in the service catalogue.

Service Catalogue Activities

- Proposing new services
- Agreeing and documenting a service definition/description with all relevant parties
- Testing services
- Assigning services to service lines and publishing them

- Interfacing with the business and IT Service Continuity Management on the dependencies of business units and their business processes with the supporting IT services, contained within the Business Service Catalogue
- Interfacing with support teams, suppliers and Configuration Management on interfaces and dependencies between IT services and the supporting services, components and CIs contained within the Technical Service Catalogue
- Interfacing with the business to ensure that the information is aligned to the business and business process.
- Reviewing and maintaining services, descriptions and delivery processes
- Retiring services

2.2.3.6 Asset and configuration management

The IT assets need to be registered in the configuration management database (CMDB) and the CMDB needs to be maintained and regularly checked. This includes the need for labelling and registration of new IT assets and stock management for provision and return of equipment. The stock of assets need to be checked on a biannual basis and an audit of the assigned end user equipment needs to be done.

Asset Management Activities (Hardware):

- Attaching asset labels (received from Finance Section of ECDC)
- Importing assets to the service desk configuration Management System
- Deploying assets as required
- Tracking/updating changes in Configuration Management System (CMS) as appropriate
- Manual Audit (Bi annual – twice per year)
- End-of-life disposal procedures

Asset Management Activities (Software):

- Software request handling
- Initiating software purchase
- Providing workarounds
- Software storage

Asset Management Licenses

- managing/monitor license assignment / subscriptions
- Monitor installations – compliance (Audit)/usage/upgrades
- Assigning/de-assigning licenses (where applicable)
- Managing white/black lists

Configuration Management Activities

- Checking import logs
- Maintaining Service Maps and/or Configuration Item (CI) Structures (Relationships in CMS)
- Checking Audit reports and dealing with exceptions

2.2.3.7 Problem management

Problem Management is the process for managing the lifecycle of all problems. The primary objectives of Problem Management are to prevent problems and resulting incidents from happening, to eliminate recurring incidents and to minimize the impact of incidents that cannot be prevented. Problem management often require cooperation with 2nd and 3rd level support groups that can be ECDC internal or other external providers.

Problem Management Activities:

- Problem identification & logging
- Problem categorisation and prioritisation
- Problem verification / Rejection (Problem Manager)
- Negotiating problem resolution resources (Problem Manager)
- Problem diagnosis / root cause analysis
- Preparing workarounds
- Logging known errors
- Resolution preparation and testing
- Managing problem related changes
- Implementing resolutions
- Major problem reviews

2.2.3.8 Integration test and deployments

Integration test and deployment is part of change management. As this is an important work area it is explained here in more detail. Beside the integration test the functional testing is performed by other parties at ECDC and not part of this contract.

In order to ensure that the service design and release will deliver a new or changed service or service offering that is fit for purpose and fit for use.

Integration testing activities:

- Review business requirements and use/test cases, where needed produce own test cases
- Review issues and test reports from functional testing
- Review RFCs and TFS / code repository items
- Review stakeholder and solution requirements and prepare integration test activities (e.g. propose test cases for ECDC's/third party QA Provider's review and acceptance)"
- Create / maintain automation test scripts
- Maintain and document the ICT-I test environment (infrastructure, patches and updates)
- Planning & prioritization meetings
- Change test planning (with the change manager) and maintaining ServiceDesk system change records
- Deploy applications, patches and hotfixes into the ICT integration test environment
- Integration, regression and smoke testing
- Troubleshooting of defects in order to determine if they are code or environment related
- Perform infrastructure security and performance testing
- Record defects in defect tracking system
- Liaising with development section /external development providers over defects and work on reproducing them and finding quick/permanent fixes
- Producing test reports
- Reproduce issues found in production in order to assist troubleshooting by administrators

2.2.3.9 IT security management

The goal of the ISM process is to align IT security with business security and ensure that information security is effectively managed in all service and Service Management activities

Security Management Activities:

- Antivirus management (server & client)

- Patch management
- Bit locker management
- Local admin management
- Active directory management
- Load balancing (F5 managed by ECDC)
- Certificate management
- File system auditing
- Alert management
- Continuity planning & testing
- Backup management (Exchange, Client, Database, SharePoint & file system with optional encryption)
- Group policy management
- Contributing to security breach reporting
- Administration of the Symantec Endpoint Security environment
- establish security system baselines (hardening) for all relevant technologies such as operating systems, databases, applications.

2.2.3.10 Technology watch support

ECDC has domain expertise to define the technology selection, upgrade planning and architecture planning. Nevertheless, ECDC expects the provider to have expertise in that area so that upgrades, infrastructure planning etc. can be done in common agreement.

2.2.4 Work descriptions

The work to be covered by the contractors has the following work areas:

- **Work area 1**: "**Frontoffice**- user facing services including the service desk, service management, end user services and some technical services";
- **Work area 2**: "**ICT BackOffice** – background mainly the hosting services and technical services to support the hosting services and the end user services".

2.2.4.1 Frontoffice incl. Service desk and Audio Visual

This area represents the first line support and the single point of contact (SPOC) that an end user will have with the IT services of ECDC. As described in ITIL, it should manage all the entering tickets (phone, Service Portal, in person and/or email), solve them or escalate them to the next level if they need an advanced technical expertise or an on-site intervention. That is why within this service the contractor shall present a very good image and a high level of efficiency.

All these requests and incidents should be managed according to the defined process with a service desk tool and are called hereafter “tickets”.

The FrontOffice main responsibilities are to:

1. Provide First-Line and partly second line Support for all IT related issues to all internal and external end-users
2. To register and to classify received incidents and to undertake an immediate effort in order to restore a failed IT service as quickly as possible with a minimal disruption for the business, based on agreed service levels.
3. If no ad-hoc solution can be achieved, the first line support will transfer the incident to the second line support or to any other support team for 2nd or 3rd line support .

4. Correctly assign tickets to technical teams within the scope
5. The first line support also processes service requests and keeps users informed about their incidents or request' status at agreed intervals.
6. Follow up of tickets
7. Provide quality control on all tickets handled
8. Client computer management
9. User account Management
10. Participate in projects and changes related to the Service Desk services.

FrontOffice registers or completes the user's request by creating or updating for example a ticket for each incident and each request. FrontOffice receives and registers all calls and emails from the end users in a IT service management tool. It shall have the overall view of ECDCs environment and shall make full use of the tools (IT Service Management (ITSM) Tool, remote connection tool, etc.) in the accomplishments of their tasks. It shall resolve/fulfil or forward all the incidents/requests already during the 1st level support phase as far as no physical intervention is required.
Incidents shall be resolved/closed in such a way that provided documentation makes it possible to do a correct analysis of the type of incidents and its resolution, as well as to provide appropriate information leading to a problem solution where applicable. To ensure that the ticket represents the incident correctly and completely, the service staff should provide in the service desk tool at least the default end user information, incident details as well as prioritisation details the following information:

- The initial assessment,
- The actions performed,
- Theneeds of the end-user to the 2nd and 3rd line support.

FrontOffice is also in charge of the follow-up of the support activities. Examples of these follow-up activities are:

11. Reviewing all non-resolved tickets and reminding the assignee & escalate to Incident manager.
12. Ensure efficient “floor management” ensuring to quickly and dynamically (re-)assign staff to the technical teams that have an increase in workload.
13. Monitoring and escalating to ECDC’s IT infrastructure (IT-I) supervisor team or ECDC’s IT-I management in case of serious / critical outages
14. Detecting and avoiding the unnecessary (excessive) reassignments (ping-pong), ensure appropriate flagging and escalation.
15. Provide enhanced follow-up of Critical/Urgent tickets.
16. Reviewing the accuracy of the data encoded in IT Service Management (ITSM) Tool (currently IVANTI Servicedesk)
17. Monitoring the progress of Critical/Urgent tickets
18. Monitoring of acknowledgement of tickets by 2nd and 3rd level groups
19. Resolution within the target indicator timescales.
20. Depending on the priority, initiate an escalation to supervisors or to relevant ECDC stakeholders (process owners or work area responsible as per 2.6.1).
21. Client management tasks including client patch management, software deployment, image creation, image deployment, image updates, mobile device management, encryption and file backup of client computers
22. Ensuring Antivirus protection client infrastructure, monitor and maintain the client infrastructure
23. Preparing client related scripts, Active Directory administration, set up and update of documentation, procedures, reporting and processes
24. Monitoring of software usage

25. End user hardware support including laptops, mobile phones, phones, smart phones, tablets, scanner, printer, projectors, conference equipment
26. Audio Visual system design, installation, support and operating of audio-visual systems including sound systems, video conferencing, streaming, screens, video and still cameras and multimedia display equipment,
27. Technical conference and meeting support including maintaining and performing minor repairs on mechanical components of A/V equipment and the maintenance of voting systems
28. Support and user management of cloud hosted conference systems
29. Creation and updating of user documentation, related to Infrastructure systems and services
30. Performing user introduction sessions

The requirement to achieve a high resolution rate requires the FrontOffice to include an internal 2nd line support function. The FrontOffice 2nd line in line with the ITIL definition of the second line support is expected to:

31. Quickly free up first-line agent, thus improving call reception performance
32. Have the technical skill to resolve a high number of incidents assigned to them by the first-line support
33. Contribute significantly in achieving a high first-line resolution rate.
34. Respond to "How-to" questions or requests for coaching on standard office and corporate applications and assistance to teleworkers.
35. Logistic interventions (moves, transport of material, repairs, tracking) and the support for the end users hardware and software configurations and installation (remotely or in user's office), including local components, network connections, PC, phones, laptops, printers, screen and other peripherals.
36. Management of the audio-visual equipment (microphone, projectors, etc.) and end user coaching on this kind of material.
37. Management of the IT equipment inventory (bar code scanning) and stock (PC, phones, screen, printers, audio-visual equipment, etc.)
38. The 2nd line function require staff with special technical knowledge on one or more specific business applications and with a high degree of technical knowledge of the IT platforms related to the IT business service.

Part of the work is also the IT welcoming of newcomers: provision and update of the "IT starter kit for newcomers", contact with all newcomers to verify the proper operation of IT equipment and understanding of basic technical systems (identification, email, etc.). If necessary, a specific short-time coaching (not more than 20 minutes) should be proposed in the IT user support.

The FrontOffice team is also entitled to assign tickets to 2nd and 3rd level technical teams (e.g. the ECDC networks team, the ICT BackOffice service team, development teams or others), after due analysis of the ticket. The technical teams shall also be involved in problem management, problem definition, analysis and resolution, knowledge management activities, creating and maintaining knowledge.

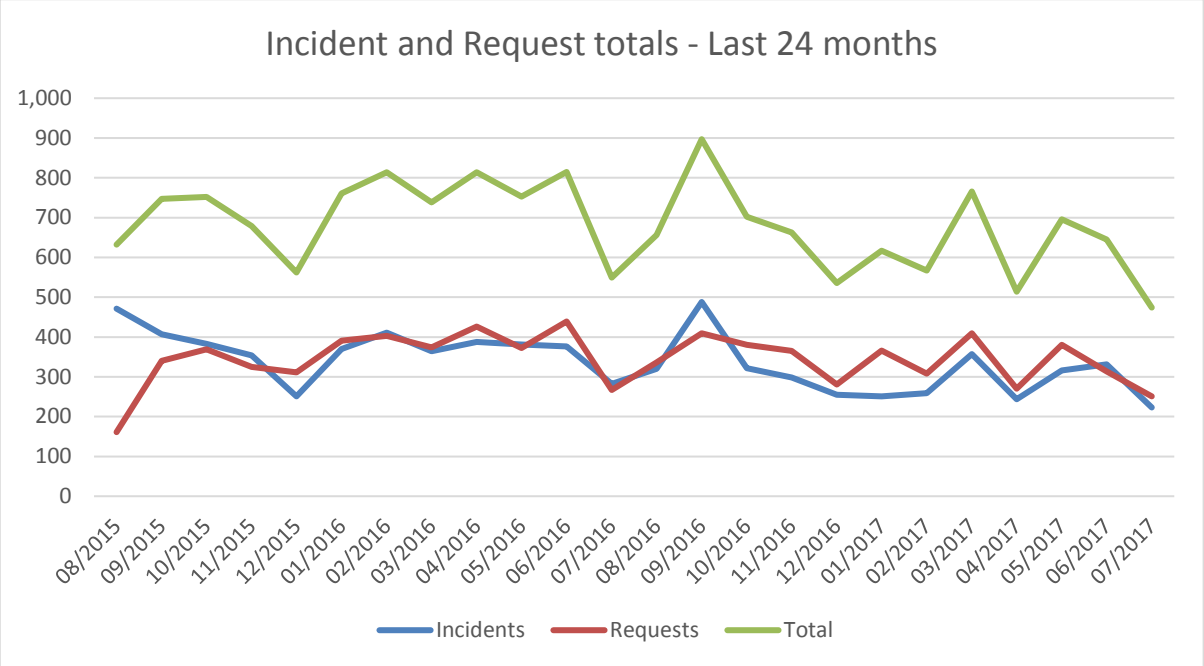
Additional tasks may be requested, e.g. coaching, logistic interventions, support for the end users hardware and software installation and configuration, support and management of audio-visual equipment, inventory.

The ECDC IT end user stock is currently composed of:

Equipment	Stockholm
Laptops	388
Desktops	34
Tablets (Microsoft Surface)	17
Monitors	594
iphones	20
ipads	22
Deskphones	375
Conference phones	10
Network Printers	27
Projectors	20
Videoconferencing Units	11

An average of 350 incidents and 350 of requests are recorded each month

The following graphics show the evolution of the activity over the last two years:



An incident is defined as an unplanned interruption to an IT service or reduction in the quality of an IT service.
A request is defined as a demand from a user for something to be provided – for example, a demand for information or advice, to reset a password or to install a workstation for a new user.
The main tools currently used by the Support team are:

- *IVANTI service desk* version 2016.4
  - Incident/request recording and monitoring
  - Statistics on incidents management/request fulfilment management
  - Change management

- *IVANTI management suite* version 2016.3
  - Remote control
  - Software and patches remote installation
  - Windows image deployment

The provider will be in charge of maintaining the Service desk tool and management suite. For new consultants and IT induction training should be done.

2.2.4.2 ICT BackOffice

The ICT BackOffice team provides 2nd and 3rd line support include the day-to-day operations, support and maintenance of applications, technology and platforms.

A key task of this team is to assure in a proactive manner Availability, Continuity and Integrity of the Services.
The IT technical services are responsible for all applications and all ECDC environments, being the only role allowed to manage and operate the different applications and underlying platforms of ECDC and to perform all necessary actions on these systems. A clear separation of resources between the production environment and the test environment is required.
The workload can be divided in 4 main areas: the management of the applications and systems; the application deployment; integration, support acceptance testing, software quality control; data centre services and virtualisation.

The area of management of applications and systems entails the following tasks:

1. Installation, configuration and operation of servers, both physical and virtual, cloud-based and on-premise (development, test and production environments), both Windows and Linux.
2. Server management/deployment tools/applications virtualization tools, configuration, maintenance and monitoring.
3. Ensure up-to-date patching of the server Operating Systems and their applications
4. Ensure up-to-date system and environment documentation
5. Installation of system and software components (operating systems, databases, application servers, web servers, and other Commercial Off-The-Shelf Products) in all the environments (if not carried out directly by suppliers).
6. Propose improvements to deployment of custom developed software
7. Monitoring of servers, incident and problem resolution, preliminary diagnosis of software and hardware problems in coordination with the local IT team and with third-party maintenance contractors.
8. Management of the SAN: management of LUN's, storage pools and groups, hosts, zoning
9. Monitoring of the SAN and follow-up of issues
10. Definition, validation and testing of the backup, archiving and disaster-recovery procedures and rules.
11. Advice to the local IT team in areas such as capacity management, contingency planning, IT service continuity management, automation of repetitive tasks, security.
12. Maintenance of the operation manual and the parts of the disaster-recovery plans related to local systems and applications.
13. Ensuring 24-hours 7-days standby IT support for critical systems.

14. Installation, configuration and management of office automation servers (Exchange, File Cluster, Print servers, Windows Domain - AD 2012r2/2016).
15. Installation, configuration, management and monitoring of SharePoint Environment (System Architecture, Permissions/Roles Management, Backup).

16. Installation, configuration, management and monitoring of Database Environment (System Architecture, Permissions/Roles Management, Backup), both Microsoft SQL and MySQL/Mariadb.
17. Actively monitor and control database performance
18. Installation, configuration and management of the archiving Environment (File and mail archiving).
19. Monitoring of office automation and applications servers, incident resolution, and preliminary diagnosis of software and hardware problems, coordination with the local IT team and with third-party maintenance contractors.
20. Opening and management of tickets with external providers. A regular and close follow-up of cases opened with the different software vendors is requested.

The Current server infrastructure in operation looks like this in numbers:

Operating System Version & release	**Total**
Windows Server systems (version 2012r2 and 2016):	**470**
Window 2016 physical servers	***45***
Windows virtual servers	***425***
Red Hat Enterprise Linux (RHEL) Server release xx instances **(x86)**:	**26**

Current software components in operation:

Database Version & release	**Total**
Database instances:	**142**
Windows SQL server v.2012r2 (64 bit) up to v. 2016 (64 bit)	***50***
MariaDB	***9***
Applications servers	**Total**
Applications servers	
Sharepoint	***159***
.NET and IIS	***60***
Apache	***10***
Main Commercial Off-The-Shelf Products	
MS Exchange	
Totara LMS	
Drupal	
Enterprise Vault	
K2	
CRM/MS Dynamics	
NetWrix	
LanDesk / Ivanti Management suite	

Team Foundation Server *Microsoft FIM* *Verint Telligent* *Bionumerics* *Microsoft project server* *QLIk*	

21. The contractor monitors the servers and the applications according to the agreed Service Level Agreement using several tools (Windows System Center Operations Manager).
22. The contractor manages incident and problem resolution using the ECDC Service desk tool, does preliminary diagnosis of software and hardware problems in coordination with the local IT team and with third-party maintenance contractors.
23. The contractor performs the Changes on ECDC's applications in Production using a change management and tracking system.

The area of application deployment and integration, testing, software quality control entails the following tasks:

24. Installation and configuration of any new information system in the test environment of the ECDC based on the installation/configuration documentation delivered by the information system supplier.
25. Integration of any new information system in the test environment of ECDC.
26. Integration testing of all new information systems based on test plans in order to ensure correct working of the information system after release in production. This includes the provision of a test report describing the tests performed, the observations made, conclusions and recommendations that can be made.
27. Validation of all new information systems (including the technical documentation) in order to evaluate the quality and adherence to directives and standards of ECDC regarding software deliveries.
28. Technical documentation of any new information system
29. Manage, configure, and administer the source code management system.
30. Interface with all stakeholders (service manager, IT project manager…) asking for application modifications and perform related tests in test environments,
31. Perform other regular tasks that include validation and test tasks,
32. Provide information about the information systems to help with trouble-shooting issues and give technical advice,

The area of data centre services entails the following tasks:

33. Hardware asset inventory, patching, intervention planning such as removal or installation of hardware.
34. Hardware management

The area of virtualisation entails the following tasks:

35. Define with the other teams several standard configurations
36. Ssetup "images" of standard configuration,
37. Design of templates to be used to request new virtual machines generated via our Standard Configurations available in the Service Catalog.
38. Ensure that the architecture can evolve (capacity to deliver new virtual machines),
39. Ssupport the load of the production services.
40. Monitor on a daily basis of the capacity of the Virtual Infrastructure
41. Design and creation of a "Service Catalog". Based on this, the contractor will have to instantiate "pre-configured" virtual machines.

42. Aanalyse performance issues. The objective is to identify the source of the bottlenecks and remove it to deliver the most efficient service possible.

43. A scaling of the Infrastructure where required: ECDC should be able to add additional resources to scale without impacting the production services.

44. The design of the Virtual Infrastructure must be done to minimize as much as possible any service disruption with the objective to reach the availability of the production services

2.2.5 Requirements on contractor's staff

The expertise and commitment of the assigned contractors staff is a key success factor for the quality of the services and for that reason ECDC has the below described requirements.

2.2.5.1 Requirements concerning the profiles

The proposed persons shall fulfil requirements concerning: education, knowledge, skills and expertise, experience and languages as specified in the corresponding profile definition (see Annexes 3).

The following tables define the CVs that have to be provided for the technical and professional capacity (3.2.3) for the proposed service team:

Work area 1 – FrontOffice services:

Profiles required (code)
Frontoffice analyst
Frontoffice administrator
Service Level Manager
AV support technician

Work area 2 – ICT BackOffice services

Profiles required (code)
Server administrator
SharePoint administrator
Database administrator
Integration Tester

2.2.5.2 Human resources issues and replacements

The following requirements have to be met:

- The contractor will ensure a security background check of contractor's staff and provide proof in case of ECDC request.
- ECDC reserves the right to verify, at any point of time, if the human resources fulfil requirements of the specifications. ECDC reserves the right to reject the human resource on the basis of insufficient quality qualifications. ECDC must request the contractor 20 working days in advance of desired changes on the human resources of the contractor.
- The contractor must replace human resource unable to carry out the assignments conforming to the specifications and required standards;
- The contractor must inform ECDC 20 working days in advance of any foreseeable human resource change. For a human resource proposed for the first time to ECDC, detailed information (CV) has to be provided by the contractor. ECDC reserves the right to reject the proposed human resource on the basis of insufficient quality qualifications.
- The initial human resource remains in place until the replacement is fully operational;
- A replacement has to be immediately operational when the original human resource is withdrawn;

- As a consequence of any replacement of the human resource an adequate handover respective introduction period of at least fifteen (15) working days must be foreseen. All costs related to the handover (e.g. training or travel expenses) are to be borne by the contractor;
- If the human resource is unavailable due to reasons beyond the contractor's control, the contractor has immediately to inform ECDC and make available an equivalent replacement (in term of profile) within ten (10) working days;
- The contractor has the right to ask for an adjustment to the profile attribution of a human resource. This request has to be accompanied by an updated CV, including a proposition concerning the new profile and a justification. The request has to be validated by ECDC. ECDC has the right to reject the request.
- For the scheduled absences (i.e. holidays, trainings) of a human resource, the contractor has to assure equivalent replacements (in term of profile). ECDC shall be notified no later than 10 working days before the beginning of the scheduled absence.

2.2.5.3 Training

The following requirements should be respected:

- The contractor will ensure that the contractors staff is trained in IT security (e.g. in the contractor's internal security awareness training).
- The contractor must provide sufficient number of training days per person and per year for its human resources involved in the contract's execution so that the person remains knowledge for the responsible technology.
- The number of training days are defined through indicators (see Technical Annex 4).
- The training shall be validated by ECDC and shall be in line with the technical background required for the corresponding profile as described in Technical Annex 3.
- The acquisition of new certifications should be a priority for the training plan of each human resource.
- All the costs are solely borne by the contractor and cannot be reimbursed in any way by ECDC. Moreover the man-days devoted to training cannot be invoiced in any way by the contractor to ECDC.

2.2.5.4 Knowledge and business continuity

Some aspects of ECDC's IT landscape and service requirements are rather complex. To perform effectively, the Contractor team must build up a good understanding of the service requirements and technical landscape. Both the Contractor and ECDC shall invest significantly in ensuring that the Contractor team members acquire sufficient business domain knowledge, technical expertise and command of the technical platforms.

Due to this investment, the Contractor must strive to best ensure that Contractor team members are committed to staying in service for the long term.

The contractor should always ensure the daily business Continuity of the service, meaning that each member of the team must be able to take over the tasks of the other members of the team during their planned or un-planned absence. This also means that regular training will have to be followed by all members of the team to stay at the "State of the Art" and get the capacity to ensure business continuity during the holiday's periods.

The contractor is responsible to organise the holiday planning and knowledge transfer in a manner the services are continued without any interruption.

2.2.5.5 Annual workload estimates for the standard services

As an indication, the following table contains an estimated distribution of the workload for the different processes in the 2 teams in % of the overall workload plus an estimation annual volume of workload based on the experience with the consultants currently in place based on:

- fixed prices for 220 working days and permanence days
- time and means working hours for technical interventions if necessary outside normal working hours.
- This estimation excludes the standby duty services

It should be noted that the offer is not necessary to be in line with this work organisation. It aims to help the tenderers to plan their capacity, but the organisation of work can be organised in different ways.

Work area 1 - IT Frontoffice

Process area	**(i) Fixed price**	**(ii) Outside office hours Quoted T&M**
	Estimation of the workload distribution % in Frontoffice	**Estimation of the annual workload in man-hours**
IT user support - incident management and request fulfilment	55%	20
IT user support administration e.g. imaging, patching, Antivirus etc	9%	10
Audio visual support	11%	10
Service level management	6%	N/A
Incident, problem and request management	6%	40
Asset management	2%	N/A
Change management	1%	N/A
Small projects e.g. upgrades, testing of client software etc	4&	N/A
Service desk Tool administration	6%	10

Estimates for Work area 2 - ICT BackOffice

Profiles[1]	**(i) Fixed price**	**(ii) Outside office hours Quoted T&M**
	Estimation of the workload distribution in % in ICT Backoffice	**Estimation of the annual workload in man-hours**
Server and system administration	8%	20

[1] Please refer to Annex 3 for a detailed description of the profiles.

Integration testing	15%	N/A
Sharepoint administration	12%	20
Database administration	13%	20
Change management incl. system deployments and upgrades	17%	100
Incident, problem management and request fulfilment	15%	20
Cloud and virtual machine management	7%	N/A
Data centre support	2%	10
Security management	5%	20
Small projects e.g. pilots, testing of software etc	5%	N/A
Asset management	2%	N/A

2.2.6 Security requirements

2.2.6.1 Off-site infrastructure requirements

ECDC will provide each consultant with a laptop with the standard ECDC configuration and software. This will include the VPN client software that will allow secure remote access to ECDC.
On addition to the laptop ECDC can provide a docking station, so that in the contractor's office the laptop can be used with external screen(s) and peripherals.
After completing the assignment, or when Supplier Personnel is transferred to other tasks, the contractor shall without delay inform ECDC of the change and return any hardware, visitor's badges and similar items.
The Contractor is responsible for to physically protect and secure the ECDC laptops.
Connections to ECDC should be done only from a controlled environment, which is secured against intrusion and protected by Antivirus. The contractor shall protect Information Processing Facilities against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures in supporting utilities. This includes physical perimeter and access protection.
The provider should not use his own hardware or software for the service delivery on the ECDC networks and systems. The contractor shall not store or process ECDC data on their equipment or cloud services.
ECDC reserves the right at any point in time during the execution of the contract to perform an on-site audit related to the Contractors infrastructure. During this audit ECDC will be supported by all technical teams necessary for a successful completion of the audit.
The contractor should outline in the offer from which office and where the offsite work will be performed.

A clear requirement from the data protection regulation on the contractor's infrastructure location is the need to have data processing within the EU.

The contractor has to provide a telephone number for ECDC users to call to register requests and incidents. This phone number should preferable be a local Swedish phone number without additional charges. The telephone system should be able to log the calls and provide statistics as per Key performance indicators. The system should not record messages and the retention time for logs should be 3 months only.

When, for the purposes of the services provided under the FWC and under the condition that no software is recommended by ECDC, the contractor intends to use its proprietary software or software belonging to a third party or parts of such software, the contractor shall seek ECDC's prior written assent when presenting its specific tender

For that purpose, the contractor shall:

- properly identify the software (by reference to its commercial name and version) and explain the intended purpose
- state whether the use of such software by ECDC or by third parties (for example the Member States, other institutions or persons and entities working for the ECD) will involve licence payments for development or use and provide an estimate of those payments.

Provided ECDC agrees with the use of pre-existing software a license agreement shall be signed between the parties specifying the modes of exploitation of such software and the overall amount of licence payments due for the whole duration of the licence.

2.2.6.2 Minimum security measures by Contractor

The contractor shall have a defined and documented information security management system (ISMS) including an information security policy and procedures in place, which shall be presented in the tender, approved by ECDC and communicated to relevant contractor personnel. Part of this should be to have defined and documented security roles and responsibilities within its organization.

The contractor shall have a defined and documented access control policy for facilities, sites, network, system, application and information/data access (including physical, logical and remote access controls), an authorization process for user access and privileges, procedures for revoking access rights and an acceptable use of access privileges for the contractor Personnel in place.

In case of subcontracting, the contractor shall reflect the content of these contractor Security rules in its agreements with sub-contractor that perform tasks assigned under the Agreement.

Access to the ECDC buildings by contractor's staff must be controlled in line with the ECDC physical access control rules:

According to the internal procedure *ECDC/IP/86 on access to premises* each member of contractor's staff working at the ECDC premises has to sign an individual non-disclosure declaration. After signature, each member of contractor's staff will be provided with a building access card. Everyone must visibly wear his/her identification card in the ECDC building. It is recommended not to wear it outside the building so as not to attract undue attention.

For access to the ECDCIT systems, staff must be controlled in line with the ECDC rules:

- Each member of contractor's staff working at ECDC must read, sign and comply the ECDC IT use policy (Annex 9)
- Each member of contractor's staff that will work on ECDC systems will sign a Declaration on confidentiality and security requirements (Annex VI of the framework contract)
- ECDC internal adaption of the EC(2006)3602 of 16 August 2006 of the Commission concerning the security of information systems used by the European Commission (Annex 10)

The following no disclosure rules must be respected:

- The contractor shall ensure that the contractor Personnel handles information in accordance with the level of confidentiality required under the Data protection Framework contract Agreement Annex IX .
- The contractor shall ensure that the contactor's Personnel uses a personal and unique identifier (user ID), and use an appropriate authentication technique, which confirms and ensures the identity of users. Administrative tasks should be executed using a dedicated, personal account with higher privileges on addition to the standard user account.

- Any information, data and/or materials of whatever kind or nature that is transmitted to the contractor related to ECDC shall be considered as proprietary to ECDC, unless explicitly released as public information and must be treated as such by the Service Provider.
- The contractor shall neither use nor copy ECDC information for any purpose other than the execution of the service agreement and shall neither directly nor indirectly disclose or permit such information to be made available to any third party without prior written authorization from ECDC.
- Third parties may not access the ECDC internal processing systems unless formal contractual agreement is signed.
- The contractor undertakes that it will only disclose any information to those of its employees, subcontractors, or any other third parties on a "need to know basis". Prior to disclosing any information to any third party the contractor will:
    - inform that third party of the restrictions on the use and disclosure of ECDC information,
    - ensure that the third party is bound by a confidentiality undertaking.

The ECDC production systems are subject to strict change control management. All patches and service packs must be tested and validated before promotion to production, while vulnerabilities of all relevant technologies such as operating systems, databases, applications should be managed proactively and in a timely manner Automated updates must not be used as some updates may cause applications to fail. The decision to install changes in production is taken by the ECDC Infrastructure manager. Installation is typically performed after business hours; otherwise the service interruption procedure must be used in agreement with the ECDC Infrastructure manager.

Development, test and production software must run on different systems. Test and development software should run on either physically separated systems or different virtual partitions. The test system environment should emulate the production system environment as closely as possible. Production data including sensitive or private data should not be used to test applications software.

The contractor has the obligation to report all security incidents, software malfunctions, security weaknesses or threats to systems or services that their staff notice or is made aware of to the ECDC infrastructure manager andthe ECDC LISO (Local information security officer).

ECDC has the right to monitor and examine any information stored on its information processing systems or communicated over its network or equipment. For several systems auditing is implemented to audit trail system changes and internet browsing.

All unnecessary system software, compilers, editors, and other development tools or system utilities are removed from the standardized ECDC production servers. All applications must be able to run on the standardised ECDC production servers configured to only offer functionality that is absolutely necessary for the provision of the envisaged service. Software must be controlled and checked to protect against possible covert channels and Trojan code.

2.2.6.3 Personal data protection

Personal data handling has to be done according to the specific data protection agreement (annex IX)

2.2.7 General requirements and conditions

2.2.7.1 Service hours

In line with the current IT service desk SLA the incident management as well as the request fulfilment service must available between 08:00 and 18:00 each ECDC working days. All other services must be operational between 09:00 – 17:00 each ECDC working day. ECDC has during 2017 242 working days.

It is up to the contractor to organize the service delivery so that the indicators defined in the SLA (see 2.2.7) satisfy the target or threshold.

2.2.7.2 Work outside service hours

In some occasions regular work need to be performed outside standard service hours e.g. for planned system upgrades, support for AV event outside office hours or in case a disease outbreak leads to extended office hours at ECDC.

ECDC acknowledge that the work outside office hour depend on various factors and might vary throughout and from year to year. **For that reason, will the work outside service hours not be included in the fixed price contract, but contract separately via a purchase order.**

Instead will ECDC order a contingent of hours for work outside office hours. The contingent will be used over time and when the contingent is used additional hours will be ordered. The usage of these outside service hour work will be done upon mutual agreement between the ECDC and the contractor's service manager.

The contractor is responsible to monitor the hours used in order not to execute hours without contract coverage. ECDC will not pay for work executed without contract coverage.

2.2.7.3 Standby service

Part of the IT services is the possibility to recover critical systems, support the Epidemiologist on standby, support special missions and disease outbreaks and provide first line support for one single critical system also outside office hours. For that purpose, a IT Frontoffice analyst and a ICT server administrator need to be available always on standby. Both work in cooperation with the ECDC IT manager on standby in case of need.

During 2016 in 20 cases of standby duty services were needed and during 2015 they were used 17 times.

During outside office hours (between 18:00 CET and 8:00 CET), weekends (Friday 18:00 CET until Monday 8:00 CET) and ECDC holidays (24 hours) the standby consultant will be provided with a phone and laptop and should be available to perform work as requested by ECDC.

Primarily the stand by duty service will be provided via remote access off site, but in case of need the consultant should be available on site within 1 hour.

While on standby duty, the consultant should always be available on phone and SMS and should check on the weekend twice a day (in the morning and in the afternoon) for service requests via email or the Sevice Portal.

The standby duty services should be included in the fixed price offer for the takeover, the standard service and the handover period.

Currently ECDC has the following profiles on permanent standby and the performance of each role is shifted on weekly basis:

Role	Tasks
FrontOffice analyst	Provide end user support to the Epidemiologist on standby, to EWRS users and initiate incident management for system outages
Server administrator	System troubleshooting and recovery for critical system outages
ECDC Manager	Escalation function to coordinate and supervise the standby intervention

In the future model the standby services will be covered partly by ECDC and partly by the contractor. The ECDC management role would be performed always by ECDC, while the role for standby of the IT Frontoffice analyst and the Server administrator would be for some weeks covered by ECDC and for some by the contractor. The number of weeks where the contractor would need to cover standby are the following:

Role	Weeks/ year performed by contractor	Weeks/ year performed by ECDC
FrontOffice analyst	42	10
Server administrator	42	10
ECDC Manager	0	52

The contractor and ECDC will agree on the schedule in which weeks the contractor will be responsible to perform standby duty early in advance.

2.2.7.4 On site and off site work

It shall be expected that a considerable part of the work under this Framework Contract will be carried out off-site at the Contractor's premises. However, the Tenderer acknowledges the requirement that for some profiles still a significant percentage of the work may require the Contractor to work in on-site mode at ECDC premises. In addition, the Tenderer acknowledges that when working in off-site mode and if so requested by ECDC, the Contractor shall undertake regular travel to ECDC premises to ensure efficient collaboration and smooth delivery of high quality services. ECDC will not reimburse any travel costs.

Consultants working at ECDC premises must comply with current and future rules at ECDC.

Where deemed appropriate by ECDC, ECDC staff involved in project, service or contract-related topics shall also travel to meetings taking place at the premises of the Contractor. This shall be done on mutually agreed dates.

In general, in order to ensure efficient overall execution of the FwC, a high level of interaction between the service managers, the service teams and ECDC personnel is required. Other means than on-site presence, such as online web conferences (e.g. using WebEx or similar tools), shall be encouraged and embedded to the normal ways of working between ECDC and the Contractor team members.

ECDC is aiming to provide the following office space for the provider within the ECDC building (although can not currently guarantee the number of available seats):

- Frontoffice/AV - **4 seats**
- ICT BackOffice - **1 seat**

ECDC expects that the available office space seats will be used not fixed to a dedicated person, but via a regular job rotation, so that different members of the contractor's personnel get familiar with the local environment and people at ECDC.

On site presence for the IT user support consultants (incl. AV support) is between 08:00 – 18:00, the contractor has to arrange a shift planning (e.g. 2 early shift working from 08:00 – 16:30 and 2 late shift working from 09:30 – 18:00)

On temporary basis in case of need additional desk space will be made available e.g. in case of additional onsite resources are needed to support for example an ongoing disease outbreak.

For the offsite work a certain level of proximity to the contractor's office will ease the job rotation and onsite meetings and is thus taken into consideration in the evaluation of the offer (see also 2.2.6.1)

2.2.7.5 Service level definitions

The service desk software currently used by ECDC provides some rules to classify the incidents treated by the support services.

The priority is determined according to the urgency and the impact. Those two criteria are defined by the initiator after the analysis of the incident. For details see the Annex 6 Incident and request priory matrix. Any exception details are provided in the incident logging tool.

Once the priority of an incident is determined the following business agreed targets are applied:

Incident priority	Working Hours	Response* Target (Working hours)	Resolution Target (Working hours)
1	24 Hours 7 Days	1	4
2	08:00 – 18:00 5 Days	1	8
3	08:00 – 18:00 5 Days	2	30 (3 Days)
4	08:00 – 18:00 5 Days	4	50 (5 Days)
5	08:00 – 18:00 5 Days	4	100 (10 Days)

*Response target is the measurement of time between creation and assignment to the correct analyst.

ECDC infrastructure is currently hosting 3 systems with the business impact assessment (BIA) priority 1, 6 systems with BIA priority 2 and 18 systems with BIA priority 3.

2.2.7.6 Language requirements

The working language of the Agency is English. The English language shall be used throughout the execution of this Framework contract for all communication, reports and other documentation.
Therefore, it is required that all members of the Contractor's staff involved in the FwC have working knowledge of English. In particular, whenever a particular person is required to work on-site at ECDC, or otherwise needs to be in collaboration with ECDC staff during the assignment, it is necessary that the person possesses understanding, speaking and writing English language skills at level C1 (Common European Framework of Reference for Languages) as a minimum. ECDC reserves the right to request the replacement of a resource if s/he does not have the adequate knowledge of English as deemed necessary for the execution of the tasks.

2.2.7.7 Communication and documentation

Transparency, good communication and documentation are a key success factor for a service provider and ECDC expects the contractor to pay attention to this area.

Part of the Frontoffice work is to keep the end users informed about planned maintenance, outages, security warnings or give proactive advice. Good user guidelines help to limit the workload and troubleshooting guidelines ease the work and lead to consistent results.

Part of the transparency is to provide statistics in a monthly dashboard about availability of hosting services and enterprise infrastructure services, call number and resolution compliance, number of standby interventions, number of releases, test and changes. For system outage and security incidents an incident report is provided (see attached Annex 7 sample of an incident report).

The provider will contribute to all these communications and documentations.

2.2.7.8 Close co-operation with ECDC and with 3rd Parties

Throughout the delivery of services, the contractor shall be required to co-operate closely with ECDC and/or 3rd parties with which ECDC has signed contracts, in order to achieve integration or synchronisation between other projects, products, or services. E.g. for a new application both parties have a common

interest for a smooth deployment of the application. This will require good cooperation and mutual support e.g. for troubleshooting.
Another example is when the Fontoffice need to create an incident with an external vender e.g. open a ticket with Microsoft or make a subscription for a mobile in order to provide the service. In such cases, the Contractor shall interact directly with a 3rd party upon approval of ECDC.
Primarily, unless otherwise specified in the specific contract, the interaction will take place via ECDC's ticketing system (currently IVANTI service desk).

2.2.8 Contract phases

The lifecycle of the contract will have 3 phases: in the takeover phase the supplier will learn and take over the services. After the takeover phase, the regular standard service provision will take place. At the end of the framework contract the handover phase will ensure a controlled termination of the contract and handover of the service delivery to the next service provider or back to ECDC.

2.2.8.1 Takeover phase of the existing services

The objective of the takeover work is that the contractor performs the necessary activities such that by the end of the takeover period, the contractor is in a position ready to start the IT services and IT operations activities independently and without any interruption of services.
The contractor shall actively engage and collaborate with ECDC and the previous Contractor (or any other 3rd party acting on behalf of ECDC) in order to build up the necessary knowledge and set up the necessary technical, operational and administrative infrastructure and systems.
ECDC will ensure that the parties with which the Contractor needs to cooperate with are available, and that the appropriate material including documentation, is made available to the Contractor, for the purposes of taking over.
Typically, there shall be different independent 'takeover' phases for different services. Some of these may run in parallel. Takeover of individual service duration will vary according to many factors including the timeline requirements of ECDC, and the complexity of the service being taken over. ECDC will provide human resources to support the takeovers.

ECDC would like to state that takeover activities are meant to transfer knowledge from one party to another so that the party receiving the knowledge becomes fully independent of the other party. It is expected that the contractor executing the takeover activity (i.e. the party receiving the knowledge) will take a pro-active, leading role in this activity. The contractor will name a main contact responsible for the overall takeover coordination. By the end of the activity, ECDC must have confidence that all of its services will run without interruption once the takeover to the contractor is completed. It is therefore strongly recommended that the contractor provides continuity in the profiles executing and participating in the takeover activities and the profiles running the service afterwards.
For an efficient and effective knowledge transfer ECDC foresees that some handover / takeover activities will be performed onsite at ECDC.
Regular progress meetings will take place during the takeover period in order to monitor the progress. The progress of takeover activity shall be reported to ECDC identifying relevant risks (and their mitigations) and issues. In addition, a takeover report describing the activities performed during the takeover, achievements, lessons learned, and risks and issues, as well as explaining the procedures and technical means (e.g. infrastructure) put in place shall be delivered ten (10) working days before the end of the takeover period, at the latest. ECDC shall have ten (10) working days to accept or reject the report. The contractor may be requested to provide additional information/introduce modifications to the takeover report. In such a case, an updated takeover report shall be provided within two (2) working days following the request reception by the contractor. It is advised to the contractor to deliver draft versions of the takeover report to facilitate the acceptance of the final version.

The tenderer has to propose and describe a solution to smoothly take in charge all the operations.

The proposal should describe in a structured way how the new contractor shall:

- set up the services during the takeover phase including procedures, accesses, working infrastructure and its security aspects,
- make their human resources familiar with the ECDC's environment: key-persons, procedures, tools, software, methods, applications, services and their documentation,
- take over all unresolved issues in the scope of their activities reported in the issue tracking system during the takeover period,
- demonstrate its capacities to deliver the services requested.

The proposal will include a detailed planning with a list of all the tasks and their deliverables foreseen by the tenderer during the takeover phase. For each task, a brief description and the estimated effort in man-days per profile have to be also indicated.

Appropriate number of regular meetings should be foreseen and organized by the contractor.

The kick off meeting will be the first meeting during which the following items are presented:

- the organisation of the contract (structure, human resources and their profile / roles),
- the SLA,
- the proposed takeover planning.

A final report will be delivered not later than five (5) days before the end of the takeover phase for acceptance of the takeover.

ECDC reserves the rights to visit the contractor's premises in order to check the eventual infrastructure and its security aspects put in place in the framework of the contract.

2.2.8.2 Takeover costs and duration

The tenderer must specify a fixed price for the takeover phase under specific conditions.

At the start of the framework contract the first contractor on the cascading list shall implement the takeover phase. The contractor must be ready to provide the requested services the day after the arrangement with current contractor ends, as long as the FWC has been signed by both contracting parties.

Should the framework contract with the first contractor in the cascade be terminated the second (or third) contractor on the cascading list would be requested to implement the takeover.

The takeover phase should be completed within 2 month.

2.2.8.3 Handover phase

The objective of the handover is to ensure a complete, timely, suitable and smooth transition between the contractor and ECDC or with the next service provider.

The contractor will hand over to ECDC or to next service provider all specific activities and existing tools, which have been acquired, developed and operated for the purpose of the service of the contract.

The latest version of the SLA and Service management reporting will be delivered to ECDC.

Handing over the services cannot have a negative impact on the business services or potentially create services level degradation: business continuity and quality of the services should be maintained. This is also the case where a transition phase takes place between the current and the next contractor – the current contractor should fully co-operate with ECDC and the next contractor.

No distribution of the on-going work or any other kind of cross-work between the existing contractor and the future one is foreseen.

A handover phase could be launched:

- in case of termination or upon expiry of the contract,
- at any moment of the course of the contract upon request of ECDC.

Upon termination of the FWC, the contractor is obliged to execute the handover, but the handover will be subject to an individual specific contract.

The contractor has to propose and describe a solution to smoothly handover all the operations.

The proposal should describe in a structured way how the contractor shall deliver the handover report and will include a detailed planning with a list of all the tasks foreseen during the handover phase. For each task, a brief description and the estimated effort in man-days per profile have to be indicated.

Appropriate number of regular meetings should be foreseen and organized by the contractor. During the first one the handover planning is presented.

A final report will be delivered not later than five (5) days before the end of the handover phase for acceptance of the handover.

The final report will describe or contain:

- how the services have been set up,
- the consolidated report with all the reports delivered during the contract's duration,
- the backups of the entire software configuration of every service component stored in a secure manner prior to its delivery to ECDC,
- the archives and all associated information according to specifications defined by ECDC,
- the tools or scripts and all data that have been managed, further developed or newly developed under the contract),
- all relevant documentation and working procedures,
- the list of all unresolved issues in the scope of its activities reported in the issue tracking system,
- recommendations of improvements,

In case of termination or upon expiry of the contract, all computer hardware, software and other equipment paid for or provided by ECDC shall be handed back by the contractor. This also applies to all documentation. The contractor will destroy any security critical information and piece of software that was provided by ECDC for the purpose of accessing its servers during the execution of the contract. This may include sensitive information, passwords, encryption keys, personal data of persons involved in the project, firewall and router configuration files, etc.

ECDC reserves the rights to visit the contractor's premises to check the eventual infrastructure in place.

2.2.8.4 Handover costs and duration

The contractor must specify a fixed price for the handover phase. The handover phase should be completed within 2 month.

2.2.8.5 Regular standard service phase

Between the period of take over phase and the hand over phase regular standard service provision will take place, where all the above described services should be delivered according to the below described governance.

2.2.9 Framework contract governance

2.2.9.1 Governance responsibilities

ECDC will designate an official responsible for monitoring of the proper execution of the FWC in general, one for each work area and one for each process.

The contractor shall designate a Service Delivery Manager or an Account Manager (SDM or AM) who will have an overall responsibility for the execution of the FWC. For each work area and for each process a technical manager will be assigned. In the SLA the names and contacts of these responsible should be defined and updated in case of change.

:

The costs related to the FWC management shall be included in the prices foreseen in the price schedule and shall not be invoiced separately.

2.2.9.2 Service level agreement (SLA) of the framework contract

The SLA should define the areas of activities, their services and their related levels that match the quality requirements expected by ECDC. The contractor will make a proposal of the SLA as part of the offer, which shall base on the technical Annex 4 Draft service level agreement.

Thus the establishment of the SLA ensures that ECDC and the contractor share:

- A common understanding of the levels of services required in the key areas of activities;
- A common approach in measuring the levels of provided services.

The SLA is intended to establish a clear set of measurable parameters against which the performance of the contractor will be measured.

The Service level agreement will be measured by key performance indicators. ECDC might involve a third party QA Provider that will support ECDC with the monitoring and follow up of the contractor's performance. The QA provider support areas are:

Review of service reports

Contribute to analysis and recommendations

Audits to verify service report information

2.2.9.3 Key performance indicators

A set of relevant key performance indicators is defined in the SLA and is the basic metrics to monitor the execution of the FWC.

2.2.9.4 Penalty point system on the Key performance indicators

When a key performance indicator is not met a deep analysis of the root-causes need to be performed and some consequences may arise at various levels:

- CONTRACTUAL: see article I.11 of the FWC.
- TECHNICAL: the service or indicator should be reviewed.
- HUMAN RESOURCES: ECDC may request exchange of the consultant
- Penalty points collection based on the Key performance indicators

2.2.9.5 Service management reporting

Service management reports are produced by the Contractor's service manager and handed over to the responsible service manager at the Agency. Generally, monthly reporting on the service management activities is required and needs to cover all the aspects related to service management. A template for the service reporting is included in Technical Annex 8 draft service reporting template.

ECDC might involve a third party QA Provider that will support ECDC with the monitoring and follow up of the contractor's performance. The QA provider support areas are:

- Review of service reports
- Contribute to analysis and recommendations
- Audits to verify service report information

2.2.9.6 Meetings and travel

The work for this FwC will include on-site meetings (at ECDC) as necessary during the implementation of the framework contract.
The chairmanship of the meetings lies with the Agency, and the responsibility for keeping the minutes for meetings between the Contractor and the Agency lies with the Contractor, unless otherwise decided by the Agency.
Based on mutual agreement some meetings may be concluded via audioconferences or videoconferences.

The frequency of the working meetings will be defined individually, whereas the steering committee meetings will be held every month, although the frequency may be modified depending on specific situations.

Meetings may be arranged at short notice meaning that the contractor must be available within 3 working days.

The costs of all meetings shall be included in the prices and shall not be invoiced separately.

For each meeting/remote conference (audio and/or video), the contractor shall:

- prepare an agenda and distribute it at least two (2) days before the meeting;
- ensure the participation of the relevant contractor's staff;
- draft detailed meeting minutes including additions to the Action Items list, and submit them to ECDC for comments within five (5) working days following the meeting;
- collect and integrate the corrections requested by ECDC to the meeting minutes during ten (10) working days following the submission of the draft version;
- distribute the final version of the minutes.

2.2.9.7 Steering committee meeting

A Steering Committee shall be established for the duration of the Framework Contract. The Steering Committee consists of representatives of both parties and is responsible for overseeing the overall implementation of the Framework Contract and for addressing escalated issues regarding the Framework Contract and the implementation by specific contracts.

2.2.9.8 Regular incident review and other technical meetings

Some processes will require regular technical meetings, taking place at ECDC or via online meetings. These will be defined during the takeover period. These will include e.g.:

- Daily review of incident to pending incidents, stop clocks etc
- Weekly review of incident with proposals for reduction of incidents.
- Weekly change approval board meeting
- ICT BackOffice deployment planning meetings
- System administration meetings for ICT BackOffice coordination of work every 2 weeks.

2.2.10 Exceptional work in project mode

On addition to the above described services that should be all included in the fixed price services, ECDC would like to reserve the option to order consultancy that would be requested and delivered outside the scope of the services.

Such necessary consultancy could be necessary to operate projects or other activities that are not within the scope of 2.2.1 - 2.2.9.

This type of consultancy is expected to be required only on exceptional cases.

The implementation of these will be by specific contracts times and means.

The contractor shall offer the profiles of Annex 3 with prices for times and means contracts with hourly prices intra muros and extra muros ECDC.

3 Exclusion and selection criteria

3.1 Exclusion criteria

All tenderers shall provide a declaration on their honour (see Annex III), duly signed and dated by an authorised representative of the tenderer, stating that they are not in one of the situations of exclusion listed in the Annex III.

The successful tenderer shall provide the documents mentioned as supporting evidence in Annex III before signature of the contract and within a deadline given by the contracting authority. This requirement applies to all members of the consortium in case of joint tender.

The contracting authority may waive the obligation for a tenderer to submit documentary evidence if such evidence has already been submitted for another procurement procedure and provided the documents were issued not more than one year earlier and are still valid. In such cases, the candidate or tenderer must declare on his honour that the documentary evidence has already been provided in a previous procurement procedure, provide reference to that procedure, and confirm that there has been no change in the situation.

3.2 Selection criteria

All tenderers shall provide the declaration on their honour (see Annex III), duly signed and dated by an authorised representative of the tenderer, stating that they fulfil the selection criteria applicable to them.

3.2.1 Legal capacity

Requirement
A tenderer is asked to prove that they are authorised to perform the contract under the national law as evidenced by inclusion in a trade or professional register, or a sworn declaration or certificate, membership of a specific organisation, express authorisation or entry in the VAT register.

Evidence required
The tenderer shall provide a duly filled in and signed Legal Entity Form (see **Annex VIII**) accompanied by the documents requested therein.
(Where the tenderer has already signed another contract with ECDC, they may provide instead of the legal entity file and its supporting documents a copy of the legal entity file provided on that occasion, unless a change in his legal status occurred in the meantime).

3.2.2 Economic and financial capacity

Requirement
The tenderer must be in a stable financial position and have the economic and financial capacity to perform the contract.

The tenderer must have for each of the past three financial years for which accounts have been closed, an average annual turnover of at least € 4.000.000[2].

Evidence required

For-Profit Organisations (whose primary goal is making a profit) shall provide, as part of their tenders:

- duly completed and signed Simplified Financial Statement, available in Annex VI
- copy of the profit & loss account and balance sheet for the last three years for which accounts have been closed.

Non-Profit Organisations (formed for the purpose of serving a public or mutual benefit other than the pursuit or accumulation of profits for owners or investors) shall provide, as part of their tenders:

- duly completed and signed Simplified Financial Statement, available in Annex VI,
- copy of the statement of financial activities and statement of the financial position for the last three years for which accounts have been closed.

Public sector entities (including public universities and international organizations), which according to the law of the country in which they are established are NOT required to publish balance sheets, shall:

- complete line 14 (Revenue) of the Simplified Financial Statement only (version for non-profit organisations) available in Annex VI,
- provide extracts from their last three budgets (including the current one) as evidence of their average budget amounting to at least € 4.000.000 which satisfy the requirements under the Simplified Financial Statement.

Individuals shall:

- only complete line 14 (Revenue) of the Simplified Financial Statement (version for non-profit organisations), available in Annex VI
- provide extracts from any available documents (e.g. income tax returns) as evidence on their average income for the last three financial years amounting to at least € 4.000.0000 which satisfy the requirements under the Simplified Financial Statement.

When completing the Simplified Financial Statement tenderers are requested to observe the following:

1. It must be signed by the authorised representative of the tenderer or tendering entity.

2. In the case of a consortium submitting a tender, or in cases of subcontracting (if the tenderer relies on the capacities of subcontractor(s) to fulfil economic and financial requirement), the Simplified Financial Statement must be included in the tender for all consortium partners and subcontractors.

3. ECDC reserves the right during the tendering process and before award of contract to request further evidence of the tenderer's compliance with the economic & financial capacity requirement. In this instance copies of official financial statements (e.g. balance sheets and

[2] In the case of tenderers from outside Eurozone, ECDC will calculate amounts of turnovers using exchanges rates for December of the relevant financial year as published in the Official Journal of the European Union: http://ec.europa.eu/budget/contracts_grants/info_contracts/inforeuro/inforeuro_en.cfm.

profit & loss accounts or financial position and financial activities statements) for up to three financial years may be requested or any other document enabling ECDC to verify the tenderer's economic and financial capacity.

4. If additional evidence is not provided in response to ECDC's request within the deadline specified, or if the information provided is proved false, ECDC reserves the right to reject the tender as non-compliant with selection criteria.

3.2.3 Technical and professional capacity

Requirement(s)

To pass the selection phase:

- The contractor need to have sufficient recent experience, minimum of 3 years in the provision of services in customer engagements similar in scope, nature and complexity to those relevant for this tender.
- The contractor must have sufficient staff capacity for the execution of the service: minimum a total number of 20 staff members meeting all the profiles described in the Technical and Contractual Specifications (2.2.5 and Annex 3) in average during 2015 and 2016

Evidence

To pass the selection phase tenders need to submit:

- A description of the **tenderer's professional activity** (maximum of 3 A4-pages, font Times New Roman, size 12) including activities with regard to the scope of this call for tender. Proof of 3 relevant references to projects with a short description detailing the Methodologies/tools/operating systems/hardware/software involved (maximum of 1 A4-pages, font Times New Roman, size 12) with annex of signed reference letter by client.
- Sample CVs covering all the profiles described in the Technical and Contractual Specifications
- A description of the roadmap for the implementation of the security controls after signature of the relevant specific contract (maximum 3 pages).

4 Award of the contract

Tenders are opened and evaluated by a committee, possessing the technical and administrative capacities necessary to give an informed opinion on the tenders. The committee members are nominated on a personal basis by ECDC under guarantee of impartiality and confidentiality. Each of them has equal voting rights.

4.1 Technical proposal

The assessment of technical quality will be based on the ability of the tenderer to meet the purpose of the contract as described in the terms of reference. To this end, the technical proposal shall contain the following information to allow evaluation of the tender according to the technical criteria mentioned in section 4.2:

1. A document of maximum of 30 pages, A4 format, font Calibri size 12, maximum of 3000 characters with spaces (all inclusive – see above) per page presenting the tenderer's proposal for a **Service delivery Plan (SDP)** to be used during the execution of the FWC.

   This document shall at least cover the following points and maintain the order and the headings as listed below:

   - IT Infrastructure services management approach to be applied during the execution of the FWC in the following areas:
     - Service management,
     - Service strategy,
     - Resource planning and task allocation,
     - delivery management,
     - change management
     - communication management,
     - documentation management,
     - training management,
     - human resources management,
     - problem management.
2. The tenderer must propose a team for the service delivery[3], where the submitted CVs have to fulfil the requirements defined in 2.2.12.

[3] Please see also the indicators for the turnover of the initial proposed team. ECDC has the expectation that the proposed team is largely available for the service implementation with the understanding that a certain level of staff turnover can be expected.

3. A document presenting the tenderer's proposal for a **Service Level Agreement (SLA)** to be used during the execution of the FWC and a document presented the tenders **service reporting** proposal. Both documents should base the templates provided (technical Annex 4 and 8)

   This SLA document shall at least cover the following points as listed below:

   - Definitions from the SLA template Technical Annex 4;
   - Additional definitions and details the tenderer would like to propose
   - All mandatory key performance indicators need to be included.
   - For the recommended key performance indicators, the tenderer might propose derivations
   - Additional Key performance indicators the tenderer would like to propose

   The Service reporting proposal should at least contain the following points as listed below:

   - Service statistics
   - Key performance indicator measurement
   - Other service reporting proposals from the tenderer

4. A document of maximum of 20 pages, A4 format, font Calibri size 12, maximum of 3000 characters with spaces (all inclusive – see above) per page presenting the tenderer's proposal for a **takeover** phase with regard to this call for tenders.

   This document shall at least cover the following points and maintain the order and the headings as listed below:

   - Standards, methods and tools the tenderer is going to use during the takeover phase;
   - Planning;
   - List of tasks foreseen and their description;
   - Allocation of (human) resources (composition of the team), estimated effort in man-days per profile, per activity and in total;
   - Deliverables;
   - Information concerning familiarisation of the tenderer's human resources with the environment;
   - Information on working environment setting-up;
   - Reporting;
   - Meetings.

5. A document of maximum of 20 pages, A4 format, font Calibri size 12, maximum of 3000 characters with spaces (all inclusive – see above) per page presenting the tenderer's proposal for a **handover** phase with regard to this call for tenders at the end of the FWC.

   This document shall at least cover the following points and maintain the order and the headings as listed below:

   - Standards, methods and tools the tenderer is going to use during the handover phase;
   - Planning;
   - List of tasks foreseen and their description;
   - Allocation of (human) resources, estimated effort in man/days per profile, per activity and in total;
   - Deliverables;
   - Reporting;
   - Meetings.
   -

4.2 Technical evaluation

The quality of technical tenders will be evaluated in accordance with the award criteria and the associated weighting as detailed in the evaluation grid below.

No	Criteria	Max points
1	The tenderer's **service delivery plan** will be evaluated, considering the following: • Adequacy, completeness and relevance of the proposed IT infrastructure services management approach, 110p • relevance of the foreseen tasks and adequacy of the allocated resources; 110p • delivery management, 40p • change management, 40p • communication management, 40p • documentation management, 40p • training management, 40p • human resources management, 40p • problem management. 40p	***500***
2	Adequacy, completeness and relevance of the global organization for all services proposed in the Service Level Agreement and service reporting template. For each service/group of services, adequacy, completeness and relevance of the description, levels, specific organization and infrastructure, methods and tools to fulfil the recommended Indicators. • Contract governance, 20p • General HR, 20p • Process area Asset management, 20p • Process area Service catalogue management, 20p • Process area change management, 20p • process area incident management, 20p • work area Frontoffice, 20p • work area ICT BackOffice . 20p • other performance indicators proposed 20p • Adequacy, completeness and relevance of the proposed service reporting template 20p	***200***
3	The tenderer's proposal for a **takeover** will be evaluated, considering the following:	***150***

	• appropriateness of the overall strategy; 30p • appropriateness of the working environments to be set-up; 20p • Adequacy, completeness and relevance of the standards, methods and tools. 10p • Adequacy, completeness, feasibility and relevance of the proposed planning. 20p • Adequacy, completeness and relevance of the foreseen tasks and of the allocated resources. 20p • Adequacy, completeness and relevance of the proposed deliverables 20p • Adequacy, completeness and relevance of the proposed meetings and reporting 30p	
4	The tenderer's proposal for a **handover** will be evaluated, considering the following: • appropriateness of the overall strategy; 30p • appropriateness of the working environments to be set-up; 20p • Adequacy, completeness and relevance of the standards, methods and tools. 10p • Adequacy, completeness, feasibility and relevance of the proposed planning. 20p • Adequacy, completeness and relevance of the foreseen tasks and of the allocated resources. 20p • Adequacy, completeness and relevance of the proposed deliverables. 20p • Adequacy, completeness and relevance of the proposed meetings and reporting. 30p	***150***
	TOTAL	***1000***

Only tenders scoring **700 points** or more (of a maximum of 1000) points against the technical award criteria will have their financial proposal evaluated.

Tenders scoring less than **60%** for any award criterion will be deemed to be of insufficient quality and eliminated from further consideration.

4.3 Financial proposal

The financial proposal should be presented in the format found in **Annex II**.

4.4 Choice of the selected tender

The contractors will be awarded and ranked to the tenderer offering the best value for money, taking into account the awarding criteria listed above. No award criteria and sub-criteria other than those detailed above will be used to evaluate the tender.

The weighting of quality and price will be applied as follows:

Score for tender X	=	cheapest price / price of tender X	*	100	*	40 (in %)	+	Total quality score (out of 1000) for all criteria of tender X	*	60 (in %)

"Price of tender X"–is the total price of the Financial Scenario table**Annex II** "Financial Proposal Form".

4.5 No obligation to award

Completing the procedure of the call for tenders in no way imposes on the ECDC an obligation to award the contract. ECDC shall not be liable for any compensation with respect to tenderers whose tenders have not been accepted, nor shall ECDC be liable when deciding not to award the contract.

4.6 Notification of outcome

Each tenderer will be informed in writing about the outcome of the call for tender.

If tenderers are notified that a tender has not been successful, tenderers may request additional information by mail. At the discretion of ECDC, this information can be given in a follow-up letter providing further details in writing, such as the name of the tenderer to whom the contract is awarded and a summary of the characteristics and relative advantages of the successful tender. However, ECDC would like to stress that it is not free to disclose any information affecting the commercial interests of other tenderers.

List of Annexes

Annex I — Draft contract

Annex II — Financial proposal form

Annex III — Declaration of honour on exclusion criteria and selection criteria

Annex IV — Authorised signatory form

Annex V — Tender submission checklist

Annex VI — Simplified Financial Statements (for profit and non-profit organisations)

Annex VII — E submission guide

Annex VIII — Legal entity form, Financial identification form and curriculum vitae template

Annex IX – Data protection agreement

Technical Annexes:

Technical Annex 1 - List of Software used at ECDC

Technical Annex 2 - List of services in online service catalogue

Technical Annex 3 - Consultancy profiles

Technical Annex 4 - Draft Service level agreement (SLA)

Technical Annex 5 – not applicable

Technical Annex 6 - Incident and priority matrix

Technical Annex 7 -sample of incident report

Technical Annex 8 draft service reporting template

Technical Annex 9 - Information system security policy

Technical Annex 10 - IT use policy