Call for tenders' details

Title: Provision and Management of Necessary Transversal Cloud Security and Integration Services

Start date: 25/05/2020

Time limit for receipt of tenders: 10/07/2020

Contracting authority: European Investment Fund

Status: Closed

Call for tenders question list

#	Submission date	Publication date	Question subject	Question	Answer
1	25/05/2020 16:12	27/05/2020 11:20	Scope of services	You mention integration, does this mean that part of the scope is the provisioning of connectivity services (bandwidth) into your cloud environment(s)? If this is the case, is the scope divided in lots? Thank you.	**27/05/2020** Provisioning of connectivity services (bandwidth) is not part of the scope of this Call for Tenders. We are talking about IT Applications integration and not network connectivity. The scope is not divided into lots.
2	26/05/2020 22:08	27/05/2020 11:31	Tender Documents / Requirements and Scope of Work	I can't retrieve the documents with the requirements. Not sure if trying to retrieve them from the right place. In the link I am directed to the Documents Library where I find some documents to fill but no requirements.	**27/05/2020** There are 21 documents published under the tab "Document library". All requirements are included in the Annex 4 - Terms of Reference - this is the last document on the list. Please check all pages in the Document library (or you can modify that 25 results/documents can be seen on the screen). Thank you!

#	Submission date	Publication date	Question subject	Question	Answer
3	27/05/2020 09:30	03/06/2020 13:36	Extension request	Due to COVID-19 and measures taken by local governments throughout the European Union, our company as well as our partners have adopted a work-from-home model. Despite our efforts to ensure that our daily business is not impacted in a negative manner, some delays may be inevitable. In this context, we would like to kindly request for an extension of the deadline for the submission of the request to participate by three (3) weeks. Thank you.	**03/06/2020** Unfortunately, the EIF cannot extend the deadline by 3 (three) weeks, but only by 1 (one) week. Therefore, the new time limit for receipt of tenders will be 07/07/2020. The corrigendum to the Contract Notice has been sent for publication. As soon as it will be published the dates in e-Tendering will be modified accordingly.

#	Submission date	Publication date	Question subject	Question	Answer
4	02/06/2020 15:16	04/06/2020 17:26	Section 4.1.5 Federated Multifactor Authentication System File EN-Annex 4 - Terms of Reference.pdf	Hello, We have some questions regarding the Federated Multifactor Authentication System. 1. What is the disavantages of OneLogin, now that you want to consider replacing it? 2. What is the current IAM infrastructure on your premise? Active Directory/LDAP 3. Why have the integration with 2 new applications not yet started? What is the main problems? From OneLogin or from the applications? Or the problem lied with the current vendor? 4. Do the new solution have to cover on-premise infra (client machines, network equipments, mobile devices ...) or just for Core Business Applications only?	**04/06/2020** 1.Onelogin has considerable presence in the market and the solution is working rather well. As EIF is solution agnostic, we can simply not oppose to the idea that there could be a better solution on the market or that it would not be in the portfolio of a specific tenderer. Please note, that EIF has also no direct contract with OneLogin (service is part of a larger service). 2.IAM infrastructure on prem is not connected to the EIF cloud eco-system so this question is not relevant. 3.They have started but they are currently idle. EIF lacks proper support and access to direct expertise on this solution because of initial contractual terms. EIF would like to improve this situation with its new partner. 4.No, just the Core EIF applications.
5	02/06/2020 15:41	04/06/2020 17:29	Section 4.1.6 Log Collection, Storage and Event Monitoring Services File EN-Annex 4 - Terms of Reference.pdf	Hello, We have some questions regarding the Log Collection: 1. Is that only application logs(not includes endpoint and network) will be collect and monitor ? 2. Is on-premise's apps(ex: Directory services) in scope of log collection & security monitoring?	**04/06/2020** 1.First focus is on related to application logs down to web application firewall logs or threat monitoring. This does not include endpoint logs or internal network logs. 2.On-premise apps are not in the scope of log collection / security monitoring. They are managed by EIB directly.

#	Submission date	Publication date	Question subject	Question	Answer
6	02/06/2020 15:43	04/06/2020 17:44	Section 4.1.7 Vulnerability Scanning and Reporting Management File EN-Annex 4 - Terms of Reference.pdf	Hello, We have some questions regarding the Vulnerability Scanning: 1. What is the current vulnerability scanning toolset? What tools EIF prefer for scanning? 3. Is Vulnerability scanning included client applications like mobile apps? 4. Vulnerability scanning should be fully automation or partially? 5. reporting management dashboard should be intergrated to SOC or independency?	**04/06/2020** 1.There is no tool to date. 2.EIF is solution agnostic. EIF cannot impose a solution but favours a service provider that will particularly be agile regarding the expected reporting. 3.Client mobile apps are not included in primary scope but may be looked at in mid-long term. 4.It should be automated to the largest possible extend though manual exceptional scans may be requested from time to time. 5.There is nothing that prevents reporting to be part of a larger SOC dashboard that could help to follow vulnerabiities over time but EIF will be interested in exported individual reports to possibly work on the individual data too.
7	02/06/2020 15:48	04/06/2020 17:58	Section 4.1.9 Ticketing System File EN-Annex 4 - Terms of Reference.pdf	Hello, We would like to have some questions regarding the Ticketing System 1. How many users are using the ticket system? How many users grow every year? 2. What is the model, version, and license of the current Jira ticket system? 3. Is the jira ticket system currently in use on-premise or on-cloud? 4. Do you want to integrate the ticket system log into the SOC system?	**04/06/2020** 1.To date, we have 22 users. We foresee a growth of 10-15 users per year as it is not an EIF wide application. 2.Delivery is Cloud\SaaS based. Version is up-to-date as updated permanently in the cloud. Licenses are not attached directly to EIF's name and bundled into software fees and cannot be transfered. 3.Cloud based. 4.Ideally yes mostly for authentication services.

#	Submission date	Publication date	Question subject	Question	Answer
8	02/06/2020 15:50	04/06/2020 18:01	Section 4.1.11 Pentesting Services File EN-Annex 4 - Terms of Reference.pdf	Hello, We are having some questions for Pentesting as below: 1. What is the minimum and maximum number of targets (i.e. web app, mobile app, API, server...) for pentesting? 2. The number of maximum effort (80 mandays per year) is fixed or mutable? 3. Junior engineer is required or not? 4. pentesting service could be implement remotely from offshore via VPN connection or require running from an EU-28 Member State?	**04/06/2020** 1.We target web applications. Minimum is 5, maximum probably 10. 2.We have a small margin to increase the yearly number of mandays if needs be. 3.Since we will request yearly pentesting of the same applications and that the service provider can learn on past pentests, junior consultants may be sufficient for certain exercises. 4.We have concerns about NDA that could be signed outside of EU's jurisdiction so we prefer any execution to be run from any EU-28 member state.
9	05/06/2020 11:30	09/06/2020 13:55	Question deadline	It is our understanding that since the submission deadline has been extended by one week, the same applies to the question deadline as well. Please confirm our understanding or clarify further.	**09/06/2020** The deadline for questions has been extended to 12/06/2020 at 23:59.
10	08/06/2020 10:45	09/06/2020 13:57	Q&A deadline	We appreciate the extension of the time limit of the receipt of tenders. However, could it be possible to extend also the deadlines for sending questions (and providing answers) in line with the new proposal deadline?	**09/06/2020** The deadline for questions has been extended to 12/06/2020 at 23:59.

#	Submission date	Publication date	Question subject	Question	Answer
11	08/06/2020 11:53	09/06/2020 13:58	Questions. deadline	As the deadline for the receipt of tenders has been extended a bit, could you consider to extend also the question deadline ? Thank you.	**09/06/2020** The deadline for questions has been extended to 12/06/2020 at 23:59.
12	08/06/2020 17:10	09/06/2020 14:00	Time limit to ask questions 15/06/2020 ?	As the time limit for receipt of tenders has been extended to 07/07/2020 at 23:59 CET, could you please extend the time limit to ask questions to the 15/06/20 as well ?	**09/06/2020** The deadline for questions has been extended to 12/06/2020 at 23:59.
13	04/06/2020 10:49	17/06/2020 09:36	Annex 5a - Template of the Technical Offer	It is our understanding that we can use one separate document for our response, 40 pages in total, keeping exactly the format provided in your template (fonts, page margins). In that way we will be able to present in a better way figures, tables etc. in our responses, and each response will be more accurate and complete. Please confirm our understanding or clarify further.	**17/06/2020** It is a correct understanding.
14	04/06/2020 10:50	17/06/2020 09:44	Annex 5a - Template of the Technical Offer / CVs	It is our understanding that the required CVs should be provided as annex to the Technical Offer and will not be counted in the limit of 40 pages. Please confirm our understanding or clarify further.	**17/06/2020** It is a correct understanding.

#	Submission date	Publication date	Question subject	Question	Answer
15	04/06/2020 10:51	17/06/2020 09:46	Appendix 2 to Annex 5a / Presentation of the Tenderer	It is our understanding that we can provide a separate document for the presentation of the Tenderer presenting size, principal markets served, products and services, length of activities in the relevant market, number of staff employed with relevant experience, a confirmation that the Tenderer comply with the generic requirements in Section 4.1.2, including a short description etc. with no limitation to number of pages. Please confirm our understanding or clarify further.	**17/06/2020** It can be done this way indeed although we would suggest a "reasonable" number of pages for this presentation of the company, its compliance and its relevance.
16	04/06/2020 10:51	17/06/2020 09:49	Appendix 2 to 5a / Assignment Reference Tables	Should be the description of the project limited in one A4 page or is it allowed to be more than one?	**17/06/2020** If the project comes with a very large scope related to the Terms of Reference then it can probably be more than an A4 page but we would suggest not more than 2. The Tenderer has to use also the provided template - Appendix 2 to 5a.
17	04/06/2020 14:06	17/06/2020 09:51	4.1.4.3 Secure cloud document storage (...)	Regarding 4.1.4.3, do you have requirements on the ways (user interfaces, protocols) to offer to upload documents in the secure file transfer service ?	**17/06/2020** Ideally a web client interface with TLS protocol would be the easiest in terms of integration. A fat client based on web protocols or a web browser plugin could also be acceptable.

#	Submission date	Publication date	Question subject	Question	Answer
18	04/06/2020 14:31	17/06/2020 10:00	Economic and financial capacity	The tender specifications say "The total annual turnover associated with the type of Services, to which the Tenderer is tendering should be more than EUR 2,000,000 for each of the last three (3) available financial years (e.g., 2017, 2018 and 2019 ideally). Where applicable, this requirement applies to each member of a group of economic operators on a consolidated basis and/or to any foreseen subcontractor (reference is made to section 6.5.1 and 6.5.2)." Can you please confirm that this requirement applies to a group of economic operators (potentially made of subcontractors / freelancers) as a whole on a consolidated basis?	**17/06/2020** We confirm that this requirement applies on a consolidated basis in case of joint tender. If the Tenderer intends to subcontract above 50% of the total contract amount to a single economic operator, the Tenderer and that subcontractor shall provide the above-mentioned documents in relation to the economic and financial capacity. If the Tenderer intends to subcontract less than 50% of the total contract amount, the Tender itself has to prove its compliance with this requirement. In any case we need to be able to measure that the consortium or the Tenderer and subcontractors can be considered as a solid security and integration player.
19	04/06/2020 16:22	17/06/2020 10:01	3 Purpose of the Call for Tenders (page 6)	a Vulnerability management tool/service to scan all EIF Cloud platforms to provide monthly and quarterly aggregated reports on vulnerability; Should the management tool include compliance test of the cloud infrastructure itself? Too permissive network rules, roles, etc?	**17/06/2020** These features are of clear interest for EIF. First priority is to get a clear and consolidated vision on the applications security exposure overtime but this can be looked after with "build mandays".

#	Submission date	Publication date	Question subject	Question	Answer
20	04/06/2020 16:23	17/06/2020 10:03	4.1..4..1 Key Management System for the Management of requested services (page 11)	"Encryption of storage; Encryption of data in databases;" Shall indexed logs be encrypted?. Raw long term logs can be encrypted on storage but indexed real time access logs cannot	**17/06/2020** By default, everything shall be encrypted but we can understand that some technical constraints may prevent encryption of specific elements of the services. Those shall be explained and documented.
21	04/06/2020 16:53	17/06/2020 10:06	4.1..6..1 Background (page 22)	"A SOC is by definition an organised and highly skilled team whose mission is to continuously monitor and improve customers' security posture by preventing, detecting, analysing and responding to cyber security incidents" Are forensic services under the scope of the security monitoring? Do you have an estimation about the number of forensic activities to be performed? In case of forensic activities are under the scope of the service, could you provide detail about location of facilities where a forensic analyst would be needed?	**17/06/2020** Forensics have not been formally described as a required service in the Terms of Reference. In specific cases, EIF could indeed require consultancy for specific forensics assignments. But numbers cannot really be foreseen at this stage. It may also be that EIF relies on the Service Providers or its partners to execute the forensics analysis. The tenderers are free to present CVs related to forensics analysis.
22	04/06/2020 16:54	17/06/2020 10:07	4.1..6..1 Background (page 22)	"A SOC is by definition an organised and highly skilled team whose mission is to continuously monitor and improve customers' security posture by preventing, detecting, analysing and responding to cyber security incidents" Can all activities be accomplished remotely?	**17/06/2020** Yes, EIF does not intend to host this SOC.

#	Submission date	Publication date	Question subject	Question	Answer
23	04/06/2020 16:55	17/06/2020 10:09	4.1..6..2 Technical and service level requirements (page 22)	"ensuring consistent and uninterrupted logging from all EIF applications detailed above (as well as future new applications) to provide the necessary data quality for log analysis. The applications considered are moderately intensive in terms of user activity and log verbosity" Is it available any log volume estimation? Events per second (EPS), or daily volume of raw (not compressed) logs (GB/day) would be advisable	**17/06/2020** EIF as around 550 users but some systems may have a larger number of users because systems are slightly more opened than just for EIF. Not all users connect to all applications on a daily basis. But overall we estimate 5000 connexions per day, so let's say 6000 events per day if we consider various type of events (admin or cloud generated events).
24	04/06/2020 17:44	17/06/2020 10:12	4.1..6..2 Technical and service level requirements (page 22)	"Security use cases are implementations in the log management system of new (advanced) indicators of compromises (IOC) that the team should detect" Is there a working repository of uses cases being used nowadays? Is it defined in any standard syntax (e.g SIGMA) or propietary package of rules (e.g Arcsight, Splunk, Qradar)?	**17/06/2020** To date, this monitoring service does not exist at EIF and should be built from scratch. The implementation project related to "log monitoring services" is there to define any methodology and some first use cases then we shall use "build days" to further extend use cases. EIF expects to rely on the experience of the service provider in that area to quickly build a first set of basic IOCs.

#	Submission date	Publication date	Question subject	Question	Answer
25	04/06/2020 17:45	17/06/2020 10:13	4.1..6..2 Technical and service level requirements (page 22)	"Security use cases are implementations in the log management system of new (advanced) indicators of compromises (IOC) that the team should detect" Is there available any estmation about number of incidentes / security use cases being triggered nowadays even through manual reviews?	**17/06/2020** To date, this monitoring service does not exist at EIF and should be built from scratch so these values do not exist.
26	04/06/2020 17:46	17/06/2020 10:14	4.1..6..2 Technical and service level requirements (page 22)	"Security use cases are implementations in the log management system of new (advanced) indicators of compromises (IOC) that the team should detect" Who will be responsible of potential further investigations on affected systems not accesible by the Service Provider? E.g end user contact in order to confirm root cause behaviour, end point artefacts extraction, forensic activities (if included in the scope), etc.	**17/06/2020** Escalation to EIF (to a named person) of a possible security incident will trigger the internal "EIB Group Incident Management process". From there, EIF will contact the affected Cloud Provider and will manage the incident directly with it. In specific cases, a forensics assignment might be requested to the Service Provider (or a Provider designated by the Cloud Provider itself) but this is something to be further explored.

#	Submission date	Publication date	Question subject	Question	Answer
27	04/06/2020 17:47	17/06/2020 10:16	4.1..6..2 Technical and service level requirements (page 22)	"ensuring consistent and uninterrupted logging from all EIF applications detailed above (as well as future new applications) to provide the necessary data quality for log analysis. The applications considered are moderately intensive in terms of user activity and log verbosity" It is not described any other infrastructure to be monitored, e.g firewall, web proxy, VPN solutions, DNS, Active Directory Platform, End Point security software, mail protection, mail relay, … Are those platforms under the scope of log management and monitoring? Is it available any log volume estimation?	**17/06/2020** These logs are internal EIB group logs and not managed by EIF. They are not in the scope.
28	04/06/2020 17:48	17/06/2020 10:21	4.1..6..2 Technical and service level requirements (page 22)	"ensuring consistent and uninterrupted logging from all EIF applications detailed above (as well as future new applications) to provide the necessary data quality for log analysis. The applications considered are moderately intensive in terms of user activity and log verbosity" What is the number of EIF users / endpoints mailbox?	**17/06/2020** EIF as around 550 users but some systems may have a larger number of users because systems are slightly more opened than just for EIF. Not all users connect to all applications on a daily basis. But overall we estimate 5000 connexions per day, so let's say 6000 events per day if we consider various type of events (admin or cloud generated events).

#	Submission date	Publication date	Question subject	Question	Answer
29	04/06/2020 17:49	17/06/2020 10:25	4.1..6..2 Technical and service level requirements (page 22)	"alerting EIF in case of suspicion of a security incident and follow up with EIF until incident is fully closed with the “Application Cloud Provider“. Any escalation must be sustained by a final report upon the incident or suspected incident closure;" Would you require a formal report summarizing all relevant aspect regarding incident response process lifecycle or information in the ticketing tool would comply?	**17/06/2020** Information in the ticketing tool should be sufficient. For more complex cases a full report may be required.
30	04/06/2020 17:50	17/06/2020 22:47	4.1..6..3 Implementation project (page 24)	"Besides monthly service reviews with a Service Delivery manager (transversally to all services), the EIF also expects the regular presence of a senior engineer (30 days per year to help with the on-boarding of new applications and to devise new IOCs and their implementation)." Would this presence be activated on demand upon deployment of new applications? Would it be scheduled, let´s say 5 days every two months, …	**17/06/2020** The presence will be activated upon deployment of new applications or for important reviews of use cases of existing applications.

#	Submission date	Publication date	Question subject	Question	Answer
31	04/06/2020 17:52	17/06/2020 22:49	4.1.9 Ticketing system (page 27)	"The EIF is currently using JIRA as an internal ticketing system …" Is the tool being provided as a service (cloud) or on-premissess? In case the tool JIRA is adopted is the renewal of the tool under the scope? Could you provide maintenance / support contracts dates?	**17/06/2020** As of Today the JIRA implementation is not centralised across EIF cloud ecosystem and is a simple utility provided close to the source application and nothing holistic to EIF solution management. Should JIRA be the selected tool, we would require a new implementation with demand management, change management and incident management for the whole EIF cloud ecosystem.
32	04/06/2020 17:55	17/06/2020 22:50	4.1.9 Ticketing system (page 27)	"the interfacing with the above mentioned federated multifactor authentication system (SSO and MFA) in #4.1.5 and log management system in #4.1.6." Which interaction is required with Log Management System? Automatic creation of cases upon alert triggering?	**17/06/2020** It is more to be read the other way around. We expect the access to the ticketing system to be authenticated by the auth/SSO/MFA solution, access logs to be sent to the central repository and the ticketing system to be part of the continuous vulnerability scanning. EIF may be interested by automation of ticket issuance but this is not a short/mid term expected delivery.

#	Submission date	Publication date	Question subject	Question	Answer
33	04/06/2020 17:57	17/06/2020 22:54	Applicable EU regulations and security standards	The ToR states “to address various security requirements necessary to comply with applicable EU regulations and security standards when processing, storing, transmitting or maintaining confidential company data “ Which regulations is it referring to?	**17/06/2020** A very important regulation would be The General Data Protection Regulation (EU) 2016/679 (GDPR) that is a regulation in EU law on data protection and privacy in the European Union (EU) and its EU derivatives EU-GDPR. There may be other local laws/regulations to be complied with but since they depend on where services are operated from or hosted in, it is a matter where the Provider is able to show its knowledge.
34	04/06/2020 18:42	17/06/2020 22:55	SSO and Identity Federation Solutions:	Are the SSO /Identity Federation solutions just for the business applications, or do they also need to cover the services to be included under this contract (e.g. vulnerability management, log management, ...)	**17/06/2020** The main scope is indeed business applications. Authentication to provide access to the technical dashboards for EIF (very limited number of people) may be provided initially by different mean such as user certificates and eventually by the central SSO/Identity federation tool.
35	04/06/2020 18:43	17/06/2020 22:57	Technical Proposal maximum number of pages	The technical proposal needs to be limited to 40 pages length. Does this include the CVs of the proposed experts? Could it be included in an Annex (out of the 40 pages limit). Is it acceptable to do the same with the proposed products descriptions (e.g. product leaflets)?	**17/06/2020** CVs can be provided as annex to the core answer. The solutions shall be clearly described as part of the proposal but additional non-core information could also be attached as annex.

#	Submission date	Publication date	Question subject	Question	Answer
36	05/06/2020 09:24	17/06/2020 22:58	4.1.4.3 Secure Cloud document storage (...)	Can you please clarify how many end users are going to use the service ? What is the average file size ? Which volume maximum of exchanged files at the same time ?	**17/06/2020** At the earliest stage, we would target 25 initially and up to 50 users. In average file size is probably 1 to 5MB. This solution is for specific exchanges of sensitive documents so the volume and its increase should be limited (probably up to 5GB).
37	05/06/2020 11:19	17/06/2020 22:59	Terms of reference: Vulnerability Management, page 6	How many IP addresses are in scope of the recurring security testing and penetration testing?	**17/06/2020** Today up to 30 IP addresses including PROD/UAT/DEV are in scope of continuous vulnerability management. For the penetration testing, it is probably up to 10 IP addresses to assess.
38	05/06/2020 11:20	17/06/2020 23:00	CV format	Can you please confirm that we are free to choose the format of the CVs?	**17/06/2020** Yes, EIF does impose the format. What we would expect though is that all CVs follow the same format and make clear evidences of hard or soft skills to complete the projects they would be assigned to or to cover the "run activities".
39	05/06/2020 11:21	17/06/2020 23:01	Page limitation technical offer	Can you please confirm that the CVs do not count towards the total number of pages limited to 40?	**17/06/2020** No they do not count, they can be inserted as annex.

#	Submission date	Publication date	Question subject	Question	Answer
40	05/06/2020 11:23	17/06/2020 23:03	Licence procurement	For managed services: Does EIF intend to purchase the licenses for the underlying tools (e.g. IAM platform), or shall the Service Provider acquire the license in accordance with the requirements of the Managed Service delivery model from the respective software vendor?	**17/06/2020** EIF is expecting a price estimate of some specific licenses (including the IAM platform) as part of the answer to this Call for tenders. So we can expect to have these licenses subscribed under EIF's name. For the rest, licenses can be embedded in the service fees.
41	05/06/2020 11:26	17/06/2020 23:04	License procurement	If the service provider needs to procure the licences for software, does EIF then consider the software providers to be sub-contractors in the sense of this tender?	**17/06/2020** This all depends on the delivery model adopted. If the provider is hosting itself a licensed software then no. Otherwise if the provider is operating directly in the cloud then the Cloud provider is a sub-contractor. If the provider is consuming service operated by the another Cloud service provider using a cloud hosting, then both Cloud Application Provider and Cloud Infrastructure provider are subcontractors.
42	05/06/2020 11:28	17/06/2020 23:06	Open-source tool	Does EIF qualify open-source tools as suitable, provided that Service Provider can demonstrate appropriateness for the purpose of the service delivery?	**17/06/2020** Open-source tool can be accepted but they should not be "niche" software. Stability of long-term support is of prime importance.

#	Submission date	Publication date	Question subject	Question	Answer
43	05/06/2020 11:30	17/06/2020 23:07	Exclusion criteria	Are there any tools/platforms that EIF has defined as non-eligible for the purposes of the service delivery?	**17/06/2020** EIF is vendor/product agnostic by nature though of course would favour solutions with good reputation and excellent support. If the provider is confident to provide services at the expected service level and responding to all hosting requirements or integration requirements, then EIF will consider such solution in its assessment.
44	05/06/2020 11:33	17/06/2020 23:09	References	Providing client contact details for reference can be problematic with respect to client confidentiality and data privacy. Would EIF accept, that we first indicate the contact details of an employee of the service provider and that this person would establish the contact with the client once EIF requests so?	**17/06/2020** That is acceptable for EIF. What matters is that references are verifiable.
45	05/06/2020 11:37	17/06/2020 23:11	References	The service provider is an independent legal entity and is a member firm of a professional services network. If the service provider wishes to use a reference from another member firm of this professional services network, does this require the member firm providing the reference to be a sub-contractor of the main tenderer in the sense of this tender?	**17/06/2020** We would say yes (for being a sub-contractor) although it would make sense that the "sister" company providing references is actually the one delivering the service otherwise the reference is not very relevant. Joint tender is also allowed (please see the Terms of Reference for more information).

#	Submission date	Publication date	Question subject	Question	Answer
46	05/06/2020 16:22	17/06/2020 23:14	Volume maintenance	Les 330 jours de maintenance annuelle seront-ils comptabilisés à partir de la fin de la phase d'implémentation ?	**17/06/2020** Since we have the need to implement several services, for the first year, we may start maintenance progressively service by service and then if possible later align all maintenance to the same date.
47	05/06/2020 16:25	17/06/2020 23:15	Nombre de pages pour la partie TECHNICAL OFFER ?	40 pages recto-verso signifient 40 feuilles et donc 80 pages ou 20 feuilles et 40 pages ?	**17/06/2020** 20 sheets and 40 pages purely for the technical answer (CV being annexes)
48	05/06/2020 16:27	17/06/2020 23:17	Vulnerability management	Will it be necessary to install probes in the different clouds for the internal scans of the vulnerability management platform?, if so, how many?	**17/06/2020** The provider may consider a specific cloud instance were probe could be run but this is not a must. Initially, the scans may be run from a remote location. If we were to consider authenticated scans at a later time and proven maturity of the vulnerability management this may be reconsidered and implemented as a specific project.
49	05/06/2020 16:27	17/06/2020 23:18	Services professionnels des fournisseurs	Les fournisseurs de services professionnels sont-ils considérés comme des sous-traitants ?	**17/06/2020** Yes they are. The main reasons that there needs to be a control on the way they are operating too and that specific security requirements may need to be crossed checked with them too.

#	Submission date	Publication date	Question subject	Question	Answer
50	05/06/2020 16:29	17/06/2020 23:19	Collection de logs : volumétrie ?	EIF peut-elle fournir une estimation de volumétrie des LOGS ?	**17/06/2020** An indicative estimation would be 6000 events per day in the beginning of the contract.
51	05/06/2020 16:32	17/06/2020 23:20	Collection de logs	Quels types de logs sont souhaités : logs système, logs sécurité, les deux ?	**17/06/2020** We are mostly looking at application (user/admin) logs, possibly a couple of cloud related security logs.
52	05/06/2020 16:36	17/06/2020 23:22	Protocole SFTP	Le protocole SFTP est-il obligatoire ? Une solution "Sync & Share" est-elle envisageable ? Une solution de collaboration plus étendue intégrée avec Microsoft peut-elle être proposée ?	**17/06/2020** The goal is to allow cloud to cloud file exchanges in a context where not all applications have APIs. Underlying hosting OS can be Windows or Linux. A short term solution should probably still rely on SFTP or similar protocol. A mid-long term solution could be proposed additionaly to foster a modernised integration layer. Collaboration suites are not targeted by this Call for tenders.
53	05/06/2020 16:37	17/06/2020 23:23	Vulnerability management	EIF a-t-elle besoin d'accéder à l'outil mis en place ?	**17/06/2020** EIF does not plan to do any operation or scan with it but a read-ony access might be of interest

#	Submission date	Publication date	Question subject	Question	Answer
54	05/06/2020 16:40	17/06/2020 23:25	ServiceNOW	In chapter "4.1..9..2 Functional requirements", we find the following sentence "the creation of dedicated and segregated projects (instances) for each solution". What do you mean with "each solution" ?	**17/06/2020** Solution here refers to any EIF Cloud application for which we expect to support work orders, incident and change management processes.
55	05/06/2020 16:44	17/06/2020 23:26	ServiceNOW	Is there an existing Service Catalog ? If yes, can you provide details ?	**17/06/2020** There is no service catalogue to date. This should be built during the implementation project.
56	05/06/2020 16:46	17/06/2020 23:27	ServiceNOW	Is it possible to have the average number of incidents and work order tickets you are managing per month or per year ?	**17/06/2020** A rough estimation would be 500 work orders and 600 "application helpdesk" requests across all Cloud applications per month.
57	05/06/2020 16:50	17/06/2020 23:28	LOG collection	Is Data anonymization done on server side or does EIF expect Data to be anonymized on Provider's side?	**17/06/2020** Since we are talking about security logs mostly, it remains important to be able to link an event with an identity especially in the case of a incident. Therefore we do not really see data anonymisation in the picture here. Data protection to be more addressed by privilege access management, proper profile assignments and encryption.

#	Submission date	Publication date	Question subject	Question	Answer
58	05/06/2020 16:52	17/06/2020 23:30	Log collection	Is it possible to install an agent on the servers in order to retrieve logs or do we have to use syslog ?	**17/06/2020** By default, we should consider a syslog approach or even possibly the need to fetch logs even more manually. Installing agent will be a target at some point in time but will require "Cloud application builder" approval.
59	05/06/2020 17:41	17/06/2020 23:31	Use existing procurement framework agreements	Does the offer of the bidder needs to include the cost of the required technologies (licences or subscriptions) or will the EIF consider using existing procurement framework agreements, like SIDE 2 and Cloud II, benefiting from pricing and/or Data protections, compliance and privacy provisions that are already in place with those frameworks.	**17/06/2020** The offer shall include the cost of the required technologies. Setting up properly secured services is part of the assignment and the Provider shall not rely on another framework to do so.

#	Submission date	Publication date	Question subject	Question	Answer
60	08/06/2020 15:31	17/06/2020 23:34	4.1..4..2 Key Management System for the EIF Core Cloud services	1.- Could you please provide an architecture of the systems to be protected with encryption key management BYOK (systems that self-encrypt), * Could you please describe the different elements that implement the systems to be protected (storage, OS file system, database, application) * Could you please specify which technology are they based on (NAS/SAN/DAS/other, Linux/Windows/UNIX/other, Oracle/SQLServer/MySQL/other, application name/type).	**17/06/2020** There is not so much an architecture in place today, it is ad hoc encryption on a per Cloud application basis. EIF Cloud Providers are using the existing KMS of the infrastructure cloud provider like AWS or Azure. Encryption is used across EIF solutions to encrypt storage (S3, blob), OS (EBS or equivalent), database (via TDE). Understanding what BYOK could bring to EIF, what are its advantages and how the implementation would go on, is part of the initial assignment.

#	Submission date	Publication date	Question subject	Question	Answer
61	08/06/2020 15:32	17/06/2020 23:36	4.1..4..2 Key Management System for the EIF Core Cloud services	2.- Could you please provide an architecture of the systems to be protected with encryption and key management BYOE (systems that do not self-encrypt and would need BYOE), * Could you please describe the different elements that implement the systems to be protected (storage, OS file system, database, application) * Could you please specify which technology are they based on (NAS/SAN/DAS/other, Linux/Windows/UNIX/other, Oracle/SQLServer/MySQL/other, application name/type).	**17/06/2020** There is not so much an architecture in place today, it is ad hoc encryption on a per Cloud application basis. EIF Cloud Providers are using the existing KMS of the infrastructure cloud provider like AWS or Azure. Encryption is used across EIF solutions to encrypt storage (S3, blob), OS (EBS or equivalent), database (via TDE). Understanding what BYOE could bring to EIF, what are its advantages and how the implementation would go on, is part of the initial assignment.
62	08/06/2020 15:32	17/06/2020 23:37	4.1..4..2 Key Management System for the EIF Core Cloud services	Could you please provide number of public cloud accounts to protect ? (AWS, Azure, others)	**17/06/2020** We are talking about 5 AWS accounts and 2 Azure accounts.
63	08/06/2020 15:33	17/06/2020 23:38	4.1.5 Federated Multifactor authentication system	Do you use or intend to use Certificate Base Authentication as one factor of the authentication system?	**17/06/2020** We have not foreseen it so far.
64	08/06/2020 15:34	17/06/2020 23:39	4.1.5 Federated Multifactor authentication system	Do you have a PKI infrastructure with client certificates that you would like to use as a factor for authentication?	**17/06/2020** No we do not have such infrastructure.

#	Submission date	Publication date	Question subject	Question	Answer
65	08/06/2020 15:34	17/06/2020 23:40	4.1.5 Federated Multifactor authentication system	If not, are you planning to deploy a PKI infrastructure?	**17/06/2020** It is not anticipated so far but if you have good reasons to believe it is of interest for EIF please detail it in your answer.
66	08/06/2020 15:35	17/06/2020 23:42	4.1.8 SFTP Service	Does this point refer to a specific technology? In that case would you please specify which one: the IETF Draft-standard SSH File Transfer Protocol, FTP tunneling over SSH, the IETF Standard FTP over SSL, other?	**17/06/2020** We need to be able to transfer files in the context of automated transfers between Cloud applications. Please detail your proposal according to the requirements outlined in the Terms of Reference. **18/06/2020** We need to be able to transfer files in the context of automated transfers between Cloud applications. The protocol used shall be standard enough to not create integration issues nor disruption in services. SFTP seems rather standard in that way.
67	08/06/2020 15:35	17/06/2020 23:43	4.1.8 SFTP Service	Is this service intended for EIF end-user usage or for automated secure communication between EIF Cloud bases processes and systems?	**17/06/2020** It is intended for automated secure communication between EIF Cloud based processes and applications.

#	Submission date	Publication date	Question subject	Question	Answer
68	08/06/2020 15:36	17/06/2020 23:44	4.1.8 SFTP Service	Could we please know how many users/accounts will use this tool?	**17/06/2020** Since it is intended for automated secure communication between EIF Cloud based processes and applications, it will be a very limited number of technical accounts 10-20 probably.
69	08/06/2020 15:42	17/06/2020 23:47	Single Sign-on	What is the user directory currently used (LDAP, AD...) ?	**17/06/2020** The corporate user directory is not in EIF direct control, currently it is the one located within the Onelogin application.
70	08/06/2020 15:52	17/06/2020 23:49	Estimated Log Data size per day	What is the estimated Log Data size per day, generated by the Applications/Services, whose logs shall be monitored?	**17/06/2020** We estimate that our systems will generate roughly 6000 events per day in the beginning.
71	08/06/2020 15:58	17/06/2020 23:50	6.5 Joint Tenders (e.g. consortia) and subcontracting	What are the possibilities for a technology vendor/provider to participate in such CFT, knowing those technology vendors cannot prevent their solutions being offered by multiple bidders/service providers?	**17/06/2020** EIF is looking for a single partner company or consortium. The technology vendor can be part of a larger consortium.
72	08/06/2020 16:02	17/06/2020 23:53	Selection criteria - Tenderer’s relevant experience	Should we provide anything else apart of ART (references, certificates of satisfactory execution issued by the clients, protocol of delivery and acceptance and etc.)	**17/06/2020** This seems sufficient, but it is up to the Tenderer to decide, what kind of proves/documents they will provide.

#	Submission date	Publication date	Question subject	Question	Answer
73	08/06/2020 17:24	17/06/2020 23:54	Ticketing system	Are the 100 users you are refering to the number of ServiceDesk people dealing with incidents and work orders ?	**17/06/2020** Incident are not yet managed in the exisiting ticket. So the use is indeed more to submit or complete work orders.
74	08/06/2020 17:27	17/06/2020 23:55	SFTP protocole	Is a SaaS service suitable?	**17/06/2020** Yes it is perfectly suitable.
75	08/06/2020 17:30	17/06/2020 23:56	Vulnerability scanning	Does the tool have to scan WEB applications (WAS - Web Application Scanning / OWASP top 10 system)?	**17/06/2020** Yes, that is an expected feature since it will help EIF understanding its direct security exposure on the targeted solutions.
76	08/06/2020 17:31	17/06/2020 23:57	Vulnerability scanning	Does the tool need to assess the risk associated with vulnerabilities?	**17/06/2020** Yes it is important to have an evaluation of technical risk related to vulnerability. EIF and application providers will be in charge to try to see if remediation exists possibly based on recommendations provided by the service provider or by the software itself.
77	08/06/2020 17:32	18/06/2020 14:27	Vulnerability scanning	Is the Identity Federation Platform an internal platform or a SaaS?	**18/06/2020** It is a SaaS platform.
78	08/06/2020 17:32	18/06/2020 14:28	Vulnerability scanning	Could you confirm that M-FILES and ORBUS are ADFS compatible?	**18/06/2020** Yes they are (minimum support of SAML2 is ensured).

#	Submission date	Publication date	Question subject	Question	Answer
79	08/06/2020 17:34	18/06/2020 14:29	SOC	Do you talk about monitoring and /or SOC? Regarding SOC, is it only about logs of security ?	**18/06/2020** We are only considering a SOC and security logs. Pure system monitoring is not centralised and is theoretically managed by each "Cloud solution provider".
80	08/06/2020 17:37	18/06/2020 14:30	SOC	Regarding the business application, could you please define which security log needs to be forwarded or if an analysis has to be done?	**18/06/2020** By default, we need to centralise all security events as part of the log collection. Analysis has to be done on the security use cases and possibile IOCs and this is part of the implementation project linked to "log monitoring".
81	08/06/2020 17:39	18/06/2020 14:31	SOC	In order to avoid any misunderstanding: do we have to take the endpoints into account?	**18/06/2020** No, endpoints are not part of the scope.
82	08/06/2020 17:42	18/06/2020 14:33	SOC	Regarding the weekly reports, if we have a customer Portal on which we can integrate the info related in Software Asset Management for incident/escalation with a call-conf in case of question, is it enough?	**18/06/2020** Please detail those aspects in your proposal for assessment. Email notification when reports are generated and available would be appreciated.

#	Submission date	Publication date	Question subject	Question	Answer
83	08/06/2020 18:48	18/06/2020 14:35	Privileged users for the PAM tool	Could the EIF provide the estimated number of administrator (privileged) users for the PAM solution? Only figures for the SSO/MFA are provided.	**18/06/2020** EIF does plan to operate solutions. If the software is here to provide specific accesses to the service providers solutions and reporting, maximum number on EIF side should be 5 people. Using this tool to provide access to EIF cloud application themselves is a long term goal and should be further analysed but probably limited to 10-20 people.
84	08/06/2020 18:50	18/06/2020 14:36	Preproduction environments	Preproduction environments (integration, testing, ...) are mentioned explicitly in the Terms of Reference only for the Log Management and Vulnerability services. Which are EIF's expectations for non-production/operational environments for the rest of the services?	**18/06/2020** These environments shall also be integrated with the authentication/SSO system (the test instance preferably).
85	08/06/2020 19:21	18/06/2020 14:37	SFTP	For the SFTP, are we expected to provide access thru static public IPs or DNS is enough ?	**18/06/2020** We believe a static public IP is advisable.

#	Submission date	Publication date	Question subject	Question	Answer
86	08/06/2020 22:18	18/06/2020 14:40	Office 365	Is there a need to consider/integrate with Office 365 in the a near future, assuming that currently it is EIB that is providing the email an collaboration environments to EIF ?	**18/06/2020** At this stage, Office 365 is not considered on EIF side. Such move should indeed be led by EIB (including security considerations) and EIF would certainly be offered an access to it.
87	08/06/2020 22:19	18/06/2020 14:43	IAM	1/ Are there any legacy applications in the EIF that should be integrated with the IAM solution, or do they all support standard such SAML, OpenID connect, oAuth2? 2/ Is there currently a PAM solution in place? How is privileged access currently dealt with? 3/ Should the Ticketing system be integrated with the IAM/SSO solution? Is it required to administer the accounts of the ticketing system in the central directory service?	**18/06/2020** 1)All EIF applications support either SAML2, or openidConnect.(including OAuth2). 2)There is no PAM in place to date. Privileges are only managed through roles defined at the application level. 3)Yes it should be integrated with the IAM\SSO solution.
88	08/06/2020 22:26	18/06/2020 14:44	Services	Are the penalties the exclusive remedy of the EIF in case the SLA are not met ?	**18/06/2020** EIF does not consider penalty as the only remedy. Penalties are the last resort of a degrading situation that has been reported for some time and for which no improvement would be noticed by EIF. EIF is looking for a partnership so will expect proper service management to address issues reported long before requesting penalties to be paid by the Service Provider.

#	Submission date	Publication date	Question subject	Question	Answer
89	08/06/2020 22:26	18/06/2020 14:46	Remediation	Would the EIF consider remediation period as well as remediation plan in case of KPI failure before imposing the payment of penalties ?	**18/06/2020** It is a possibility. Penalties are the last resort of a degrading situation that has been reported for some time and for which no improvement would be noticed by EIF. EIF is looking for a partnership so will expect proper service management to address issues reported long before requesting penalties to be paid by the Service Provider. These discussions have to be part of regular service delivery meeting.
90	08/06/2020 15:42	18/06/2020 14:53	Single Sign-On	Do the different applications in scope (tableau, Efront, M-File, etc.) support the SCIM protocol ?	**18/06/2020** SCIM is not supported by all EIF Core Cloud Applications.

#	Submission date	Publication date	Question subject	Question	Answer
91	08/06/2020 19:54	18/06/2020 15:34	CVs of staff	As per section 1.3 of the Annex 5a, the tenderer needs to submit CVs of staff demonstrating the capacity and level of expertise to implement, run the services and further build on them. According to the TOR, the following CVs are required for the specific technical areas described below: 4.1.6.2 Technical and service level requirements - CVs for senior and standard security services engineers experienced in analysis, forensics and malware. 4.1.10 Advisory services CVs for: Cloud technologies subject matter expert and cyber and information security subject matter expert 4.1.11 Pentesting services: CVs for: Senior engineer pentesters and Junior engineer pentester Can you please confirm if any additional CVs other than the ones listed above need to be submitted at this stage? If yes, what are the additional profiles per technical area to be provided?	**18/06/2020** The Provider shall demonstrate its capacity to build and run for all services described in the document section 4.1. Read below the following requirements: Pages 12/13, 4.1.4.2 subject matter expert and standard engineer. Pages 13/14 4.1.4.3 senior engineer and standard engineer. Page 20 4.1.5.6 senior engineer 4.1.5.7 missing seniority indeed: expectation is standard engineer. Page 26 4.1.7.3. senior engineer 4.1.7.4 standard engineer Page 27 4.8.1 standard engineer Page 28 4.9.3 senior engineer Optionally and link to 6, the service provider may present the CV of possible service delivery manager.

#	Submission date	Publication date	Question subject	Question	Answer
92	08/06/2020 19:56	18/06/2020 15:38	Support Documentation in Annex 5a	1.4. Support Documentation The Service Provider may provide any other relevant documents to be broughts to the attention of the EIF in the context of this qualitative assessment process. Are the documents submitted as support documentation also considered in the overall page limit of 80 pages for the Technical Offer?	**18/06/2020** Technical additional documentation not fully necessary for the understanding of a proposed solution / services can be added as annexes (such as specific white paper pdf or vendor's information). The written solution may then refer to these annexes for reading of "more detailed technical elements". Please note that the following is stated in the Technical Offer template: The Technical Offer shall not exceed the total of forty (40) recto-verso A4 sheets outside mandatory annexes.
93	08/06/2020 19:57	18/06/2020 15:40	CV template (Annex 5a - 1.3)	CVs of staff demonstrating the capacity and level of expertise to implement, run the services and further build on them. Is there any specific template that we need to use to submit the CVs?	**18/06/2020** We have no requirement in that area but would expect all CVs are based on the same template. Europass CV template could be used for instance but this is not mandatory.

#	Submission date	Publication date	Question subject	Question	Answer
94	08/06/2020 22:15	18/06/2020 15:42	Cross providers relation	It is our understanding that the Cloud Federator provider will not provision nor manage the other existing cloud infrastructure platforms of EIF. These will be provided and operated by existing providers, but they will need to follow security prescriptions and integrate with the new security services (IAM, Encryption, SOC, ...). Could you confirm this understanding is correct ? If yes, can you confirm that the EIF will be coordinating the providers ?	**18/06/2020** Yes, this understanding is correct and EIF will indeed coordinate with the various "cloud application providers". Some direct channels of communications may be established at some point in times between the Service Providers and the Application providers but not at the beginning.
95	08/06/2020 22:16	18/06/2020 15:45	Cross providers relation	What are the EIB SaaS Cloud services considered? Will they also need to be integrated with the Cloud Federator new services as for the third party providers platform ?	**18/06/2020** The SaaS services are fully described in section 4.1.1 of Annex 4 document. They indeed need to be integrated with the new provider services. There is nothing else to date. We do not request to monitor the third party's own infrastructure cloud besides what is dedicated to EIF.

#	Submission date	Publication date	Question subject	Question	Answer
96	08/06/2020 22:17	18/06/2020 15:47	Current Cloud Infrastructure	Do you have a description of the current cloud infrastructure: Platform location, number of servers, firewall, WAF, DB, …?	**18/06/2020** We cannot provide network diagrams because we have NDA with cloud application providers. All systems are hosted in EU area. That being said, the applications are usually following the same pattern with a first line ensuring IDS protection, IP filtering on public access, Load-balancing, web frontend and application server. Network segmentation is in place between different types of environments using the notion of VPC or equivalent and subnetting. WAF are not used to date but considered. Standard storage is used and DB subscribed generally as a service by the cloud application providers.

#	Submission date	Publication date	Question subject	Question	Answer
97	08/06/2020 22:19	18/06/2020 15:48	Log Aggregation & Monitoring	Could you share a view on the amounts (GB,event) and sources of logs? Would the application sources: I&AM(OneLogin or other), eFront app, SAS systems, Tableau systems, M-files systems, Orbus systems? What about EIB one in the cloud or on premise? What about the end users devices ? Does EIF have a view on the logs types to be collected (free or fixed Formats, via Syslog (with encryption), specific agent software, Import files, IDS from cloud vendors, application logs (as defined by the use-case onboarding))?	**18/06/2020** You have captured properly the list of EIF sources. We estimate roughly 6000 events per day in the beginning. EIB cloud applications are not in the scope, we may look at synergies later but not at the initial stage. Endpoints are not concerned. Most logs should be collected via syslogs but may need to automate some process to grab some local log files or in best case scenario install required agents. There is an analysis to provide just before implementation of the solution. We will have application logs and possibly IDS/security logs when made available by the cloud providers.

#	Submission date	Publication date	Question subject	Question	Answer
98	08/06/2020 22:20	18/06/2020 15:50	General	Can IEF share a high level design (HLD) of all applications or systems in scope of this tender in order to design a proper tailored made security solution?	**18/06/2020** We cannot provide network diagrams because we have NDA with cloud application providers. That being said, the applications are usually following the same pattern with a first line ensuring IDS protection, IP filtering on public access, Load-balancing, web frontend and application server. Network segmentation is in place between different types of environments using the notion of VPC or equivalent and subnetting. WAF are not used to date but considered. Standard storage is used and DB subscribed generally as a service by the cloud application providers.
99	08/06/2020 22:20	18/06/2020 15:51	Logs consumption	Are the logs only to be consumed by the Cloud federator services provider ? or are there other EIF stakeholder looking at leveraging the collected logs. If so for what purpose ?	**18/06/2020** So far, we only see the logs being consumed by the security provider for pure security monitoring, no other specific use case at the beginning.

#	Submission date	Publication date	Question subject	Question	Answer
100	08/06/2020 22:21	18/06/2020 15:53	Vulnerability management	1/ Does this include threat-management: internet scanning on known vulns in the SAAS used? 2/ Will EIF obtain 3th parties approval for the scans and confirm authorizations to scan the infrastructure. 3/ Does this include IAAS, PAAS and SAAS environment ? How many servers to be considered and how many applications ?	**18/06/2020** 1) Yes this is in the scope. 2) It is indeed EIF's responsibility to get the 3rd party approval 3) So far we are talking about SaaS environments only. However, it is clear that behind a SaaS, there are technical platforms for which a risk exists too. Our view is that scans have to be holistic and do not stop at the application/web layer.
101	08/06/2020 22:21	18/06/2020 16:11	General Requirements	With reference to section '3 Purpose of the Call for Tenders', page 6, '...additional days to strengthen the solutions and build on them (per day for each required profile)...', please clarify if these days are part of the quotation to be offered or a "price per day" to be procured separately if needed	**18/06/2020** A price per day per profile is preferable as those days may not be consumed at once or in full (approach is rather "time and material").

#	Submission date	Publication date	Question subject	Question	Answer
102	08/06/2020 22:23	18/06/2020 16:43	Encryption services	Annex 4 p11:"Another encryption goal pursued by the EIF is to try to decouple the management and access to Master and encryption keys and the actual support to the infrastructure by the mean of a “Bring your own encryption/CloudHSM” service." - > Could you clarify this request? Do you mean comparing the standard services of cloud providers in the areas of HSM and KMS with a commercial/off the shelf/custom platform? Or are you talking about a separate, dedicated encryption service?	**18/06/2020** Today, encryption is based on KMS provided by the infrastructure cloud providers. We know this theoretically offers a possibility (not necessarily simply) to the infrastructure Cloud provider to access our content. So indeed we need to compare with alternative offers such as BYOK/BYOE/Cloud HSM what would be the main advantages but also which impacts this would have in terms of operations.

#	Submission date	Publication date	Question subject	Question	Answer
103	08/06/2020 22:23	18/06/2020 16:50	General Requirements	With reference to section '3 Purpose of the Call for Tenders', page 6, '...ad hoc consultancy costs....', please clarify these costs. Are these part of the needed offering? If so for how many days? Else is a "price per day" needed here also?	**18/06/2020** Consultancy may be required for the following: *implementation project of services *build / improvement of services *advisory services *pentest services We see all these services to follow a ""time and material"" approach for which we have provided an estimate of mandays. Providers may have different views on implementation duration, this is then to be described and explained in the offers. Therefore, we need a proposal detailing price per day per required profiles. Run cost of services should be embedded in the quotation but not as separate consultancy.
104	08/06/2020 22:23	18/06/2020 16:51	IAM	Is the consolidation on a common IAM solution already started leveraging One login? Has the assessment of the implemenattion been made ? If so what is the timeline and effort foreseen ?	**18/06/2020** The consolidation of IAM solution is a clear goal of EIF. Onelogin may be a solution but if better market solution exist, we are ready to consider a change with a migration involved.

#	Submission date	Publication date	Question subject	Question	Answer
105	08/06/2020 22:24	18/06/2020 16:53	Ticketing System	What is EIF's current view on JIRA? Are there any particular reasons EIF would like to discontinue the usage of JIRA?	**18/06/2020** JIRA has been used at EIF for many years to support the management of tickets for several applications. The solution has always managed to fit our needs thanks to its flexibility. After using the on premise version of the tool, we migrated in 2017 to JIRA Cloud to be aligned with our preferred delivery model (SaaS). While the Cloud version showed limitations, bugs and performance issues shortly after our migration, the solution evolved and corrections were made to arrive to what we consider now as a stable solution. There are no particular reasons that would encourage EIF to discontinue the usage of JIRA.
106	08/06/2020 22:24	18/06/2020 16:55	General Requirements	With reference to section '3 Purpose of the Call for Tenders', page 6, '...run services costs (a bundle of services and license fees is acceptable)...', please clarify the expected run costs especially in terms of Log management and IAM	**18/06/2020** Run costs can be a bundle of license fees (to contract a product or run a software and maintain it over time) and the cost of running and supporting the service for EIF. Implementation project and build activities are to be considered as consultancy activities so not in the run costs.

#	Submission date	Publication date	Question subject	Question	Answer
107	08/06/2020 22:24	18/06/2020 16:56	Licenses	Could you confirm that the EIF wants to owns the licenses directly ?	**18/06/2020** EIF needs to own the licenses when there is a risk they may not be transferable if for some reasons, EIF was needing to change from provider but keep the service. For the sake of awarding, EIF has requested real license fees for the IAM solution and ticketing system.
108	08/06/2020 22:24	18/06/2020 16:57	Specific terms	For the procurement of the software, are we ok to consider that the standard terms and conditions of the Software Editors shall be applicable upon the EIF ?	**18/06/2020** Usually, EIF requests that its terms and conditions shall be applicable on the software vendor. We consider it is up to the vendor to notify EIF about any terms or conditions that may not be properly applied by a subcontracted cloud provider.
109	08/06/2020 22:25	18/06/2020 17:02	General Requirements-Description of Services	With reference to section 'EIF solutions' architecture', page 8, '...Diagram...', please clarify the term SaaS. Are the applications owned by EIF and hosted on cloud (e.g. Azure, AWS), accessing VMs, OSes, DBs and Application or EIF purchases a app as a service?	**18/06/2020** EIF is trying to only contract "app as a service" as you name it. We are not doing any direct operations on VMs, OSes, DBs but our applications are indeed supported by such elements in AWS or Azure (those may be operated by our application providers).

#	Submission date	Publication date	Question subject	Question	Answer
110	08/06/2020 22:25	18/06/2020 17:03	Data protection	Shall the Service Provider have an access to or process personal data as defined under the GDPR ? If yes, Do you agree to detail these personal data in order to comply with the GDPR requirements ?	**18/06/2020** EIF needs to follow EU-DPR which is close to GDPR. During the implementation of services both EIF and the service Provider shall pay attention to personal data. We mostly see this issue for the log monitoring services but shall pay attention for any type of service in scope.
111	08/06/2020 22:25	18/06/2020 17:06	Specific terms	For the provision of the cloud environment, are we ok to consider that the standard terms and conditions of the cloud provider shall be applicable upon the EIF ?	**18/06/2020** Usually, EIF requests that its terms and conditions shall be applicable on the cloud provider. We know it may be a tough subject with big cloud players but we consider it is up to the vendor to notify EIF about any terms or conditions that may not be properly applied by a subcontracted cloud provider.

#	Submission date	Publication date	Question subject	Question	Answer
112	08/06/2020 22:26	18/06/2020 17:08	Generic Requirements	With reference to section '4.1.3 Generic Requirements', page 10, '..... to implement secure access to the services solution by implementing a central Privilege Access Management (PAM) tool or equivalent to access the environments (when relevant) and/or rely on strong authentication mechanisms to manage the solutions themselves;...', please clarify: 1) Which environments is expected the contractor to access with PAM tool? 2) is PAM a part of the offered services? Will PAM be used by the EIF users, or should be the service provider's PAM?	**18/06/2020** The PAM solution is a requirement for EIF to ensure that the Provider operating the security services follows security and operations best practices. It may be shared later with specific EIF cloud application provider's to access very specific EIF resources.
113	08/06/2020 22:26	18/06/2020 17:10	Generic Requirements	With reference to section '4.1.3 Generic requirements', page 10, '...the right to Audit its solutions and run assessments as part of the Framework Agreement or minimally to request security audit and assessments reports conducted by reputable third parties;...', please clarify: The cost of the audits should be quoted separately?	**18/06/2020** EIF requires also the right to audit the provider. We would indeed require an independent company to audit the provider so there is no need of a specific quote here as it would be invoiced to another company.

#	Submission date	Publication date	Question subject	Question	Answer
114	08/06/2020 22:27	18/06/2020 17:11	Penetration testing	In the context of the penetration testing in order to assess the security of its Cloud core environments, Can the EIF confirm that it has received or will receive the consent from all third parties (including the different service providers) involved in the relevant Cloud core environments so that the Service Provider will be legally allowed to perform such penetration testings ?	**18/06/2020** We understand the legal concern here and EIF will commit to get these consents when necessary.
115	08/06/2020 22:27	18/06/2020 17:17	Encryption services	With reference to section '4.1.4 Encryption services', page 11, '.....', Can IEF share the encryption requirements and the applications or systems that KMS/HCM will need to support?	**18/06/2020** Encryption is used across EIF solutions to encrypt storage (S3, blob), OS (EBS or equivalent), database (via TDE).

#	Submission date	Publication date	Question subject	Question	Answer
116	08/06/2020 22:28	18/06/2020 17:20	Encryption services	With reference to section '4.1.4.1 Encryption services ', page 11, '...Considering the provision of all the Services described in the TORs, the EIF expects the Service Provider to propose and describe a “key management system” (KMS)...', please clarify: 1) Is is acceptable for the requested KMS to be built upon a multi cloud solution i.e. integrate relevant services from multiple cloud providers ? 2) Is there a list of acceptable encryption algorithms and ciphers for symmetric and assymetric encryption services? Is it acceptable if the solution is only capable to offer a limited number of enryption options that are considered "secure" by means of cryptographic strength? 3) Are there any estimates on the number of keys, including the master keys that need to be managed by the KMS on a monthly basis? Are there any estimates on the number of requests to the KMS on a monthly basis? 4) Does the KMS need to be compatible with other cloud providers apart from Azure and AWS mentioned in the tender?	**18/06/2020** 1) We do not see an issue with the concept. 2) We have no such list but clearly agree to limit exclusively to secure algorithms with appropriate (up to date) encryption strength. 3) Since encryption is mostly application based and not user based, the number of keys to manage is probably a small multiple of the number of EIF Cloud applications. 4) EIF cannot foresee at this stage the use of any other Cloud Infrastructure Providers but a large inter-operability is always preferred.

#	Submission date	Publication date	Question subject	Question	Answer
117	08/06/2020 22:29	18/06/2020 17:22	Encryption services	With reference to section '4.1.4.1 Encryption services ', page 11, '...Encryption of data in databases...', please clarify: What kind of database encryption is acceptable? Is solely Transparent Database Encryption (TDE) acceptable? Which database technologies (Microsoft, Oracle, etc.) except MySQL, SyBASE which are already mentioned in page 9, of the tender are within the scope of this tender?	**18/06/2020** If you have alternative to TDE, it can be mentioned in the offer. Microsoft "database as a service" is also used.
118	08/06/2020 22:29	18/06/2020 17:34	Encryption services	With reference to section '4.1.4.1 Encryption services ', page 11, '...Encryption of storage...', please clarify: What types/models of storage need to be encrypted, and/or what cloud storage services are within the scope of this tender?	**18/06/2020** Storage can be file shares such as S3, blob, EBS or equivalent (on OS).
119	08/06/2020 22:30	18/06/2020 17:36	Federated Multifactor authentication System	With reference to section '4.1.5 Federated Multifactor authentication system', page 14, please clarify: Is MFA applicable only for in-premises solutions or for SaaS as well?	**18/06/2020** MFA is applicable only for SaaS, on premise solutions are out of scope.

#	Submission date	Publication date	Question subject	Question	Answer
120	08/06/2020 22:31	18/06/2020 17:38	Federated Multifactor authentication System	With reference to section '4.1.5 Federated Multifactor authentication system', page 14, please clarify: We assume that the operation of the IAM is done by EIF, please verify.	**18/06/2020** Provisioning the IAM solutions with accounts, groups, roles is indeed with EIF. Installing, configuring (including intergration with othe cloud applications when required), supporting and maintaining (when applicable) is with the service provider.
121	08/06/2020 22:31	18/06/2020 17:40	Federated Multifactor authentication System	With reference to section '4.1.5 Federated Multifactor authentication system', page 14, please clarify: Please clarify the feed for new accounts/users. How a new user will be provisioned? Is there an HRMS system? Does it cover external users?	**18/06/2020** Provisioning the IAM solutions with accounts, groups, roles is with EIF and will be manual (besides potential migration from existing tool if needed/applicable). The HRMS is not planned to be used at this stage to trigger an automated provisioning but considerations could be given at a certain point in time to seek federation with a larger EIB Group directory.

#	Submission date	Publication date	Question subject	Question	Answer
122	08/06/2020 22:32	18/06/2020 17:42	Federated Multifactor authentication System	With reference to section '4.1.5.4', page 17, '...The solution shall come with at least two segregated instances and dedicated logically. One instance will be used for all production accesses for both EIF internal needs (800 users) and for all external EIF needs (up to 1200 users)...', please clarify: What is the directory hosting the internal users today? Who operates it? How the provisioning of users to the directory is achieved / Manually?	**18/06/2020** The directory hosting internal users to authenticate on EIF SaaS solutions is that of OneLogin. It is operated by oneLogin as SaaS and provisioned by EIF (manually).
123	08/06/2020 22:32	18/06/2020 17:44	Federated Multifactor authentication System	With reference to section '4.1..5..4 Technical requirements', page 17, '.... Licenses acquisition may be progressive over time (starting from 800 users today);...', please clarify the increase steps since this affects the pricing.	**18/06/2020** Roughly: 800 hundreds seats should cover the first 3 years. Then, we may progressively increase.

#	Submission date	Publication date	Question subject	Question	Answer
124	08/06/2020 22:33	18/06/2020 17:45	Federated Multifactor authentication System	With reference to section '4.1.5.4', page 17, '...The Solution shall support SAML-2 (Security Assertion Markup Language) and openId Connect/ oAuth2 to achieve maximum coverage of “Single sign on” solutions and to manage authorizations in the EIF applications (the latter not being an immediate objective)....', please clarify: 1. what is the "latter" which is not an immediate objective? 2. Do all the existing EIF Applications support SAML-2 and/or oAUTH2? Can you please list which application supports what protocol?	**18/06/2020** 1. Managing authorizations in EIF application from the Tool is not an immediate objective. 2.They all support SAML-2. M-Files, Tableau and eFront also support oAuth2

#	Submission date	Publication date	Question subject	Question	Answer
125	08/06/2020 22:33	18/06/2020 17:47	Federated Multifactor authentication System	With reference to section '4.1.5.4', page 17, '... The solution should be supported by a “state of the art” directory (LDAP, Active Directory)...', please clarify: 1) What type of users will be included in the "state of the art" directory? Will it host only the exernal users? Or both internal and external use 2)Should this directory be part of the offering? 3) New Active Directory/LDAP will be installed in terms of this tender or they are already installed in EIF environment?	**18/06/2020** 1) The directory will host both internal and external users. 2) We assume that the solution is embedding a directory, simply describe what it is in the offer. 3) No, see 2) the directory is embedded in the solution, it may as well be proprietary.
126	08/06/2020 22:34	18/06/2020 17:52	Federated Multifactor authentication System	With reference to section '4.1.5.4 (diagram)', page 18, policy scenario-1 (two factors authentication) is applied to "centralised Access", and policy scenario-2 (without two factors authentication) is applied to "Direct Access, please clarify: 1) Why two factor authenitcation for "Direct Access" is not as well required? Is simple authentication accepted? 2) Should the solution distiguish between simple authentication when some applications are accessed by the EIF internal network, and 2FA if they are accessed by the public cloud?	**18/06/2020** 1) Direct access requires as well MFA but for some applications/cases it may only use simple authentication. 2) No, MFA is the current way of accessing SaaS applications.

#	Submission date	Publication date	Question subject	Question	Answer
127	08/06/2020 22:35	18/06/2020 17:54	Federated Multifactor authentication System	With reference to section '4.1.5.6', page 20, '...the Service Provider will be expected to propose a migration project with a clear timeline and foresee resources to run it with the EIF at the earliest stages of the transition phase. The overall cost and the number of expected mandays/profiles required must be defined explicitly in order to achieve the following objectives:..." "...estimated activity of 100 mandays.."...', please clarify: 1) The 100 days effort estimation is to cover the users migration project only? 2) What is the effort estimation for the implementation of the infrastructure and the connectors to the existing applications?	**18/06/2020** 1) 100 mandays is the expected project effort to ""design"" and install the solution (if not based on SaaS), create required connectors, migrate users and authorizations and support EIF to prepare internal communication before migration. 2) See 1), we identified this task as part of the 100 mandays. It is a high level estimation, feel free to provide what you believe is the actual effort to implement the proposed solution.
128	08/06/2020 22:35	18/06/2020 17:55	Federated Multifactor authentication System	With reference to section '4.1.5.7', page 20, 21, '...The responsibilities of the Service Provider are:...', please clarify: 1) What is the effort estimation for the supprt & maintenance activities? 2) Is the Users management Operation a requirement for the ServiceProvider?	**18/06/2020** 1) Support and maintenance activities should be quoted as part of the run cost. The tenderer has a description of the technical scope, number of applications, number of users and will not be in charge of users' provisioning so it should base its answer on that information and its own knowledge and experience. 2)No, EIF will cover the provisioning activities.

#	Submission date	Publication date	Question subject	Question	Answer
129	08/06/2020 22:36	18/06/2020 17:57	Federated Multifactor authentication System	With reference to section '4.1..5..6 Migration of current users and settings', page 20, please provide the existing information to be migrated. We assume that similar data is expected to be held.	**18/06/2020** The assumption is correct, userid (and related information), status, permissions (when applicable), roles membership should be kept from one system to another. Other technical settings (such as timeout values for instance) should be kept as well.
130	08/06/2020 22:36	18/06/2020 18:33	Federated Multifactor authentication System	With reference to section '4.1..5..7 Support and additional maintenance requirements', page 20, please clarify: The support/maintenance effort is not estimated. can you please clarify if needed? Is it only the platform support needed?	**18/06/2020** Support and maintenance activities should be quoted as part of the run cost. The tenderer has a description of the technical scope, number of applications, number of users and will not be in charge of users' provisioning so it should base its answer on that information and its own knowledge and experience. To clarify as well, EIF will cover the provisioning activities.
131	08/06/2020 22:37	18/06/2020 18:35	Logs collection, storage and event monitoring services	With reference to section '4.1.6.2', page 22, '...Providing access to the logs for each desired EIF application is the sole responsibility of the EIF ……', please clarify: 1) How will the application logs be collected? 2) Do they have an API?	**18/06/2020** 1) Analysis is part of the assignment. Since a good number of systems are running on Linux, we may use syslog to forward logs. It may be that on Windows hosted applications, we need to manually fetch from (or push to a specific place) the logs or install an agent if applicable. 2) API may exist as well but this not a generic feature.

#	Submission date	Publication date	Question subject	Question	Answer
132	08/06/2020 22:37	18/06/2020 18:37	Logs collection, storage and event monitoring services	With reference to section '4.1.6.2', page 22, '...monitoring and controlling events in the IT Security domain related to the EIF ecosystem on an 8x5 (working hours per working day) basis from 9AM to 5PM;...': 8x5 is very appropriate if a "security log monitoring service" is to be provided eg for reviewing the users accesses or the admin activities. However if "treat hunting" and protection against cybersecurity attacks is a requirement, a 24x7 SOC service should be more suitable, because eg if a IOC appears within the weekend, this will be considered next working day. 1) Please verify that a 24x7 service is not a requirement. 2) What kind of incidence response SLAs will be used? Tender specifies only reporting SLAs but not incidence response scheme.	**18/06/2020** 1) Given the scope focusing mostly on application logs initially, we shall start by 8x5. We do not oppose to a proposal with 24x7 as an option. 2) Once an incident will be escalated to EIF, it will trigger the EIF incident management process. Escalation will be done to the Cloud application provider and followed-up with EIF carefully. The service provider shall be notified. For specific cases we may trigger consultancy for forensics analysis.

#	Submission date	Publication date	Question subject	Question	Answer
133	08/06/2020 22:38	18/06/2020 18:39	Logs collection, storage and event monitoring services	With reference to section '4.1.6.3', page 23, '...A project planning shall be given as well as the number of mandays needed to complete the integration and the type of profiles needed. The EIF estimates that the effort on this is of 100 mandays...', please clarify: What is the foreseen effort for the maintenance and support of the infrastructure and for the Security Monitoring-logs monitoring operations?	**18/06/2020** Support will be response to incident related to the service (disruption, security) as well as possibly answering to a reasonable number of EIF questions and proceeding to minor changes (such creating very simple use case or updating a more complex security use case for instance). More demanding effort (such as building complex use cases) should probably require use of "build" mandays.
134	08/06/2020 22:38	18/06/2020 18:41	Logs collection, storage and event monitoring services	With reference to section '4.1..6..4 Additional maintenance requirements', page 24, please clarify: In the maintenance section 4.1.6.4, no effort is mentioned for the platform/solution maintenance. Will this effort has to be estimated by the bidders?	**18/06/2020** In section 4.1.6.4, we have written: "Besides monthly service reviews with a Service Delivery manager (transversally to all services), the EIF also expects the regular presence of a senior engineer (30 days per year to help with the on-boarding of new applications and to devise new IOCs and their implementation)."

#	Submission date	Publication date	Question subject	Question	Answer
135	08/06/2020 22:39	18/06/2020 18:42	Vulnerability scanning and reporting maangement	With reference to section '4.1..7..2 Technical and service level requirements', page 24, '...Scans should be run independently from each other: 1 external scan (from a public network) to assess the perimeter security and 1 internal scan by the mean of Virtual Private Cloud...', please clarify: how the service provider will gain access for performing the internal scan ?	**18/06/2020** The design needs to be defined in detail first but it might be that a dedicated VPC or equivalent needs to be created on the Provider side and that a peering could be the solution to connect a probe and the "cloud application provider" environment.
136	08/06/2020 22:39	18/06/2020 18:45	Vulnerability scanning and reporting management	With reference to section '4.1..7..4 Additional maintenance requirements', page 26, please clarify: In the maintenance section 4.1.7.4, no effort is mentioned for the platform/solution maintenance. Will this effort has to be estimated by the bidders?	**18/06/2020** In section 4.1.7.4, we have written "The Service Provider should foresee onsite activities of 30 mandays of a standard engineer per year at the EIF or remotely in order to: • On-board new applications into the vulnerability management process; • Improve the dashboard and the reporting based on additional requirements."

#	Submission date	Publication date	Question subject	Question	Answer
137	08/06/2020 22:40	18/06/2020 18:48	Pentesting Services	With reference to section '4.1.11 Pentesting services', page 29, '...Any time during the term of the Framework Agreement, the EIF may request specific penetration testing in order to assess the security of its Cloud core environments. Consultancy Services in Fixed Price (FP) mode shall be used onsite at the EIF. The EIF will target to “pentest” all its environments on a yearly basis. Besides initial testing, Pentesting exercises will require single retesting of supposedly fixed environments (by the application providers)....', please clarify: Pentest scope includes Applications only or Applications and their respective systems and DBs? If scope includes systems and DBs, can we setup a VM into EIF infrastructure? Please clarify how often EIF will request the specific penetration testing.	**18/06/2020** We try to have a holistic approach here so testing (when relevant) of systems and DB is of interest although a priority must be given to the accessible application interfaces (publicly or privately). Preferably a VM should rather be installed on the Provider's end as it would have no interest in EIF premises (as a reminder only Cloud applications will be tested). The process to request a pentest shall be simple: *EIF will submit a formal assignment to the provider and will describe the scope and expected modus operandi (a prior step will be for EIF to obtain formal acceptance of the Application provider on the possibility to run the pentest). *the Provider will submit a proposal with a number of mandays based on the scope and the expected seniority. *Once accepted by EIF, preparation meetings shall happen between EIF, the Service provider and the third party to be pentested and a date to start activities will be convened.

#	Submission date	Publication date	Question subject	Question	Answer
138	09/06/2020 15:59	18/06/2020 18:52	Page limit of Technical Offer	Our understanding is that, the CVs provided as part of Question 1.3 of the Technical Offer will not be included while calculating the overall page limit of 80 pages. CVs will be considered as additional supporting documentation which is outside the 80 page limit for Technical Offer. Please confirm.	**18/06/2020** Indeed, CVs can be added as annexes. Please note that the following has been stated in the Template of the Technical Offer: The Technical Offer shall not exceed the total of forty (40) recto-verso A4 sheets outside mandatory annexes.
139	09/06/2020 17:27	18/06/2020 18:55	Section 4.1..5..3 Description of the user experience File EN-Annex 4 - Terms of Reference.pdf	We'd like to clarify the login flow. After successfully login to the centralized SSO landing page, user will see his/her granted applications and he/she will be able to launch any those application without being requested to re-enter the credentials. However, inside this action, the Privileged Access Management has to send a login request with his/her entered credentials to the application to verify (this background action is necessary to eliminate the case user knows the application link and can access directly). Therefore, does each application provide a login API for other apps/third-parties to integrate with?	**18/06/2020** Not sure we see the relationship with the PAM here. The PAM should only be considered in the context of administrative accesses to support the applications. EIF users will not go through the PAM so the flow shall remain the same. EIF admin may have a different flow to manage the applications, that is not an issue (as long as Identity Providers and authentication system remain the same).

#	Submission date	Publication date	Question subject	Question	Answer
140	09/06/2020 17:29	18/06/2020 18:58	Section 4.1.6 Log collection, storage and event monitoring services File EN-Annex 4 - Terms of Reference.pdf	Hello, we have a few questions as below: 1. To be able to collect logs centralized, Service Provider needs to install and configure a log agent in the application's instance to ship the logs to the centralized log collection service. Is this OK? Or do you have any requirement for this? 2. What kind of event alert/notification mechanism do you prefer or expect? 3. What is maximum latency that the Monitoring Service detects the incident? 4. What is the retention period of log data in the Log Collection?	**18/06/2020** 1. We should favour the least intrusive approach here. If agent installation is required, it should be studied with EIF and the Cloud Application Provider supporting its own application with its own standards or operations. 2.Email notifications first for supposed low/medium incidents. Email and phone call for a high/critical incident. 3.4 hours should be a maximum (during working hours). 4.Ideally 6 months of "live" logs, 6 months of archived logs would be a good start.

#	Submission date	Publication date	Question subject	Question	Answer
141	10/06/2020 18:40	18/06/2020 19:01	SOC Location	In section: 4.1.6.1 Background, your tender states: “The Service Provider will host the SOC in its facilities. The location of the SOC shall be limited to countries that ensure an adequate level of protection equivalent to the one ensured by the European Directive 2018/1725 EU-DPR, no data or “metadata” shall be sent outside the EU-28 Member-States by the Service Provider.” Article 47 of the European Directive 2018/1725 EU-DPR allows for transfers to third countries on the basis of an adequacy decision, while article 48 allows for alternative mechanisms based on transfers subject to appropriate safeguards. Can tenderers propose use of these mechanisms within the regulation – e.g. part of our business is within the UK which has yet to be deemed adequate when the Brexit transition period expires; could we consider use of Article 47 if adequacy is granted or one of the mechanisms within Article 48 within a compliant response?	**18/06/2020** Yes, we follow the directive(s) including the exceptions allowed inline with proper safeguards.

#	Submission date	Publication date	Question subject	Question	Answer
142	10/06/2020 18:46	18/06/2020 19:05	4.1..4..1 Key Management System for the Management of requested services	With regards to the requirements “4.1..4..1 Key Management System for the Management of requested services” could you please specify which of the required services described in the Tender would need to be encrypted and have the key managed by this system? Would the Advisory Services and PenTest Services be included?	**18/06/2020** Today we have ad hoc encryption on a per Cloud application basis. EIF Cloud Providers are using the existing KMS of the infrastructure cloud provider like AWS or Azure. Encryption is used across EIF solutions to encrypt storage (S3, blob), OS (EBS or equivalent), database (via TDE). Understanding what BYOK/BYOE could bring to EIF, what are advantages and how the implementation would go on, is part of the initial assignment. Overall we expect encryption in transit and at rest. Any exchanges of sensitive nature between the Service provider and EIF shall be encrypted so this may apply to outcomes of advisory services or pentesting activities too.

#	Submission date	Publication date	Question subject	Question	Answer
143	11/06/2020 09:41	18/06/2020 19:07	Ressources profiles	Requirements define profile: Subject matter expert, engineer with a large experience in a specific technology filed (at least 5 years not necessarily all continuous but largely specialised); Senior Engineer, engineer with at least 5 years of relevant experience in the area of Cyber Security or IT Infrastructure (as per the scope defined in the relevant sections); Standard Engineer, engineer with 2 to 5 years of relevant experience in the area of Cyber Security or IT Infrastructure (as per the scope defined in the relevant sections); Junior Engineer, engineer with up to 2 years of relevant experience in the area of Cyber Security or IT Infrastructure (as per the scope defined in the relevant sections). On top or in replacement of years of experience, can you please recognise other ways to prove professional capacity of the team (like cloud certifications). Some areas are more recent (Cloud, SaaS products), 5 years of experience might be difficult to have even for skilled team members.	**18/06/2020** We can understand that seniority requirements for some specific areas may be difficult to reach. Relevant certifications and project achievements will then be evaluated as well.

#	Submission date	Publication date	Question subject	Question	Answer
144	11/06/2020 13:14	18/06/2020 19:16	Vulnerability assessment and penetration testing	Can you please clarify on the following aspects: By vulnerability assessment and penetration testing of the cloud services we are to include all supporting components which support the delivery of the SaaS services, including any operating systems, administrative interfaces (SSH or RDP for example), back-end databases and services, VPN infrastructure or any other physical or virtual components? Or is the scope limited to the SaaS applications/portals, and all attack vectors should focus on exploiting vulnerabilities identified in the SaaS applications (for example SQL injections, cross-site scripting, XML/JSON attacks, authentication bypass, etc.)?	**18/06/2020** Initially, we want to understand more accurately the surface attack on our SaaS applications. With the yearly repetition of pentesting exercises, we may request to look deeper at the security of infrastructure related components.

#	Submission date	Publication date	Question subject	Question	Answer
145	12/06/2020 11:58	18/06/2020 19:18	Questions deadline	As the analysis of the technical specifications for presenting a solid technical proposal requires a significant amount of time, we consider the 3 weeks given for questions submission, a rather small period. Usually, the questions deadline in EU tenders is 5-7 working days before the offer submission deadline. Since the tender deadline has been set for the 7th of July, could you please extend the deadline for submission of questions for at least 1 week?	**18/06/2020** Unfortunately we cannot extend the questions deadline any longer. We invite you to see all questions and provided answers from/to all tenderers to get additional understanding of service requirements.
146	12/06/2020 16:08	18/06/2020 19:20	Encryption services	In the description of the Encryption services, you mention that the KMS shall support all encryption processes related to delivery of the services in the TOR. Does it mean that you expect the encryption services to be provided only for the newly delivered components from the TOR, or you expect to provide encrypting services to existing systems as well? Which are these services and which are the vendors, including Databases and Operating Systems and storage components.	**18/06/2020** Of course, new components shall be integrated. Today we have ad hoc encryption on a per Cloud application basis. EIF Cloud Providers are using the existing KMS of the infrastructure cloud provider like AWS or Azure. Encryption is used across EIF solutions to encrypt storage (S3, blob), OS (EBS or equivalent), database (via TDE). Understanding what BYOK/BYOE could bring to EIF, what are advantages and how the implementation would go on, is part of the initial assignment for the existing EIF Cloud applications.

#	Submission date	Publication date	Question subject	Question	Answer
147	12/06/2020 16:16	18/06/2020 19:45	Penetration Tests	We have some questions regarding the Penetration Tests service: 1. As we understand you request one initial pentest at the beginning and additional pentest exersises during the same year for validation of the fixed environments based on the initial pentest result. Please confirm that or provide additional information. 2. Please provide a list with all the applications/systems which you need to be included in the pen test scope. 3. Do you expect PCI DSS Assessment as part of the Pen Test Services? 4. You mention that the consultancy services shall be delivered onsite at the EIF. Do you allow remote execution of part of the pen test assessment activities.	**18/06/2020** 1.Our process is indeed to have a yearly pentest for all our cloud applications. We do not currently specify that we need a retest of supposedly fixed applications but we might upfront of an assignment decide to foresee a ""retest"" depending on criticality of the application or severity of information reported by our vulnerability management process on a specific application. 2.These applications are defined in the Annex 4 document, #4.1.1 3.No 4.Besides specific considerations related to the Covid 19 pandemic, we of course agree that part of a pentest is done remotely.
148	12/06/2020 16:17	18/06/2020 19:46	Vulnerability Assessment	Do you expect scanning for vulnerabilities any Endpoint Devices or only Servers at the EIF cloud?	**18/06/2020** Only servers at the EIF Cloud.
149	12/06/2020 16:31	18/06/2020 19:49	EN-Annex 5a - Template of the Technical Offer - Resumes	Can the CVs be provided as annexes to the technical offer (disctinct files) or must they be embedded into it?	**18/06/2020** They can be provided as annexes.

#	Submission date	Publication date	Question subject	Question	Answer
150	12/06/2020 16:36	18/06/2020 19:51	EN-Annex 5a - Template of the Technical Offer	In Annex 5a, page 1, can "Encryption Services" be split into two sections "Key Management System" and "Secure Cloud document storage" as the first one is common to several other services? This is proposed to improve readability of the tenderers' proposal.	**18/06/2020** Yes, this can be done in 2 separate sections.
151	12/06/2020 16:53	18/06/2020 19:57	Identity & Access Management - Current directory	Current OneLogin integration: can we assume this is integrated with the on-premise Active Directory at EIF (or EIB?)	**18/06/2020** No, this is not integrated with on-premise AD. This may be integrated (with EIB) at a later point in time but very unlikely during the first year of service.
152	12/06/2020 16:54	18/06/2020 20:28	CVs	According to the template for the Technical Offer (Annex 5a), “CVs of staff demonstrating the capacity and level of expertise to implement, run the services and further build on them”. Also, “The Technical Offer shall not exceed the total of forty (40) recto-verso A4 sheets outside mandatory annexes”. We understand that the CVs will be annexed to the technical offer, thus not counting in the 40 pages limitation. Could you please confirm our understanding or clarify further?	**18/06/2020** Yes, CVs can be put as annexes.

#	Submission date	Publication date	Question subject	Question	Answer
153	12/06/2020 16:55	18/06/2020 20:33	Identity & Access Management: External Users	How will external users be defined? Will these get credentials in the EIF Active directory, should these be defined on the identity platform only or should these sign-in with their own company account?	**18/06/2020** They will be defined on the identity platform only as local users (that it is to say on the local directory embedded in the IAM solution).
154	12/06/2020 16:55	18/06/2020 20:37	Relevant experience	According to the Terms of Reference, section 7.2.2, “Technical and Professional criteria”, page 40, “Tenderers must have at least 3 (three) relevant and verifiable references of assignments carried out in the last 3 (three) years. Each reference shall describe an assignment of a minimum of 300 mandays”. It is our understanding that there is no specific requirement in the duration of each relevant and verifiable assignment, as long as it covers the minimum 300 man-days. Could you please confirm our understanding or clarify further?	**18/06/2020** Yes, assignments need to be longer than 300 mandays and they need to be carried out in the last 3 (three) years.

#	Submission date	Publication date	Question subject	Question	Answer
155	12/06/2020 16:55	18/06/2020 23:47	Relevant experience	It is our understanding that a verifiable reference is considered relevant if the following 3 requirements are covered: a) the provided services cover at least one of the technical services in scope of this Call for Tenders b) the services have been provided by similar type of staff, as detailed in the TOR per service c) more than 300 man-days were consumed in the assignment Could you please confirm our understanding or clarify further?	**18/06/2020** By "similar type of staff", it is meant in terms of seniority (relatively close at least).
156	12/06/2020 16:55	18/06/2020 23:49	SFTP Services	Could you please specify the profiles and seniority level of the staff EIF expects to be involved in the implementation of SFTP services?	**18/06/2020** A standard engineer profile is expected.

#	Submission date	Publication date	Question subject	Question	Answer
157	12/06/2020 16:56	18/06/2020 23:50	Cloud Subject Matter Expert	In relation to the EIF's definition of a Subject Matter Expert (at least 5 years not necessary all continuous but largely specialized), please note that broad implementation of Cloud solutions is relatively recent in the IT landscape, so the 5 years specialisation to Cloud technologies is quite rare for a Cloud Expert. It is our understanding that a candidate with long track record in state-of-the art technologies, significant experience in implementing and consulting on Cloud solutions, holding relevant certifications by accredited Cloud Providers would be considered eligible for the Cloud Subject Matter Expert profile. Could you please confirm our understanding or clarify further?	**18/06/2020** We appreciate this element and indeed relevance of Cloud experience and certifications are a guarantee to obtain subject matter expert profile.
158	12/06/2020 16:59	18/06/2020 23:51	Penetration testing	Penetration testing is requested ad-hoc basis any indication about the desired lead time within this framework agreement?	**18/06/2020** It seems fair to start discussion for an assignment 1 to 2 months before actual execution.

#	Submission date	Publication date	Question subject	Question	Answer
159	12/06/2020 17:02	18/06/2020 23:53	File Encryption	Can we have an estimated value of the content & services that are in the scope of the encryption solution? So an indication on the actual content and services that are required to be encrypted.	**18/06/2020** Today we have ad hoc encryption on a per Cloud application basis. EIF Cloud Providers are using the existing KMS of the infrastructure cloud provider like AWS or Azure. Encryption is used across EIF solutions to encrypt storage (S3, blob), OS (EBS or equivalent), database (via TDE). Understanding what BYOK/BYOE could bring to EIF, what are advantages and how the implementation would go on, is part of the initial assignment. Overall we expect encryption in transit and at rest. Any exchanges of sensitive nature between the service provider and EIF shall be encrypted so this may apply to outcomes of advisory services or pentesting activities too.
160	12/06/2020 17:06	18/06/2020 23:54	Security Log Monitoring: Log Collection	Could you provide an estimate about the amount of logs that are send on a daily basis. This can be in defined in Events per Second or X GB/day.	**18/06/2020** A high level estimate would be 6000 events per day initially.

#	Submission date	Publication date	Question subject	Question	Answer
161	12/06/2020 17:20	18/06/2020 23:56	Annex 5a - Template of the Technical Offer / CVs	In the provided Template of the Technical Offer, under the Service Provider Solutions description part, it is requested by the tenderer to provide CVs of the staff demonstrating the capacity and the level of expertise. It is our understanding that we can use the europass CV template or any other format since the authority does not provide any specific template. Please confirm our understanding or clarify further.	**18/06/2020** Yes, your understanding is correct. Europass is a valid CV format.
162	12/06/2020 17:23	18/06/2020 23:59	Annex 14 – Terms of Reference / Technical and professional capacity	Technical and professional capacity requirements, page 40/44, “Tenderers must have at least 3 (three) relevant and verifiable references of assignments carried out in the last 3 (three) years”, while in page 41/44 EIF requests “3 (three) relevant and verifiable references of assignments carried out in the last 3 (three) years. Each relevant and verifiable reference should be numbered from one to three. If a Tenderer submits more than three references, only the first three will be accepted as part of the selection procedure”. Can you please clarify if a tenderer can actually provide more than three relevant project references?	**18/06/2020** 3 references may be or not be enough to illustrate relevance on all required services so we can accept more than 3 references.

#	Submission date	Publication date	Question subject	Question	Answer
163	12/06/2020 17:22	19/06/2020 00:02	Annex 14 – Terms of Reference / 4.3 Critical success factors and key performance indicators	Annex 14 – Terms of Reference page 30/44, the Requested Services along with the Number of measured KPIs are listed. It is our understanding that in the provided Assignment Reference Tables (ARTs) by the tenderer it is not mandatory to be covered all the ten Services, but it is sufficient to be covered the majority of them, i.e. eight out of ten. Please confirm our understanding or clarify further.	**19/06/2020** Correct, the provider just needs to demonstrate its relevance as a proficient cybersecurity / Cloud service provider.
164	12/06/2020 19:36	19/06/2020 00:03	IAM	Who are external user exactly? Do the accesses or type of access differ between internal or external users, or do they have access to the same applications?	**19/06/2020** External users are business counterparts, they would access a subset of EIF Cloud applications, nothing specific (to date).
165	12/06/2020 19:37	19/06/2020 00:04	Penalties	We have different SLA and associated fees at risk associated to these. Could you confirm in which case the % of penalities is only applicable to the associated services or when it would be applicable to a broader scope of services (as is explained for encryption)? As there is no Reporting services per se, would that means that the penalties is applicable to the full set services?	**19/06/2020** To explain EIF's philosophy, penalties are the last resort case in a very degraded situation already highlighted during service management reviews. Generally, percentile applies to the service impacted and not the full range of service. Specific services that could bring a downtime on all EIF Cloud applications maybe looked differently but this is a very ultimate resort once more.

#	Submission date	Publication date	Question subject	Question	Answer
166	12/06/2020 19:37	19/06/2020 00:06	PAM	Our understanding is the privileged access management access is required for our own personal only? Could you confirm ?	**19/06/2020** That is the first goal of the PAM indeed. EIF maybe interested in mid-term to look at the possibility to extend access to its more technical staff (up to 10 people) or some third party providers but this would require some prior planning and definition.
167	12/06/2020 19:38	19/06/2020 00:07	Cloud Service consumption	Can we assume that cloud services consumption (Servers, DB, Cloud HSM..) will be procured and paid by the respective services owners of the different environments, the Cloud federator provider procuring these for its own environment.	**19/06/2020** The cost of respective underlying cloud services consumption should be factored in all the various run cost of services and invoiced as such. The Cloud Provider shall indeed procure them for its own environment but resources used by EIF shall be clearly identifiable as part of an asset register.
168	12/06/2020 19:38	19/06/2020 00:09	Cloud services consumption	In case the Cloud Federator services are hosted on Azure or AWS, is the EIF subscription to be used or is it our own subscription to be leveraged? The invoice would then directly be paid by EIF ?	**19/06/2020** The cost of respective underlying cloud services consumption should be factored in all the various run cost of services and invoiced as such. The Cloud Provider shall indeed procure them for its own environment but resources used by EIF shall be clearly identifiable as part of an asset register. A general invoice shall be sent on a monthly basis to EIF with details about run cost (not only cloud consumption cost) per service.

#	Submission date	Publication date	Question subject	Question	Answer
169	12/06/2020 19:39	19/06/2020 00:10	SFTP	Is there a specific speed or bandwidth requirement for SFTP?	**19/06/2020** Since we are targeting system to system integration only, there is no need for very high speed transfers.
170	12/06/2020 19:39	19/06/2020 00:11	Encryption	Is there a specific speed or bandwidth requirement for encryption?	**19/06/2020** As we have ad hoc encryption on a per Cloud application basis, there is no holistic view on this question. No encryption process is currently creating any bottleneck on our applications. There is no easy answer to the question. Should this have an impact on the quote on your side, we understand that you will make some hypotheses to justify volumes (low/medium volume according to our estimation).
171	12/06/2020 19:39	19/06/2020 00:13	Budget	The pricing sheet refers to a 4 year period while the annex 4 refers to a budget for 7 years. Is there a budget limit set for the 4 years ?	**19/06/2020** We indeed have a budget for 7 years. EIF only asks for pricing for the first 4 years as it is understood that committing on prices beyond 4 years is not easy. Nonetheless, it makes sense that the maximum budget for the first 4 years is relatively close to 4/7 of the maximum budget over 7 years. Deviations shall be explained to reflect on potential service cost decrease after 4 years.

#	Submission date	Publication date	Question subject	Question	Answer
172	12/06/2020 22:02	19/06/2020 00:15	General	Can you provide the background information about the problem statement that should be solved with this project?	**19/06/2020** There is no "problem statement" to mention, just the need and will to improve EIF services delivery in terms of compliance with security standards and best practices.
173	12/06/2020 22:02	19/06/2020 00:16	IAM/SSO	For how many users are you planning to enable IAM/SSO capabilities?	**19/06/2020** Please see #4.1.5.4. 800 "internal users" and up to 1200 external users. External users seats are not needed in the first stage (year) and will be licensed progressively year by year throughout the engagement.
174	12/06/2020 22:03	19/06/2020 15:22	IAM Solution	In the context of an IAM solution have you considered capabilities such as Identity Governance and Management such as joiner-mover-leaver, access management, access certification? Or is the scope limited to only providing SSO capabilities at this time?	**19/06/2020** In short/mid terms we only look at the "SSO/authentication" capabilities. In mid-long term, we may federate with a directory at EIB group level that will help with the Joiner/leaver/transfer management but this would be a "build" project to be addressed at a later stage.
175	12/06/2020 22:03	19/06/2020 15:23	SSO	Have any systems already been configured to support SSO capabilities?	**19/06/2020** See part 4.1.5 of Annex 4 document. Current system is OneLogin.

#	Submission date	Publication date	Question subject	Question	Answer
176	12/06/2020 22:03	19/06/2020 15:24	SSO	If the scope of the project is only limited to enable SSO capabilities, have you considered any SSO vendor?	**19/06/2020** No, we are vendor agnostic. There is a solution in place (OneLogin) but outlook is totally open.
177	12/06/2020 22:04	19/06/2020 15:25	SSO	What mechanisms are you currently using for providing SSO authentication? For e.g. Windows domain, Portal application or Identity management application	**19/06/2020** OneLogin is a portal application with embedded Identity management features.
178	12/06/2020 22:04	19/06/2020 15:26	Authentication	What authority is currently being used to authenticate users? For e.g. LDAP authentication, database authentication etc.	**19/06/2020** OneLogin has an embedded directory and authenticates users itself either by password or with a specific software token.
179	12/06/2020 22:05	19/06/2020 15:27	Access management	How is access currently provided/updated/revoked?	**19/06/2020** This part is being managed by EIF and follows an internal process with manual operations to date. This will continue, so the provider is not expected to intervene here directly however EIF expects some support to help in automating the process when possible.
180	12/06/2020 22:05	19/06/2020 15:28	IAM	How many applications do you plan to onboard into the IAM system as part of this project?	**19/06/2020** Today, we have 5 applications but number is likely to increase (double or even more) in mid-long term.

#	Submission date	Publication date	Question subject	Question	Answer
181	12/06/2020 22:05	19/06/2020 15:29	Integration with IAM system	What are type of systems which are in scope for integrating with IAM system? For e.g. Active Directory, Email, ERP, CRM Portals, Mainframe, etc.	**19/06/2020** See part 4.1.5.6. We are only talking about EIF cloud business applications.
182	12/06/2020 22:06	19/06/2020 15:30	IAM system	Where are these systems hosted? For e.g. on premises, cloud, which cloud provider?	**19/06/2020** All these systems are hosted in the Cloud (AWS or Azure).
183	12/06/2020 22:07	19/06/2020 15:31	privileged access management system	Do you have a privileged access management system in place? How is privileged access currently managed/certified?	**19/06/2020** No we do not have such infrastructure in place yet. High privileges are only managed at application level to date.
184	12/06/2020 22:07	19/06/2020 15:32	Integration of IAM system with ticketing	Are you planning to integrate the IAM system with SIEM/ticketing solution/PAM solution? Will this be part of the current project?	**19/06/2020** SIEM and ticketing system are in the scope. For PAM this has not been requested explicitly but would be something to consider in mid-term in a specific project (5 to 10 accesses on EIF side could be required).
185	12/06/2020 22:08	19/06/2020 15:33	Data Warehouse	(4.1.1) Where are Group Data Warehouse and Business Modelling tool hosted?	**19/06/2020** The group DWH is hosted internally by EIB. The business process tool is in the cloud (Azure).

#	Submission date	Publication date	Question subject	Question	Answer
186	12/06/2020 22:09	19/06/2020 15:35	Terms of Reference - 4.1.11	(4.1.11) Are there any specific requirements regarding the scope (type) of penetration testing and whether there will be a pentesting plan set-up at the beginning of the year for the whole year based on release plans?	**19/06/2020** The overall plan is to cover all EIF cloud applications on a yearly basis. We may indeed discuss early in the year, the scoping of each pentest (black, grey or white box) and to set-up a proper planning. This belongs to the service management delivery to be established between the Service Provider and EIF.
187	12/06/2020 22:09	19/06/2020 15:36	Terms of Reference - 7.2.2	Is the limit of 3 References applicable for the whole proposal and scope of project or for each of specific services (as described in par. 4.1)?	**19/06/2020** 3 references are foreseen for the whole scope (a reference may cover different services) but it may not be enough to illustrate relevance on all required services so we can accept more than 3 references for the whole project.
188	12/06/2020 22:10	19/06/2020 15:37	Applicable regulations	What are regulations (internal, local, global) which enforce encryption and according to which the Encryption should be compliant ? Are any certifications on the solutions prescribed ?	**19/06/2020** There is no EU regulation that "enforces" encryption. EU Commission said repeatedly it does not want to weaken encryption so encryption shall adhere to best practises in terms of algorithms and key strengths. Certifications on specific encryption hardware device are welcome.

#	Submission date	Publication date	Question subject	Question	Answer
189	12/06/2020 22:10	19/06/2020 15:38	Generic additional Encryption services	What purposes are the Generic additional Encryption services required for ? - for Data encryption on storages in the datacentre ? In what form - application, transparent data encryption on specific storage / database solution ? - End2end transfer C2B, B2B, both. (customer to business, business to business) - for standard communication channels - e.g. Outlook encryption etc - for specific communication channels - e.g. payment services etc., support of custom applications - other ?	**19/06/2020** Today we have ad hoc encryption on a per Cloud application basis. EIF Cloud Providers are using the existing KMS of the infrastructure cloud provider like AWS or Azure. Encryption is used across EIF solutions to encrypt storage (S3, blob), OS (EBS or equivalent), database (via TDE). Understanding what BYOK/BYOE could bring to EIF, what are advantages and how the implementation would go on, is part of the initial assignment. Overall we expect encryption in transit and at rest as well. Any exchanges of sensitive nature between the Service provider and EIF shall be encrypted so this may apply to outcomes of advisory services or Pentesting activities too.

#	Submission date	Publication date	Question subject	Question	Answer
190	12/06/2020 22:10	19/06/2020 15:40	type of data need to be encrypted	What type of data need to be encrypted? - data and documents in rest in databases, shared storage, cloud storage - communication messages - voice records, - instant messaging ? - VPN connection	**19/06/2020** Today we have ad hoc encryption on a per Cloud application basis. EIF Cloud Providers are using the existing KMS of the infrastructure cloud provider like AWS or Azure. Encryption is used across EIF solutions to encrypt storage (S3, blob), OS (EBS or equivalent), database (via TDE). Overall we expect encryption in transit and at rest as well so this includes as well communication channels / user interfaces.
191	12/06/2020 22:11	19/06/2020 15:42	adhoc file encryption/sharing solution	What purposes is the adhoc file encryption/sharing solution required for? - Endpoint (workstation, mobile) data encryption - sharing solution encryption - other ?	**19/06/2020** EIF would need an application that targets 25 users initially and up to 50 users. This solution is for specific exchanges of very sensitive documents so the volume and its increase should be limited (probably up to 5GB). In average file size is probably 1 to 5MB. Endpoint data encryption is not the first goal of this application.
192	12/06/2020 22:11	19/06/2020 15:43	sharing solution	What sharing solution is used since it needs to be extended by Encrpytion/sharing?	**19/06/2020** The need is to define the solution from scratch and not adapt any other solution.

#	Submission date	Publication date	Question subject	Question	Answer
193	12/06/2020 22:11	19/06/2020 15:44	encryption services	Are encryption services required to provide both symmetric and assymmetric encryption schemas ?	**19/06/2020** Both are required indeed.
194	12/06/2020 22:12	19/06/2020 15:45	cryptographic devices	Are any cryptographic devices (HSM, cloud key vaults, smartcards) already available at EIF for encryption ? What vendor ? Should it be part of a delivery ?	**19/06/2020** Today we have ad hoc encryption on a per Cloud application basis. EIF Cloud Providers are using the existing KMS of the infrastructure cloud provider like AWS or Azure. EIF users have smartcard but we did not include them in the scope right now for any cryptographic activities since we do not have our hands on the supporting PKI (this may be looked into at a later stage).
195	12/06/2020 22:12	19/06/2020 15:47	Key management system	Is any Key management system (in any form - proces-paper-application driven) in place already with established policies ?	**19/06/2020** Today we have ad hoc encryption on a per Cloud application basis. EIF Cloud Providers are using the existing KMS of the infrastructure cloud provider like AWS or Azure. Encryption is used across EIF solutions to encrypt storage (S3, blob), OS (EBS or equivalent), database (via TDE). This is being managed by Cloud application providers.

#	Submission date	Publication date	Question subject	Question	Answer
196	12/06/2020 22:13	19/06/2020 15:48	encryption keys	Is PKI infrastructure with policies set available to certify assymmetric encryption keys ?	**19/06/2020** No PKI dedicated to EIF is currently available. Public EIF certificates are generated by Globalsign with the help of EIF colleagues. Specific public certificates are created by Cloud Application builders.
197	12/06/2020 22:13	19/06/2020 15:49	encryption performance and UX requirements	What are encryption performance and UX requirements - number of messages, files, records in DB ? Prefference in GUI ?	**19/06/2020** We are talking about a number of files of about 200k. DB wise, overall 300M records.
198	12/06/2020 23:08	19/06/2020 15:54	Section 4.1.10 Advisory Services File EN-Annex 4 - Terms of Reference.pdf	We have several questions: 1. Beside of GDPR, is there any other security standards/regulations/compliances EIF must comply? 2. Please share about security solutions and security vendors you are working with (Antivirus, Endpoint Security, SIEM, Vulnarebility Scanning, IDS/IPS, Firewall, Threat Intelligence Feeds,...). 3. Please share about Artificial Intelligence technologies you are using. 4. Please share about Robot Process Automation technologies and vendors you are using.	**19/06/2020** 1. EUDPR is indeed very important. There is no specific EU regulation that we can think of to date but it is also important that the service provider complies with local/national regulations as from where the service is run and from where it is operated. 2. The monitoring services are to fully build from scratch. Some 3rd parties providers are using IDS anti DDOS protection which are native to Cloud offering at AWS or Azure. 3. No Production use to date. 4. No Production use to date.

#	Submission date	Publication date	Question subject	Question	Answer
199	12/06/2020 23:09	19/06/2020 15:56	Section 4.1.8 SFTP services File EN-Annex 4 - Terms of Reference.pdf	We have several questions: 1. What types of hardware or virtual storage does EIF request for support ? 2. Does EIF have requirement on data retention policies: - Access and modification permission - Retention period - Access and modification frequency time & volume	**19/06/2020** The SFTP solution can come with its own low level technical features/requirements. The SFTP server currently in place and to be replaced relies on the service provided by the Red Hat Enterprise 7 operating system, running on an AWS EC2 instance. The daily transfer of files through this server corresponds to approximately 85 files for a total volume (after specific file level encryption) of 50Mb for a standard day. The volume is highly dependent on the daily activity performed on EIF core solutions. These files are used to transfer data between the different EIF systems. After being consumed, the data is archived on AWS S3 with no retention limit (to date but to be discussed and tackled in the future).

#	Submission date	Publication date	Question subject	Question	Answer
200	04/06/2020 10:46	19/06/2020 17:37	Annex 2b - Declaration of honour on exclusion and selection	Declaration on Honour, section VII - SELECTION CRITERIA, points (a) and (b), it is our understanding that point 5(a) should be answered N/A and point 5(b) should be answered YES by an identified subcontractor, to whom the sole tenderer relies to fulfill only the technical and professional criteria, when the sole tenderer will answer YES to these points, as well as to the point 6(c) under the same section. Please confirm that our understanding is correct or clarify further.	**19/06/2020** It is a correct understanding. But please note that the tenderer, each consortia member and each subcontractor have to submit a separate Annex 2b - Declaration of honour on exclusion and selection.
201	04/06/2020 16:40	19/06/2020 17:41	Subcontractors	In case a tenderer relies on the capacities of the subcontractors in order to fulfil the selection criteria, it is our understanding that a signed Letter of Intent/Undertaking should be provided by the subcontractors (in free format) confirming that they will place at the tenderer’s disposal its resources for the execution of the contract. Please confirm our understanding or clarify further.	**19/06/2020** It is a correct understanding. But please note that this information has to be indicated also in the Annex 1 - Tenderer contact sheet (Bidding structure).

#	Submission date	Publication date	Question subject	Question	Answer
202	05/06/2020 17:09	19/06/2020 17:42	Appendix 1 to 5a / Turnover	It is our understanding that in the provided table we should present the overall annual turnover of the company. The proof of this figure will be tenderer’s annual accounts for the last three financial years that will be submitted with the tender as well. Please confirm our understanding or clarify further.	**19/06/2020** It is a correct understanding.
203	05/06/2020 17:10	19/06/2020 17:46	Appendix 2 to 5a / Assignment Reference Tables	It is our understanding that each Assignment Reference Table (ART), should be presented separately and each one needs to be signed by the legal representative of the tenderer. Please confirm our understanding or clarify further.	**19/06/2020** It is a correct understanding. Please not that an ART consists of the three (3) pages and all the pages must be completed.
204	05/06/2020 17:49	19/06/2020 17:54	Legal and regulatory capacity	Could you please explain the following requirement "Where applicable, a confirmation that the required license from the relevant domestic authorities to represent the EIF for the provision of the Services has been acquired.": - What do you mean by "to represent the EIF"? - By license, do you mean an "autorisation d'établissement" in case of a Luxembourg company or similar?	**19/06/2020** This sentence shall be read as 'if applicable'. If not applicable, then there is no need for this kind of license. The tenderer has to submit a relevant document/evidence from the State concerned that they are appropriately registered and authorised to carry out the activity, which forms the subject of the Framework Agreement, under national law.

#	Submission date	Publication date	Question subject	Question	Answer
205	05/06/2020 17:55	19/06/2020 17:59	Economic and financial capacity	The total annual turnover associated with the type of Services, to which the Tenderer is tendering should be more than EUR 2,000,000 for each of the last three (3) available financial years (e.g., 2017, 2018 and 2019 ideally). • Where applicable, this requirement applies to each member of a group of economic operators on a consolidated basis and/or to any foreseen subcontractor (reference is made to section 6.5.1 and 6.5.2). Question: If the main tenderer already has a turnover of more than EUR 2,000,000 for each of the last three (3) available financial years and does not intend to subcontract more than 50% to a single subcontractor, do the subcontractors still need to present their annual accounts or are the annual accounts of the main tenderer sufficient?	**19/06/2020** In the described case the annual accounts of the main tenderer are sufficient.

#	Submission date	Publication date	Question subject	Question	Answer
206	08/06/2020 13:37	19/06/2020 18:03	Tender Submission by Courier	“The Tender must be delivered either by registered post OR by messenger or courier at the reception desk of the EUROPEAN INVESTMENT FUND by 07/07/2020 - 23:59 CET at the latest, as evidenced by the postmark (if sent by registered post) or by the receipt dated and signed by the officer at the EIF reception desk (if delivered by messenger or courier).” Can you confirm that, in case of dispatch of the proposal per courier DHL/UPS, that the evidence of the postmark (i.e. pickup date of the courier service indicated on the waybill) must be dated 07/07/2020 before midnight latest?	**19/06/2020** We confirm. In case of dispatch of the proposal per courier DHL/UPS, the evidence of the postmark (i.e. pickup date of the courier service indicated on the waybill) must be dated 07/07/2020 before midnight latest.

#	Submission date	Publication date	Question subject	Question	Answer
207	08/06/2020 13:39	19/06/2020 18:11	Initialing of documents	“Tendering organisations must submit a full dossier, each page of which must be initialled. Paper version and electronic version must be identical, otherwise Tenders might be rejected for non-compliance with the Terms of Reference.” Does EIF accept not to have all pages initialed? You ask for a paper version identical to the electronic version, this means that each document must be re-scanned after having it initialed, and that the necessary copies must be made after having initialed each page of the full original proposal. For practical reasons, we ask a derogation on the instruction of the initials.	**19/06/2020** Please initial each page of the original tender (paper version). The electronic version of the tender can be without initials.
208	08/06/2020 13:40	19/06/2020 18:12	Documents requiring signature	Regarding documents which require signature, can EIF confirm that two ways of signing is accepted, i.e. ink signature (as original to be provided, or is a scan copy of the signature accepted as well given the CoVid-situation) and / or e-certified signature in accordance with Qualified Electronic Signature (QES) within the meaning of the eIDAS Regulation.	**19/06/2020** We confirm.

#	Submission date	Publication date	Question subject	Question	Answer
209	04/06/2020 10:52	19/06/2020 18:18	Electronic submission instead of paper submission	According to your instructions the final tender needs to be submitted to EIF by two ways, electronically through SmartShare application as well as in paper copy. Kindly note that due to COVID-19 conditions still many administrative authorities in many countries do not work properly and most companies still work remotely. Due to these reasons we kindly request the final submission to be only electronically through SmartShare application and no hardcopies to be sent at your premises.	**19/06/2020** All tenders still need to be submitted in both ways - in paper and electronically.
210	08/06/2020 13:41	19/06/2020 18:20	Tender Submission Requirements	Considering the ongoing Covid19 situation, we are having restricted access to our office premises and have been advised remote working as much as possible. In light of this situation, can we request the EIF to consider ONLY electronic submission of the tender and remove the requirement for paper copies and electronic version in USB stick.	**19/06/2020** All tenders still need to be submitted in both ways - in paper and electronically.

#	Submission date	Publication date	Question subject	Question	Answer
211	08/06/2020 22:21	19/06/2020 18:27	Evaluation Criteria	"For each qualified Tender, the Financial offer will then be verified, where the Financial offer found to be the cheapest will receive 100 points and the Financial offer of the other Tenders will receive a lower score, on a proportional basis." - > Could you clarify the formula that will be applied for the financial score?	**19/06/2020** Let's consider the best offer which would get a score of 100 for a price of P (considering that services requested are fully delivered). If another provider has a price P'=a*P (a >1), then the Provider will receive a grade of 100/a.
212	08/06/2020 22:27	19/06/2020 18:32	Specific terms	For the provision of the security services, additional specific terms and conditions might be required in order to clarify the scope of responsibilities of the different stakeholders. Are we ok to consider that additional specific terms and conditions will be added as part of the assignment ?	**19/06/2020** It depends what is included in those additional specific terms and conditions and whether they do not conflict with any of the EIF terms or conditions. It might be assessed for each assignment separately.

#	Submission date	Publication date	Question subject	Question	Answer
213	09/06/2020 16:58	19/06/2020 18:46	GASC section	With reference to General Administrative and Submission Clauses regarding the documents to be submitted in case of Joint Tender could you please clarify the following: • Annex 1 “Tenderer Contact sheet” should be filled, signed and submitted by the Lead Partner. Could you please confirm? • Annex 2a “Declaration of absence of conflict of interest” should be filled, signed and submitted by the Lead Partner. Could you please confirm? • Annex 2b “Declaration of honour on exclusion and selection criteria” should be filled and submitted by the Lead Partner, Partner and Subcontractors • Annex 2c “Non-collusion declaration” should be filled, signed and submitted by the Lead Partner. Could you please confirm? • Annex 3 “Deed of undertaking” should be filled, signed and submitted by the Lead Partner. Could you please confirm?	**19/06/2020** Annex 1 “Tenderer Contact sheet” should be filled, signed and submitted by the Lead Partner. Information about other consortium members must be indicated therein (Bidding Structure). Annex 2a, Annex 2b, Annex 2c and Annex 3 should be filled, signed and submitted by the Lead Partner and each consortium member separately. Subcontractor has to submit separately only Annex 2b.

#	Submission date	Publication date	Question subject	Question	Answer
214	10/06/2020 11:51	19/06/2020 18:51	Electronic version of the Tender (USB)	It is our understanding that we need to provide along with the paper copy of the Offer, one USB which will include the Technical and the Financial Offer, and not two USBs one for the Technical offer and one for the Financial Offer. Please confirm our understanding or clarify further.	**19/06/2020** It is a correct understanding - one USB with the Technical and the Financial Offer.
215	10/06/2020 11:52	19/06/2020 18:55	SmartShare application	According to the General Administrative and Submission Clauses, page 1/4, the tenderer should send its offer via EIB's Group SmartShare application as well. It is our understanding that we just need to upload all the material that constitutes the Offer (Technical and Financial Offer) before the deadline (07.07.2020 at 23:59 CET) and no specific confirmation will be received by the authority (e-mail message or an online message) confirming our on time upload. Please confirm our understanding or clarify further.	**19/06/2020** It is a correct understanding. You need to upload the Tender on SmartShare before the indicated deadline. There will be no separate confirmation. But please note that Tender must be sent also in paper format before the indicated deadline and there you will have a confirmation about the date and time.

#	Submission date	Publication date	Question subject	Question	Answer
216	12/06/2020 16:21	19/06/2020 19:02	Joint tender	In case of a joint tender, compliance with the selection criteria will be evaluated as a whole or compliance with the selection criteria will be evaluated as a whole and depending on the distribution of the participation of the persons upon the performance of the activities as provided for in the agreement on the establishment of the combination. It is not needed to submit any agreement between the individual members of the temporary grouping, as part of the tender submission.	**19/06/2020** According to Section 6.5.1 of Annex 4 - Terms of Reference: Joint Tenders submitted by consortia or joint ventures will be assessed as follows: • the exclusion criteria (Annex 2b) will be verified for each economic operator individually (see section 7.2.1); • the selection criteria for the legal and regulatory capacity will be verified on an individual basis – each economic operator individually (see section 7.2.2); • the selection criteria for the economic and financial capacity will be verified on a consolidated basis – Lead member and any other member, depending on the extent to which the other member(s) of the group put(s) their resources at the disposal of the Lead member for the performance of the Framework Agreement (see section 7.2.2); • the selection criteria for the technical and professional capacity will be verified in relation to the combined capacities of all members of the group, as a whole, depending on the extent to which the other member(s) of the group put(s) their resources at the disposal of the Lead member for the performance of the Framework Agreement (see section 7.2.2); • the award criteria will be assessed in relation to the Tender as a whole (see section 7.2.3). There is

#	Submission date	Publication date	Question subject	Question	Answer
					a whole (see section 7.2.3). There is no need to submit an agreement between the individual members of the temporary grouping, as part of the tender submission, but all roles and responsibilities and the services that will be provided by each consortium member have to be clarified in the tender.

#	Submission date	Publication date	Question subject	Question	Answer
217	12/06/2020 16:22	19/06/2020 19:06	joint tenders	2. Could EIF please confirm our understanding: 2.1 For joint tenders the award criteria shall be evaluated in relation to the tender submitted as a whole, including all consortium members. 2.2 In case of joint tenders the financial and economic capacity shall be evaluated as a whole. Appendix 1 to 5a - to be completed on a consortium level, containing the turnover figures of each consortium member (in case of joint offer/tender) 2.3 In case of joint tenders the legal and regulatory capacity shall be evaluated on an individual basis - each economic operator individually 2.4 In case of joint tenders the financial and economic capacity shall be evaluated as a whole. (Appendix 1 to 5a - to be completed on a consortium level, containing the turnover figures of each consortium member) 2.5 In case of joint tenders and subcontracting the technical and professional capacity shall be evaluated as a whole. 2.6 The offer shall be signed by the nominated leader in case of a consortium.	**19/06/2020** It is a correct understanding.

#	Submission date	Publication date	Question subject	Question	Answer
218	12/06/2020 16:54	19/06/2020 19:15	Signatures on documents	In case a consortium submits a joint tender, we understanding that: a) Annexes 4, 5a, 6, 7, 8 must be initialed by the Lead member b) Appendix 1 to Annex 5a must be completed and signed by the Lead member c)Appendix 2 to Annex 5a must be completed and each consortium member should sign the ART they provide. Could you please confirm our understandings or clarify further?	**19/06/2020** In case a consortium submits a joint tender, Annexes 1, 4, 5a, 5b, 6, 7, 8 must be initialed and signed by the Lead member. Appendix 1 to Annex 5a must be completed and signed by the lead member and each consortium member, since in case of a joint tender the minimum of economic and financial capacity apply to the group's consolidated turnover. Appendix 2 to Annex 5a must be completed and each consortium member should sign the ART they provide and it has to be signed also by the lead member.
219	12/06/2020 16:54	19/06/2020 19:17	Language of official documents	According to page 2 of the General Administrative and Submission Clauses, point 5, "Tenders must be drawn up in English". We understand that any official documents issued by national authorities that need to be provided as evidence (e.g. for legal and regulatory capacity), may be submitted at the EU language of the country that issued the document. Could you please confirm our understanding or clarify further?	**19/06/2020** It is a correct understanding.

#	Submission date	Publication date	Question subject	Question	Answer
220	12/06/2020 16:55	19/06/2020 19:22	Relevant experience	According to Appendix 2 of Annex 5a, “Assignments which started before this three (3) years period but which are still ongoing may be submitted”. It is our understanding that assignments that started before this 3 years period but ended within these 3 years, or assignments that started within this 3 years period but are still ongoing are eligible. Could you please confirm our understanding or clarify further?	**19/06/2020** The Tenderer has to provide three (3) relevant and verifiable references of assignments carried out in the last 3 (three) years. The assignment must have been carried out within the three (3) years period preceding the submission of the tender. So, assignments which started before this three (3) years period but which are still ongoing may be submitted. And also assignments that started before this 3 years period but ended within these 3 years and assignments that started within this 3 years period but are still ongoing are eligible. The main idea is that assignments are carried out in the last 3 (three) years.
221	12/06/2020 22:15	22/06/2020 17:17	TERMS OF REFERENCE: paragraph: 6.6 Estimated value of the Framework Agreement	For the last 3 years of Services, the Service Provider should be able to apply annual indexation rates based on consumer price index in the IT market (supported by Eurostat or equivalent publication) and possibly cover currency exchanges if the Service Provider procures services in a different currency.” What is the formula to be used to calculate the indexation for last 3 years?	**22/06/2020** EIF authorises the increase probably indexed on consumer price index. An average of this last index for the 5 last 10 years may be used as an estimate for calculation, for instance, if in year 4 price is p4, I is average index for 5 last years (e.g., I is to be read 1,02 if index is increasing by 2% over the last 5 years), then max price for p5 should be p5=I*p4 the max p6 =I*p5…