Cyber Security Review RFP - Questions and Answers

RFP Response and Contracting

1. Who will be the engaging party for this engagement for contracting, will it be CGIAR System Organization only or will it be CGIAR System Organization and the 15 Centers? Answer: The entity in charge of this process and subsequent contracting is the CGIAR System Organization based in Montpellier France.

2. Could you please confirm that the potential invoice address is in France? Could you please confirm if CGIAR System Organization is eligible to provide a 'Certificat d'exoneration de la TVA et/ou des droits d'accise' for the potential invoice? Answer: Yes, the invoice address is in Montpellier France and the CGIAR System Organization will provide a tax exemption certificate.

3. Does CGIAR System Organization (which has around 40 staff) has separate IT function and internal audit function? Answer: Yes, the CGIAR System Organization has a separate IT and Internal Audit Function respectively.

4. Who will be the overall engagement coordinator on the part of CGIAR? Answer: The overall engagement coordinator will be the Head, CGIAR System Internal Audit Function.

5. The review to be performed is offsite as per the RFP, please specify if you will assign point of contact from each RFP (and to whom do we address the proposal letter)? How many cybersecurity focal points are in each Centre and in the CGIAR System Organisation and are these dedicated functions. Answer: There will be one focal point and approximately 16 interlocutors. The focal point / project liaison will be the Internal Audit function of CGIAR System who will coordinate administrative logistics between the consultant and designated interlocutors from 15 CGIAR Centers and the CGIAR System Organization respectively. The proposal should be addressed to the CGIAR System Organization procurement team as indicated in the RFP.

6. What will be the consulting arrangement? Is this full outsourcing or co-sourcing of review services? Answer: Full outsourcing.

7. Do you have general contract template to be used for this engagement? Or do we use our firm’s contract format and terms? Answer: We have a contract template and terms of reference which will be shared and discussed with the selected consultant during the contracting phase.

8. Is there an incumbent and are they eligible to bid on this project? If so, who was the incumbent? Answer: No there is no incumbent. The Internal Audit function of CGIAR System has not engaged a consultant previously for similar services.

9. Are you willing to share a list of all bidders who have expressed an interest in this project? Answer: No, this information is confidential and not available for sharing. This is an open tender and all eligible firms are invited to participate.

10. As we know, CGIAR has 15 entities/members. Does the cybersecurity review have to cover all 15 entities? or can we select only the local entities we are operating in? Is there a requirement that requires us to coordinate with our colleagues abroad where the other CGIAR members operate? Answer: As specified in the RFP the review must cover 15 CGIAR Centers and CGIAR System Organisation. The level of interaction/ cooperation within your networks is at your discretion.

11. What are the regulations applicable to each of 15 Centers and the System Organisation (E.g.: GDPR in Head Office)? Does CGIAR have a complete list of all compliance obligations across all locales? Answer: There are no legal requirements in relation to Cyber Security in CGIAR; it is largely driven by stakeholder expectations. Due to the status of International Organisation of the Centers (or majority of them) local legal requirements may not be applicable.
12. Will the dates for processing of the assignments can get shift because of the current ongoing COVID scenario? The proposed timeline (p. 3 of the RFP) for the project is approaching fast. To what extent are the dates for completion outlined in the RFP project schedule flexible? Actual working days available is 31 days to submit the draft report. Will there be any extension? Answer: Taking into consideration the developments in COVID-19 situation the timelines to respond to the RFP have been updated and published on the CGIAR website. The execution and reporting timelines will be discussed and agreed with the selected consultant.

13. In case of unforeseen situations like non availability of resources from CGIAR, how soon we need to intimate for extension of timeline? Answer: It is expected that there will be an ongoing communication with the point of contact both formally and informally where delays being experienced will be discussed and escalated to concerned parties. Extension of timeline of the project will be discussed and agreed as and when need arises.

Proposal Contents & Presentation

1. We noted that the proposal format should be in Microsoft Word or similar format. Can we submit in pdf or should it be strictly in Word document format? Answer: Word document format is preferable however the proposal can be submitted in PDF.

2. Do you have preferred font style (e.g. Calibri, Arial, etc.)? Answer: The font used is at the discretion of the consultant.

3. What will be the method of shortlisted bidders’ presentation? Answer: We will communicate further details to the shortlisted bidders.

4. Do you have a proposal fee cap or maximum budget per engagement for our costing consideration in mind for this project and can you share that with us? By understanding your budget expectations, bidders can maximize their scope of work within your financial constraints and recommend ways to meet your requirements with your budget. Answer: We don't normally disclose the budget, or its range, the bidders are required to provide their financial proposal commensurate with their proposed technical approach.

5. Do we need to specify our approach in conducting PT and phishing simulation and our capabilities in this proposal? You mention that the work in phase 2 will be informed to a certain extent on the results of phase 1. This makes quoting a fixed fee for Phase 2 quite difficult to estimate. Can you please clarify that you wish a fixed fee quote to include both phases? Answer: Yes, it is desirable to include the consultant’s approach in conducting Penetration Testing and Phishing simulations. If yes, could we insert in an annex without considering the limit of 20 pages of the proposal core (phase 1)? Does the 20-page limit on the narrative proposal also includes Appendixes? Answer: The proposal should be succinct and tailored to address the requirements specified in the RFP. However, the page limit on the narrative proposal does not extend to the appendices. Could you please confirm that it is not required to quote the effort for phase 2 at the moment? Answer: The costing/quote for phase 2 is not required when responding to the RFP however please provide a rough estimate, say by a pentest

6. Can our company participate in this RFP even thought we did not receive the invitation directly from CGIAR? Answer: We confirm that this is an open bid and any eligible firm can participate.

7. Will all potential bidders receive copies of all submitted questions and answers issued as an addendum to the RFP? Answer: All potential bidders will receive all submitted questions and answers issued as an addendum to the RFP published on the CGIAR website.
8. We are asked to provide “Knowledge and experience of CGIAR/its Centers and the agriculture science sector” of the project team; Please clarify if this is mandatory or any other experience with similar size projects in other sectors is also acceptable. Answer: Knowledge and experience of CGIAR/its Centers and the agriculture science sector is desirable but not mandatory. Experience with similar size projects in similar sectors is acceptable.

9. You state that "No on-site visits are envisaged as part of this review; all work will need to be carried out remotely." However, there is a request to indicate "travel" costs in the financial proposal. Please clarify. Answer: There is a small likelihood that travel might be needed to present the results of the engagement. Please indicate related travel costs.

Project Management

1. For data and file exchange, will this be hosted also in Bluejeans portal? If not, what will be the medium of data / documents exchange? We use Zoom as its preferred virtual conferencing platform. Is this acceptable (reference page 2, consultancy details, bullet 2)? We will be using online interview-based assessment tools to effectively manage the activity, will that be permitted? will testing walk through will be provided by online video conferencing? Will you be in a position to collect screen shots as evidence, to be part of our audit work papers? Answer: Given the sensitivity and nature of assignment we will discuss and agree on the file exchange and data collections mechanisms with the selected consultant. We are flexible on the virtual conferencing platforms used and welcome suggestions from the consultants responding to the RFP.

2. Regarding this statement: "No on-site visits are envisaged as part of this review; all work will need to be carried out remotely". Does this mean we are expected to conduct the review fully by phone/e-mail? Including the presentation of the results? Do we plan to conduct project status meeting? If so, how frequent and what platform? Answer: The frequency and nature of the project status meeting will be informed with the agreed upon milestones. All meetings will be conducted remotely using agreed upon virtual conferencing platforms.

3. Do you have preferred credentials for consultants to be assigned for the project? Do you have minimum number of team members expected for this engagement? Answer: Refer to the RFP. The applicants must demonstrate prior experience and technical knowledge of conducting similar reviews within a context of a complex international organization with distributed structures. The minimum number of team member required for execution of the engagement is at the discretion of the consultant.

4. Are we required to have local counterparts in the country where a CGIAR Research Center operates or our team should be sufficient to handle the in-scope Centers, virtually? Answer: Refer to the RFP: No on-site visits are envisaged as part of this review; all work will need to be carried out remotely hence team structure and location is at the discretion of the consultant.

5. What are the departments /functions/ organisation structure of the in-scope entities? Could you please list the services that are transversal/horizontal for all the organizations? (e.g. Purchasing, human resources, legal, internal audit, etc.) Answer: All CGIAR entities predominantly have independent operations with limited transversal services. The main functions at an entity level include Research, Finance, Resource Mobilisation, IT, Human Resource, Legal, Facilities & Administration.
Execution

1. Please indicate the primary and secondary locations to be considered as a part of the review. Answer: The review will cover 15 CGIAR Centers and the CGIAR System Organization Headquarters and Field offices respectively.

2. Will CGAIR System Organisation be consenting to run the consultant’s proprietary scripts to be run on technology platforms (databases / operating system / network infrastructure)? Answer: The respective CGIAR entities coordinated through the IT community of practice will be requested to provide consent for the consultant to run proprietary scripts on the technology platforms.

3. Revalidation testing is not part of the scope as per the RFP, please confirm. Concerning point 2 Scope of Work (Phase 1), please clarify whether your request refers to a review of the validity of the processes and methodology followed in order for the assessment to be performed or to a validation of a sample of assurance activities tests results. In case your response is the latter, how many cases would be considered as sufficient sample? Answer: In line with the RFP the consultant will be expected to review results of previous assurance engagements and IT policies to assess adequacy of design of the controls to mitigate against cyber security risks and vulnerabilities.

4. How do CGIAR envisage achieving the synergy between the cyber security and the data management maturity assessments? In 2020 CGIAR System IAF will also perform a data management maturity assessment. The synergy between the cyber security and the data management maturity assessment will be highly desirable. Could we have a copy of the ICT shared services governance charter to understand its scope? Answer: We would prefer both assignments to be carried out simultaneously such that operational efficiencies are achieved.

5. How are IT policies established? Are policies established at the CGIAR System Organization level or does each CGIAR Center also establish its own policies? Concerning point 3 of Scope of Work (Phase 1), please define the number of IT Policies to be reviewed. Answer: There is no hierarchical relationship between the System Organization and the Centers. The review will cover security policies, procedures and management practices across 15 CGIAR Centers and the CGIAR System Organization established at the respective entities. The Internally developed IT Security and Cyber Risk assessment security tool can used as a reference material to inform processes and controls in places across the CGIAR System, recommendations to improve the tool will be desirable.

6. How is cybersecurity governance organized at CGIAR and all of the entities? What documentation is available to help the winning bidder respond to Phase 1, item 4 (page 3 of the RFP)? Concerning point 4 of Scope of Work (Phase 1), please clarify what aspects of governance will be assessed. Answer: Aspects to be assessed should cover the entire spectrum of Cyber Security Leadership and Governance including cyber security oversight and organizational structures, strategy, policy, culture, roles and responsibilities, awareness and security training. Cybersecurity governance is mainly established and managed at each center level hence resource documents to be sought directly from CGIAR entities. However, a ICT community of practice that brings Center/System Organization ICT leaders together to discuss and agree upon collective actions to address cyber risks.

7. What is the situation regarding the Management of IT Operations for these 15 entities? Is it centralized or decentralized for each entity? Is there a specific body within CGIAR (e.g. a Share Service IT Security Team) responsible for overseeing cybersecurity practices across the members? Answer: As specified in the RFP: the IT operations within CGIAR are largely decentralized with each CGIAR entity (i.e.15 CGIAR Centers and the CGIAR System Organization in this document) being responsible for establishing independent IT security policies and safeguards to protect the respective CGIAR entity’s
information assets against increasingly sophisticated cyber-attacks. There is no specific designated body within CGIAR responsible for overseeing cybersecurity practices across the CGIAR System.

8. Regarding the Phase-1 scope of work, do we also need to perform penetration testing and simulated phishing attacks, or are we only reviewing the results of the penetration testing and simulated phishing attacks conducted previously by other parties? For phase 2, could you please confirm that no on-site visits apply? (since internal penetration testing is requested in page 3) Answer: Refer to the RFP, phase 1 includes only review and analysis of results of relevant assurance activities (i.e. cybersecurity assessment, penetration tests, simulated phishing attacks) carried out in the past two years by CGIAR Center IT functions, Internal Audit teams and the CGIAR System IAF. Phase 2 will be informed by the results of phase 1 where all the work and presentation of results are meant to be done remotely.

9. How many cybersecurity and information security projects have been addressed in the last two years or so? (Order of magnitude). Have these projects been implemented in CGIAR (central) or also in the other 15 Centres? Answer: Across 16 CGIAR entities cybersecurity and information security assurance activities have been carried out in the last two years; the consultants should work with an estimate of at least one engagement per entity.

10. Whether Two years Risk Assessment reports of all Centers will be shared soon after the contract is signed? Whether above reports will be sent by single contact or auditor has to collect from 15 centers and the CGIAR System Organisation individually. Answer: It’s expected that the consultant will prepare a detailed information request list at inception of the project to facilitate collation of all information required for the review. The information will be collected directly from 16 CGIAR entities included in the scope.

11. Has any type of assessment like that described in the RFP been done in the past for any of the CGIAR Centers and CGIAR System Organization, and if so, will the results of that assessment be made available to the winning bidder during the engagement? Answer: Refer to the RFP relevant cybersecurity and information security projects have been carried out by CGIAR Center IT functions, Internal Audit teams and the CGIAR System IAF and its expected that results of the above-mentioned reviews will be collected and analysed as part of scope of the assignment.

12. Please describe how information technology operations are provided at CGIAR? Are services centralized or decentralized? Answer: Refer to the RFP Information Technology are mainly decentralized however there are some ICT shared services including Active Directory and Office 365.

13. Are all the 16 CGIAR entities in separately segregated network infrastructure or within single network architecture? Answer: All CGIAR entities have separate segregated network infrastructure.

14. Are there any external branches or field offices/DR site in-scope of the review? If yes, list them and indicate if they are reachable from the Head Office? Answer: Refer to RFP as pertains to operation of CGIAR entities across multiple geographical locations. Detailed information regarding location of field offices will be provided during the review.

15. Are all the 16 CGIAR entities separated with separate firewalls for each network or managed via single firewall system. Answer. Yes, the CGIAR entities have separate firewall for each network.

16. Does each IT infrastructure is on centralised cloud or data center or in distributed application & data centers? Answer: It’s a combination of both some IT infrastructure is on centralised cloud others on distributed application & data centers.

17. Is there a specific framework CGIAR wishes to be assessed against in Phase 1, item 5 (page 3 of the RFP)? Given the international nature of CGIAR, we assume that CGIAR may prefer the ISO27001 framework. We also assume that all CGIAR Centers and CGIAR System Organization will be assessed using the same framework. Is this correct? For the methodology of cyber security review, do we use
the consultant’s, or we benchmark with CGIAR entities cyber security methodology? Answer, the assumption is incorrect, the CGIAR entities have adopted different cyber security frameworks, it is expected that the consultant will recommend the framework that is appropriate for entities with similar distributed operations and the same will be used for the assessment.

18. Does CGIAR or its entities information technology groups support any research with special compliance requirements? Answer: To some extent however some of the research units have IT teams supporting the IT infrastructure (referred to as shadow IT in the RFP).

19. Can you provide an organizational chart for information technology unit(s) for each entity in scope? Answer: An organisational structure for information technology unit(s) for each entity in scope will be share or discussed with the selected consultants.

20. Do you have preferred phishing scenarios / program for Phase 2 or can we suggest our own approach for testing? Answer: The consultant can suggest their own phishing scenarios.

21. Will employees for phishing simulation be determined by CGIAR System Organisation or the Organisation? Answer: The number of employees for phishing simulations will be determined by the consultant in collaboration with the CGIAR System Internal Audit Function based on the results of phase 1.

22. Given the local and global nature of the engagement are there any language fluency requirement that are required or would impact the delivery of the service? Will all interviews be conducted in English? Answer: All interviews will be conducted in English.

23. What is the CGIAR security awareness platform? Answer: A significant number of CGIAR entities utilise knowbe4 as the security awareness platform.

Reporting

1. Regarding the expected deliverable. Although it is briefly described in the last paragraph of the first page of the RFP document we would like to clarify if:
   a. Is it expected an individual report to be developed for each centre?
   b. Or is it expected a global executive report for CGIAR with the aggregated information, and with the security evaluation report and proposal of initiatives for each center? Answer: The engagement’s output will be a combined report presenting an aggregated assessment of cyber security arrangements across CGIAR.

More specific questions related to IT infrastructure and assets are not included as they are deemed either too sensitive or irrelevant for the purposes of this RFP. Such information can be collected as part of phase 1 so that the consultant has an appreciation of the institutional context.

As outlined in the RFP, phase 1 will entail an understanding of the institutional context through a preliminary risk assessment, review of existing policies and procedures and review and analysis of relevant assurance activities conducted in the past two years on the subject matter with a focus on areas of interest specified in paragraph 1 of the RFP. Outcome of phase 1 will inform the activities that will be carried out in phase 2 hence detailed scoping for phase 2 is not required while responding to the RFP. The consultant should make an assumption as pertains to CGIAR System computer systems, applications and network devices and infrastructure when responding the RFP based on previous experience performing cyber security assessments for similar entities.