REQUEST FOR PROPOSAL

No. HPI200113US
Audit Engagement – SOC for Cybersecurity

Funded By
Heifer Project International

RFP Release Date:	January 10, 2020
Performance Period:	February 2020
Proposal Submission Deadline:	January 24, 2020
Question/ Inquiry Submission Deadline:	January 16, 2020
Electronic submission to the attention of:	Kim Ahlgrim
Electronic submission:	Procurement@heifer.org
Contact information for inquiries about this RFP:	Procurement@heifer.org

REQUEST FOR PROPOSAL

Terms of Reference

I. General Information

This document is being issued to solicit proposals from qualified auditors to perform an independent assessment of Heifer International's (Heifer) current cybersecurity controls under the AICPA's SOC for Cybersecurity guidance, with the aim toward continued development of Heifer's cybersecurity risk management program (CRMP). The contract will be managed by Heifer's Vice President of Risk Management and Assurance and will be funded through Heifer's Finance and Administration Division headquartered in Little Rock, Arkansas.

These terms of reference contain background information, the timeframe for performing the assessment and expected deliverables. This document also contains information about the kind of expertise that Heifer seeks for this activity and guidance on how to submit a proposal to conduct the activity.

Heifer anticipates awarding a contract for services (which may take the form of an engagement or arrangement letter) for this independent audit consultancy service, with payments based on deliverables submitted to and accepted by Heifer's Vice President of Risk Management and Assurance. The award agreement will include a payment schedule with specific deliverables; all payments require thirty (30) business days processing after approval of deliverables.

II. Background

Heifer International is a global not-for-profit organization working to end hunger and poverty while caring for the earth by using sustainable practices and engaging smallholder farmers in agricultural development and access to inclusive market systems.

Heifer offices (U.S. and internationally) use core global systems with centrally managed integrations, change controls, access rights, security, backups and disaster recovery controls. Most significant core systems include Unit4 Business World Enterprise Resource Management (ERM), Blackbaud Constituent Relationship Management (CRM) and LaserFiche Enterprise Content Management (ECM). Additionally, with these core systems and Heifer's web platform, Heifer headquarters (HQ) systems teams manage several incoming and outgoing data integrations, file transfers and API connections with third-party providers. Microsoft 365 provides Heifer's suite of globally standard productivity tools. Microsoft Active Directory and Active Directory Federation (ADFS) are centrally managed for Single Sign On (SSO) and network and system user access controls. Zoom Unified Communication platform with Office 365 integrations have been added to facilitate meetings, trainings and collaborations.

Issues of data protection and cybersecurity are recognized as topmost risks, associated with a wide range of damaging effects possible from a major breach. Heifer leverages processes such as penetration testing and other vulnerability and risk assessments, but has not previously undergone an independent third-party assessment specifically utilizing the AICPA's SOC for Cybersecurity guidance. Therefore, we view this engagement as an opportunity to gain assurance that the highly significant business issue of cybersecurity is being appropriately and continuously addressed by our organization as we are working to develop and continuously improve our global cybersecurity risk management program.

III. Purpose and Objective

The main purpose of this RFP is to identify an assurance partner to provide reasonable assurance over Heifer's cybersecurity risk management program (CRMP) with independent insight into the effectiveness of Heifer's cybersecurity controls.

a) Specific Objectives

Ultimately, our specific objective is an independent, entity-wide assessment of Heifer's CRMP under the AICPA's SOC for Cybersecurity guidance, providing reasonable assurance as to the adequacy and effectiveness of Heifer's CRMP and cybersecurity controls.

We acknowledge management's responsibility for establishing Heifer's cybersecurity objectives; for designing, implementing, operating and documenting its CRMP and for continuously assessing effectiveness of cybersecurity controls. To that end, Heifer management seeks independent audit consultancy services in development of the organization's CRMP.

b) Scope of Work

- Gain an understanding of Heifer's cybersecurity risk environment.
- Assess the adequacy of Heifer's cybersecurity policies, processes and controls designed to manage the organization's global cybersecurity risks.
- Identify CRMP gaps, providing actionable recommendations for improvement, prioritized based on level of cybersecurity risk.
- Provide results and reporting with documentation and content sufficient to facilitate management's continued efforts in developing and refining the organization's CRMP.

c) Deliverables:

Throughout engagement: in-person and/or Zoom update meetings; detailed pending items list (requests to/from) ensuring shared understanding throughout; immediate alerts of any critical vulnerabilities identified or other urgent observations

Reporting:

- Complete written report summarizing scope of work performed along with detailed results, recommendations and supporting content to facilitate cost- and time-efficient management action
- Concise executive summary (PowerPoint: 1 to 2 PPT slides with key points / graphics; Written: no more than 5 pages written)
- Availability to present results via Zoom meeting, possibly recordable, for internal sharing as may be requested by senior management and/or the Audit Committee

Proposed schedule:

Activity/Deliverable	Responsible	Due date
Planning*	Heifer / Audit Firm	February 3-7, 2020
Field Work	Audit Firm	February 10-21, 2020
Draft Report	Audit Firm	February 21, 2020
Final Report	Heifer / Audit Firm	February 28, 2020

d) Relationship and Responsibilities

Heifer's Vice President of Risk Management & Assurance will be the auditor's central point of contact for management of the engagement. Primarily responsible to coordinate and monitor the organization's cybersecurity controls and CRMP, Heifer's Director of Information Technology & Services will be available throughout the engagement and will facilitate information requests as needed with the various systems teams. The contractor will keep these two primary Heifer contacts informed of their progress at agreed upon intervals. During the engagement, the contractor may seek and receive additional information and clarification from the above-mentioned staff.

IV. Required Expertise

The auditor must be a reputable firm with assigned team members who are experienced in SOC for Cybersecurity consultancy and assessment services as per AICPA guidance. Knowledge and expertise with current and emerging international regulations and standards regarding cybersecurity and related issues of data protection is important. While not critical to this engagement, cybersecurity experience specific to not-for-profit organizations and, more targeted, to international non-governmental organizations (INGOs), will be recognized as a strong plus.

V. Proposal Submission Requirements:

All interested respondents will submit their proposals as outlined below.

Qualified audit firms interested in providing these services are requested to submit a proposal typed in size 12 font by January 24, 2020 to email: Procurement@heifer.org. Please include the name of the person in your organization who will be involved with negotiating the contract as well as your telephone and email contact.

Submission must be typed single-spaced on standard type white paper. All pages must be numbered. Your proposal must include Heifer's RFP reference number **HPI200113US** and the name of your organization at the bottom of each page.

1. Technical Proposal

a. **General Information** [summary not to exceed 1 page]
   i. Organization/firm's overview and capacity statement specific to this RFP
   ii. Links to website and to specific web pages or resources outlining the firm's service offerings, publications, client testimonials or other content particularly relevant to this RFP
   iii. Examples of similar previous work.

b. **Technical Approach** [summary not to exceed 3 pages]
   i. Detail of the proposed engagement approach and methodology
   ii. List and briefly describe the team and individuals proposed for the assignment, indicating the role of each and the qualifying skill set for the assignment (additional information to be included in Cost Proposal).
   iii. A clear and comprehensive work plan, outlining the major activities, responsibilities and time schedule, indicating the level of support that will be required from Heifer. Work plan should include, but not be limited to, acknowledgement and agreement with all requirements as well as explanations, where applicable, of the intended plan to achieve the objectives, requested

scope of work and deliverables. Refer to c. Attachments below for documents we are requesting as proposal attachments for the purpose of facilitating rapid kickoff and assurance planning for the anticipated engagement.

c. **Attachments**

i. Indicative / proposed Prepared by Client (PBC) List: checklist of information the auditor will require from Heifer management and systems teams to enable performance of the engagement as requested. Indicate by when the information will be needed.

ii. As applicable, standard systems or control questionnaires used by the auditor for this type of engagement. If none are used, to what inquiries must we be prepared to respond?

2. Cost Proposal

Proposed budget must be submitted separately to email: Procurement@heifer.org. The cost proposal should provide proposed hourly or task costs as well as a total cost and clear details as to how the total cost is determined. Assumptions or unknown variables that may impact the cost must be highlighted. Include information regarding:

- Hourly / daily rates by assigned staff level (building off the team proposal included in the Technical Approach outlined within the Technical Proposal)
- Anticipated hours and fees associated with each phase of engagement
- Representative engagement expenses (costs of travel, etc.)

Heifer reserves the right to request further information supporting detailed costs and prices.

3. Forms (see Appendix A, B and C)

☐ 1. References – Appendix C
☐ 2. Intent to Bid – Appendix B
☐ 3. Mutual Non-Disclosure Agreement – Appendix A

4. Late Submissions and Verification

Proposal received after the submission deadline will not be considered. Respondents are responsible to ensure their proposals are submitted according to the instructions stated herein.

Heifer retains the right to terminate this RFP or modify the requirements upon notification to the respondents.

VI. Selection Criteria

Submitted proposals must clearly demonstrate alignment with the scope of work outlined above with appropriate level of details. An agreement will be signed with the respondent whose proposal follows the instructions in this RFP, provides best price and value for Heifer. Proposals will be evaluated according to the following criteria:

Proposal evaluation focus	Percentage
Relevance of the proposed technical approach and methodology, demonstrating understanding of Heifer's request, and considering the organization's INGO environment	30%
Proposed team: expertise, competencies and availability	20%

Completeness and clarity of proposal as aligned to RFP instructions (general information, activity plan, budget, team expertise, etc.)	10%
Budget justification and costs realism	40%
Total	100%

The selection committee will evaluate the technical proposal based upon the criteria listed above and the financial proposal will evaluate the reasonableness of costs and cost-effectiveness in the budget.

VII. Validity of Proposals

Proposals submitted shall remain open for acceptance for sixty (60) days from the last date specified for receipt of the proposal. This includes, but is not limited to pricing, terms and conditions, service levels, and all other information. If your organization is selected, all information in this document and the negotiation process are contractually binding.

VIII. Award Process and Contract Mechanism

No.	Activity Deadlines	Due date
1	Issuance of Request for Proposal	Fri, January 10, 2020
2	Q&A via Email	Thu, January 16, 2020
3	Proposal Deadline	Fri, January 24, 2020
4	Selection Committee Review	Tue, January 28, 2020
5	Notification of Award	Wed, January 29, 2020
6	Award Agreement Negotiation	Fri, January 31, 2020
7	Anticipated Contract Execution	Fri, February 7, 2020

Heifer will issue a service provider contract based on submission and Heifer acceptance of the proposal. Once an award is issued, it will include payment schedule with deliverables specified above.

The ***Intent to Bid*** and ***Non-Disclosure Agreement*** must be submitted **prior** to January 16, 2020 by email to procurement@heifer.org.

IX. Limitations

This RFP does not represent a commitment to award a contract, to pay any costs incurred in the preparation of a response to this RFP, or to procure or to contract for services or supplies. Heifer reserves the right to accept or reject in its entirety and absolute discretion any proposal received as a result of the RFP.

X. Other Contract Requirements

Standard Contract: The awarded contractor will be expected to enter into a contract that is in substantial compliance with Heifer Project International's standard contract https://media.heifer.org/About_Us/inside-heifer/Procurement/US_Independent_Contractor_Agreement_SF_T&C_July_27,_2018.pdf
Proposal should include any desired changes to the standard contract. It should be noted that there are many clauses which the HPI cannot change.

Ownership Generally. Any intellectual property (including but not limited to copyrights, trademarks, service marks, and patents), intellectual property rights, deliverables, manuals, works, ideas, discoveries, inventions, products, writings, photographs, videos, drawings, lists, data, strategies, materials, processes, procedures, systems, programs, devices, operations, or information developed in whole or in part by or on behalf of Contractor or its employees or agents in connection with the Services and/or Goods (collectively, the "Work Product") shall be the exclusive property of HPI. Upon request, Contractor shall sign all documents and take any and all actions necessary to confirm or perfect HPI's exclusive ownership of the Work Product.

Prior-Owned Intellectual Property. Any intellectual property owned by a Party prior to the Effective Date ("Prior-Owned IP") shall remain that Party's sole and exclusive property. With regard to any of Contractor's Prior-Owned IP included in the Work Product, Contractor shall retain ownership, and hereby grants HPI a permanent, non-exclusive, royalty-free, worldwide, irrevocable right and license to use, copy, reproduce, publicly display, edit, revise, perform, and distribute said intellectual property, in any format or any medium, as part of the Work Product.

Work Made for Hire. To the extent copyright laws apply to the Work Product, the Parties agree that (a) HPI specially ordered or commissioned the Work Product, (b) the Work Product is a "work made for hire" under United States copyright laws, and (c) HPI shall be deemed the author thereof and shall own all right, title, and interest therein. To the extent such rights, in whole or in part, do not vest in HPI as a "work made for hire", Contractor hereby irrevocably grants, assigns, and transfers to HPI, exclusively and in perpetuity, all of Contractor's rights of any kind or nature, now known or hereafter devised, in, to, and in connection with the Work Product, and HPI shall solely and exclusively own any and all rights therein, and in the elements thereof, including but not limited to any and all allied, ancillary, subsidiary, incidental, and adaptation rights. Contractor hereby waives any and all rights known as "moral rights", and any similar rights, which Contractor may have in connection with the Work Product. The description of Services and/or Goods provided in this Agreement shall in no way limit the manner in which HPI may use the Work Product.

XI. Applicable Regulations

Respondents must be legally registered to operate within Arkansas and comply with local applicable legislation, including but not limited to labor law, financial requirements, taxes, etc.

Notices. All reports, notices, demands or other communications hereunder must be in writing, and shall be deemed to have been given to the applicable Party (a) upon receipt, if delivered by hand or via a courier service requiring a written delivery receipt, (b) within three (3) business days of mailing, if sent via Certified or Registered Mail, Return Receipt Requested, or (c) upon sender's receipt of proof of a successful electronic transmission to the applicable Party, if sent via facsimile or electronic mail. Current contact information for

the Parties is provided beneath their respective signatures below, and may be updated by the applicable Party in writing from time to time.

Miscellaneous. No amendment or modification of this Agreement shall be valid or effective, unless in writing and signed by both Parties. This Agreement is to be construed and enforced in accordance with the laws of the State of Arkansas and the United States of America, without regard to any applicable rules addressing conflicts of laws. The provisions of the *United Nations Convention on Contracts for the International Sale of Goods* shall not apply to this Agreement. The State courts in Pulaski County, Arkansas, and the United States District Court for the Eastern District of Arkansas, all located in Little Rock, Arkansas, shall have jurisdiction and venue with respect to any and all disputes arising in connection with this Agreement. In the event this Agreement is translated into a language other than English, the English language version shall prevail in the event of any difference of interpretation. This Agreement contains the entire understanding of the Parties with respect to the subject matter contained herein, and supersedes any prior or contemporaneous terms, representations, statements, or agreements, whether made orally or in writing, with respect to the subject matter contained herein. If any provision of this Agreement shall be held to be prohibited by or invalid under applicable law, such provision shall be ineffective only to the extent of such prohibition or invalidity, without invalidating the remainder of such provision or any remaining provisions of this Agreement. The failure or delay of HPI to require performance of, or to exercise any of its powers, rights, or remedies with respect to any term or provision of this Agreement, shall not affect HPI's right at a later time to enforce any such term or provision. This Agreement shall inure to the benefit of the Parties and their successors and heirs, but may not be assigned by Contractor in whole or in part. Each of the undersigned expressly warrants his or her authority to enter into and execute this Agreement on behalf of the respective Party. This Agreement may be executed manually or by any electronic means, and delivered manually or by any electronic means. This includes, but is not limited to (1) signing manually, (2) signing digitally, (3) delivering via facsimile transmission, and (4) scanning signatures into a portable document format (PDF), or any similar format, and delivering via electronic mail or any other electronic means. Facsimiles, scans, and other digitally-reproduced copies will be considered originals for all purposes. Such execution and delivery shall be valid, binding, enforceable, and fully admissible under applicable law. This Agreement may be signed in counterparts and, if so signed, each signed counterpart shall be deemed an original. Nothing in this Agreement is intended to, or shall be construed to, give any individual or entity (other than the Parties), any legal or equitable right, remedy, or claim under or in connection with this Agreement. Headings included herein shall not be used to interpret the meaning of the Agreement.

XII. APPENDIX A: Mutual Non-Disclosure Form

Mutual Non-Disclosure Agreement

This MUTUAL CONFIDENTIALITY AGREEMENT ("Agreement") is entered into as of _____, 20___ ("Effective Date"), by and between HEIFER PROJECT INTERNATIONAL, an Arkansas nonprofit corporation ("Heifer"), and _____, a(n) _____ ("Company"). For good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto (singularly a "Party" and collectively the "Parties") agree as follows:

Section 1. Relationship/Warranties. Parties contemplate a relationship whereby Company may complete certain work and/or projects for Heifer ("Project"). In order for Company to complete the Project each Party (the disclosing Party is known hereinafter as the "Discloser") must provide to the other Party (the receiving Party is known hereinafter as the "Recipient") certain proprietary, secret, confidential and/or other information not generally available to the public, which may include but not be limited to trade secrets, project participant information, donor information, fundraising and business strategies, materials, processes, procedures, systems, computer programs, devices, operations, personnel records, and financial information ("Confidential Information"). THE CONFIDENTIAL INFORMATION IS PROVIDED "AS IS", AND DISCLOSER MAKES NO WARRANTIES, EXPRESS, IMPLIED OR OTHERWISE, REGARDING THE ACCURACY, COMPLETENESS, OR PERFORMANCE OF THE CONFIDENTIAL INFORMATION.

Section 2. Confidentiality/Damages. No license is granted hereby, and the Confidential Information shall remain Discloser's property. The Confidential Information is being disclosed to Recipient solely for the express purpose of allowing Recipient to complete the Project, and Recipient shall not use the Confidential Information for any other purpose. Recipient agrees it will hold the Confidential Information in strict confidence and (a) shall not misappropriate or mishandle the Confidential Information, or otherwise disseminate, divulge, or disclose, or cause, assist, or allow any other party to disseminate, divulge, or disclose, all or part of the Confidential Information to any third party, other than Recipient's third party professionals also bound by a duty of confidentiality at least as comprehensive as that contained in this Agreement ("Authorized Individuals"), and (b) shall not take any other steps to prevent or circumvent the broad goals and intentions of this Agreement. If Recipient finds it necessary to disseminate the Confidential Information to Authorized Individuals, it shall inform them of the confidential nature of the Confidential Information, and Recipient shall be responsible for any and all damages caused to Discloser if said Authorized Individuals do not abide by this Agreement. Recipient agrees irreparable damage may result from a breach of this Agreement, and that a breach may be remedied by specific performance, immediate injunction, and any other remedies allowed by law. Within ten (10) days of Discloser's request, Recipient shall return all Confidential Information to Discloser, and will not retain any copies thereof. Confidential Information shall not include any information which Recipient can establish (a) was publicly known and made generally available in the public domain prior to the time of disclosure to Recipient, (b) becomes publicly known and made generally available after disclosure to Recipient by Discloser through no action or inaction of Recipient, or (c) is in the possession of Recipient, without confidentiality restrictions, at the time of disclosure by Discloser as shown by Recipient's files and records prior to disclosure. Notwithstanding anything herein to the contrary, Recipient may disclose Confidential Information to the extent necessary to comply with any law, regulation, or court order; provided Recipient must promptly notify Discloser of such proposed disclosure or delivery prior thereto. In addition, Recipient shall, if requested by Discloser, use its best efforts to lawfully cooperate

with Discloser to seek a protective order or other appropriate remedy to prevent the disclosure of Confidential Information.

Section 3. Miscellaneous. This Agreement may be executed in multiple counterparts which, when read together, shall constitute and comprise a single document. Facsimile signatures hereto shall be as enforceable and binding as manual signatures hereto. This Agreement shall be governed by the laws of the State of Arkansas, and all disputes that might arise hereunder shall be adjudicated exclusively in Pulaski County, Arkansas. This Agreement may only be modified or amended by a written document executed by and between the Parties. This Agreement constitutes the entire agreement and understanding between the Parties relating to the subject matter contained herein, and supersedes any prior or contemporaneous terms, representations, statements, or agreements, whether made orally or in writing, with respect to the subject matter contained herein. Each party executing this Agreement covenants that he/she has the power to enter into this Agreement and bind his/her principal, if any, thereto. Each provision of this Agreement is severable and to the extent any provision is deemed invalid or unenforceable, such invalidity or unenforceability shall not affect the validity or enforceability of the remaining provisions of the Agreement. Parties are independent contractors, and this Agreement is neither intended to, nor shall it be construed as, creating a joint venture, partnership, agency, employment relationship, or any other relationship that may result in vicarious liability. Nothing in this Agreement shall obligate the Parties to enter into any further agreements with one another. A Party may not assign this Agreement in whole or in part without the prior written consent of the other Party.

IN WITNESS WHEREOF, the Parties execute this Agreement as of the Effective Date.

HEIFER PROJECT INTERNATIONAL	_____ (COMPANY)
Signature: _____	Signature: _____
Name/Title: _____	Name/Title: _____
Date: _____	Date: _____

XIII. APPENDIX B: Intent to Bid

Intent to Bid

____ / ____ / ____
(Date)

It is _____ intention to submit information to Heifer Project International, Inc. in its search for Audit Engagement - SOC for Cybersecurity. We have received Heifer International, Inc. request for proposal and agree to its terms, conditions and schedule of events.

We will submit our RFP response no later than **2:00 P.M. CDT January 16, 2020**

_____ ____ / ____ / ____
(Signature of Authorized Representative) ***(Date)***

Vendor's Official Representative _____
Print

Address:

_____

_____

Phone Number: _____

Email Address: _____
Print

XIV. APPENDIX C: Reference Form

References

A list of at least three (3) references from Not-for-Profit organizations, state agencies, municipalities, and publicly traded or privately held corporations willing to discuss with HPI the Vendor's performance in providing services comparable to the services being sought by HPI. Utilize the table provided for each reference. Each reference must include the agency name and address; the name, title, and phone number of the contact person at the agency/company; the time period during which the services were provided; the name of the Vendor's lead project manager on the engagement; and a brief summary of the services provided.

REFERENCES			
Client Name **Contact Name/Title** **Company Address**			
Phone		**Email**	
Project Start Date		**Project End Date**	
Services Provided			
Contract Award Amount (USD) $			
What was the outcome of the project? Attach additional pages, as necessary.			