giz Office South Caucasus

German Development Cooperation

GIZ Office South Caucasus
Rustaveli Ave. 42 / Griboedov Str. 31a
0108 Tbilisi, Georgia
T +995 32 2201800
F +995 32 2201801

Your reference
Our reference

4 October 2019

კონკურსის გამოცხადება

პროექტის დასახელება: **გადასახადებისგან თავის არიდების წინააღმდეგ ბრძოლა ინფორმაციის ავტომატური გაცვლის პილოტირების გზით საქართველოში "**

პროექტის ნომერი: 15.2192.1-007.00

ძვირფასო ქალბატონებო და ბატონებო,

გერმანიის ფედერაციული რესპუბლიკის მთავრობის დავალებით შპს. გერმანიის საერთაშორისო თანამშრომლობის საზოგადოება (GIZ) საქმიანობას ეწევა გერმანია-საქართველოს განვითარების თანამშრომლობის სფეროში.

დაგეგმილი გვაქვს შევისყიდოთ **მომსახურება საქართველოში რეგისტრირებული კომპანიებისგან** დანართი 1 - ის შესაბამისად.

დაინტერესების შემთხვევაში, გთხოვთ, **17.10.2019 -ის 17:00 საათამდე** წარმოგვიდგინოთ თქვენი შემოთავაზება **<u>ამობეჭდილი</u>** სახით, 2 სხვადასხვა კონვერტში. 1 კონვერტში საფასო შემოთავაზება, ხოლო 2-ში - შინაარსობრივი შემოთავაზება.
გთხოვთ, შემოთავაზებები მოგვაწოდოთ **ქართულ** ან **ინგლისურ** ენაზე.

დაგვიანებული შემოთავაზებები არ განიხილება.

გთხოვთ, გაითვალისწინოთ, რომ 2013 წლის მაისიდან სსკ–ს 168-ე მუხლის მე–4 ნაწილის „ბ" ქვეპუნქტის თანახმად გერმანიის საერთაშორისო თანამშრომლობის საზოგადოება სარგებლობს გადასახადებისგან გათავისუფლებით (დღგ, აქციზი, იმპორტის გადასახადი) და შესაბამისად **ევროში** წარმოდგენილი ფასი არ უნდა შეიცავდეს მოცემულ გადასახადებს და ეს მითითებული უნდა იყოს შემოთავაზებაში.

Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Sitz der Gesellschaft Bonn und Eschborn

Friedrich-Ebert-Allee 36 + 40
53113 Bonn, Deutschland
T +49 228 44 60-0
F +49 228 44 60-17 66

Dag-Hammarskjöld-Weg 1 - 5
65760 Eschborn, Deutschland
T +49 61 96 79-0
F +49 61 96 79-11 15

E info@giz.de
I www.giz.de

Amtsgericht Bonn
Eintragungs-Nr. HRB 18384
Amtsgericht Frankfurt am Main
Eintragungs-Nr. HRB 12394

Vorsitzender des Aufsichtsrats
Staatssekretär Martin Jäger

Vorstand
Tanja Gönner (Vorstandssprecherin)
Dr. Christoph Beier (Stellv. Vorstandssprecher)
Thorsten Schäfer-Gümbel

გთხოვთ, კონვერტზე მიუთითოთ შემდეგი:

- სახელი, გვარი, ფირმის დასახელება;
- საკონტაქტო ინფორმაცია (ტელეფონი, საკონტაქტო პირი);
- ტენდერის დასახელება : **Information Security Management System (ISMS) Integration Support and Consultancy per ISO 27001 standard requirements for Revenue Service of Georgia (Stage 1) / ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) დანერგვის მხარდაჭერა და კონსულტაცია ISO 27001 საერთაშორისო სტანდარტის მოთხოვნების შესაბამისად შემოსავლების სამსახურისთვის (1-ლი ეტაპი)**
- წარწერა "კონფიდენციალურია";
- გთხოვთ, მოაწეროთ ხელი დალუქვის ადგილზე.

გთხოვთ, შემოთავაზება დაიტანოთ თქვენი ორგანიზაციის ლოგოიან თავფურცელზე, დასვათ ბეჭედი და ხელმოწერა.

აგრეთვე მიუთითოთ შემდეგი მისამართი:

GIZ-ის რეგიონალურ ბიუროს სამხრეთ კავკასიაში
რუსთაველის 42 / გრიბოედოვის 31ა
0108 თბილისი
მიუთითეთ პროგრამის ნომერი: 15.2192.1-007.00
და აგრეთვე ტენდერის ნომერი: 83337281

დანომრეთ კონვერტები: **(I - საფასო შემოთავაზება; II - შინაარსობრივი შემოთავაზება).**

შეკითხვების შემთხვევაში დაუკავშირდით ანა ჩხეიძეს
ელექტრონული ფოსტის მეშვეობით – anna.chkheidze@giz.de
შემოთავაზებების ჩაბარებამდე არაუგვიანეს **2 დღისა:**

წესების დარღვევის შემთხვევაში თქვენი შემოთავაზება არ იქნება განხილული.

შემოთავაზებების შეფასება სავარაუდოდ დამთავრდება 23.10.2019 -თვის.
დაკავშირება მოხდება მხოლოდ ტენდერში გამარჯვებულ კომპანიასთან

პატივისცემით,

ანა ჩხეიძე
ხელშეკრულებების განყოფილება

<u>დანართი</u>

1. ტექნიკური დავალება
2. შემოთავაზებების შეფასების ზოგადი სქემა
3. შემოთავაზებების შინაარსობრივი შეფასების სქემა

დანართი 1 - ტექნიკური დავალება

Information security management system GAP analysis and assessment

1. Brief information on the project

Project: "Eastern Partnership Regional Fund for Public Administration Reform" Sub-project: "**Combating tax evasion through piloting the automatic exchange of information (AEOI) in Georgia**"
PN: 2015.2192.1-007 (thereafter referred as GIZ project)

This sub-project, within the scope of German Cooperation, is implemented GIZ "Eastern Partnership Regional Fund for Public Administration Reform" (https://www.giz.de/en/worldwide/57219.html) with a special role over the contents of the project by the Federal Ministry of Finance (Germany) BMF and Federal Central Tax Office (BZSt).

The project was launched in November 2017 and its duration is until 09/2020. BMF and GRS are actively involved in planning of the specific activities which will lead to the main objective of this project - having implemented AEOI/CRS[1] in Georgia and exchanging actual data with other countries.

Main partner from Georgian side is Georgia Revenue Service (GRS). Other important stakeholders are OECD Global Forum, Ministry of Finance of Georgia and National Bank of Georgia.

2. Context

A new OECD Global Forum standard on Automatic Exchange of Information (AEOI or CRS) aimed at reducing the possibilities for tax evasions. It encompasses the process of exchanging financial data, for tax purposes, between the jurisdictions on systematic and uniform/standardised basis.

Confidentiality, data safeguards and proper use of the information is a critical pre-condition for the AEOI implementation. Therefore, at GRS, as a potential administrator/competent authority receiving and sending the data should fully meet OECD Global Forum standards on

[1] CRS - Common Reporting Standard. OECD Global Forum Standard on Automatic Exchange of Information

data safeguards and confidentiality. GRS has to implement information security management system entity-wide, in order to comply with the standards.

At the moment GRS applies a significant number of security controls in order to mitigate the threat of taxpayer data being misused. These controls are applied across all of the main security control 'domains' that are most relevant for a tax administration. However, at the same time there are some specific areas of weakness that need to be addressed. As a first step, before actual exchange of the data takes place Georgia, has to develop and follow an action plan on ensuring confidentiality and data protection. Among other important milestones of the abovementioned action plan, GRS has started working on information security framework and an information security policy, that is being the very first strategic IT security document to be prepared and approved shortly. As a next step, GRS, with full support from its top management, is going to implement information security management system as per ISO 27001 standard. Important part of this process is preparation and conducting stage IT security audit stage 1.

The focus of this ToR is work description and requirements for the contractor to perform stage 1/initial audit as per ISO 27001.

3. GIZ shall hire the contractor (consultant) from 20/10/19 until 20/09/20

4. The contractor (consultant) shall provide the following work:

4.1 The contractor is expected to conduct 'Stage 1 Audit' as per ISO 27001 standard.

4.2 The contractor shall review existing scope, information systems and provide a report listing all actions and documents required to meet the letter and spirit of the ISO 27001 standard.

4.3 The contractor shall actively assist organization in implementing information security management system (ISMS) in accordance with ISO 27001 and industry best practices.

4.4 The contractor shall assist company staff in carrying out an information security risk assessment for major assets and/or business processes.

4.5 The contractor shall review existing controls and help to map controls as per Annex A of ISO 27001

4.6 The contractor shall actively participate in all related activities that will prepare the company for the Stage 2 of the ISO 27001 audit and certification. During this stage the contractor shall review the effectiveness of organization's information security management system and validate if it meets all requirements of ISO 27001 standard, consequently recommending the company for the certification.

4.7 Working languages should be Georgian and English, final report should be prepared in English.

5. Deliverables and records

5.1 Scope of the ISMS (clause 4.3)

5.2 Information security policy and objectives (clauses 5.2 and 6.2)

5.3 Risk assessment and risk treatment methodology (clause 6.1.2)
5.4 Statement of Applicability (clause 6.1.3 d)
5.5 Risk treatment plan (clauses 6.1.3 e and 6.2)
5.6 Risk assessment report (clause 8.2)
5.7 Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)
5.8 Inventory of assets (clause A.8.1.1)
5.9 Acceptable use of assets (clause A.8.1.3)
5.10 Access control policy (clause A.9.1.1)
5.11 Operating procedures for IT management (clause A.12.1.1)
5.12 Secure system engineering principles (clause A.14.2.5)
5.13 Supplier security policy (clause A.15.1.1)
5.14 Incident management procedure (clause A.16.1.5)
5.15 Business continuity procedures (clause A.17.1.2)
5.16 Statutory, regulatory, and contractual requirements (clause A.18.1.1)

Records/logs to be created during the assignment:

5.17 Statutory, regulatory, and contractual requirements (clause A.18.1.1)

5.18 Records of training, skills, experience and qualifications (clause 7.2)

5.19 Monitoring and measurement results (clause 9.1)

5.20 Internal audit program (clause 9.2)

5.21 Results of internal audits (clause 9.2)

5.22 Results of the management review (clause 9.3)

5.23 Results of corrective actions (clause 10.1)

5.24 Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)

6. Required experience of the contractor:

The contractor (consultant) shall have:

6.1 Demonstrated experience in information security management system (ISMS) implementation.

6.2 Deep knowledge about ISO 27001, information security and industry best practices.

6.3 Experience as a consultant implementing ISO 27001 standard is a must.

6.4 Experience in participating in a minimum four-five ISO 27001 implementation projects at a state or private organization.

6.5 Relevant certification in the field (CISA, CISM, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, etc).

დანართი 2 - შემოთავაზებების შეფასების ზოგადი სქემა

შემოსული შემოთავაზებების შეფასება მოხდება როგორც ფასების, ასევე შინაარსის მიხედვით.
შინაარსობრივი შეფასების შემდეგ გაიხსნება და განიხილება წარმომდგენი ფირმების საფასო შემოთავაზებები. საფასო შეთავაზება მკაფიოდ და დეტალურად უნდა აღწერდეს ყველა სახის ხარჯს, რომელიც ამ ტექნიკური დავალების მიხედვით გათვალისწინებული სამუშაოების განხორციელებისთვის უნდა იქნას გაწეული.

საბოლოო შეფასებაში **შინაარსობრივი/საგნობრივი შეფასება შევა 70%-ით** და **ფასი/ღირებულება 30%** -ით.

მიღებული შედეგების მიხედვით პრეტენდენტებს პროგრამულად მიენიჭებათ რიგობრივი ნომერი. საუკეთესო მაჩვენებლის მქონე პირთან დაიწყება მოლაპარაკებები ხელშეკრულების გაფორმების თაობაზე. თუ მოლაპარაკებები არ დამთავრდა წარმატებით, მაშინ მოლაპარაკებები განახლდება რიგით მეორე კანდიდატთან.

დანართი 3 - შემოთავაზებების შინაარსობრივი/საგნობრივი შეფასების სქემა

შემოთავაზების შინაარსობრივი ნაწილი უნდა მოიცავდეს თანდართულ ტექნიკურ დავალებაში მითითებულ ინფორმაციას. წარმოდგენილ უნდა იქნას შემდეგი დოკუმენტაცია:

- ინფორმაცია ორგანიზაციის და მისი საქმიანობის შესახებ
- სხვა მსგავსი / მსგავსი პროექტები, რომლებიც კომპანიამ / პირმა წარსულში განახორციელა
- ექსპერტების CV , რომლებიც იმუშავებენ აღნიშნული პროექტზე
- დროში გაწერილი დავალებების შესრულების გეგმა გეგმა (მაგალითისთვის შეგიძლიათ იხელმძღვანელოთ ქვემოთ მოცემული სქემით)

Planning • Scoping • Context development • Policy document development • Asset Inventory • Risk assessment • Risk treatment plan development	**Implementation of Controls (Annex A of ISO 27001)** • Controls implementation plan development • Appropriate policy and procedures development
Internal Audit • Internal Audit Plan and procedure development • Internal Audit • Improvement plan development • Management review	**Pre-Audit/Certification Audit** • Support and consultancy in Audit planning • Improvement Plan development

არასაფასო კრიტერიუმები თავის მხრივ დაიყოფა წინასწარ განსაზღვრული შეწონვის კოეფიციენტების მიხედვით. **იხილეთ თანდართული ფაილი (Annex 3).**