A picture containing logo

Description automatically generated

**FINCA Bank Georgia, JSC**

**REQUEST FOR PROPOSAL**

**CYBERSECURITY AUDIT**

**2020**

**INTRODUCTION**

FINCA Bank Georgia is part of the FINCA Impact Finance Network, a group of 20 microfinance and financial institutions that provides socially responsible financial services and enables low-income entrepreneurs and small business owners to invest in the future. FINCA launched its operations in Georgia back in 1998, operating as a microfinance institution till 6 August, 2013. On 6 August 2013 institution received its banking license from the National Bank of Georgia.

Being a part of Global network of financial institutions, a group comprised of shareholders such as FINCA International, USA,  International Financial Corporation (IFC, World Bank Group)- USA, KfW Bankengruppe, the German development bank, FMO, the Netherlands development bank, and Triple Jump, a Netherlands-based microfinance investment manager, FINCA Bank Georgia is a bank with strong corporate governance, and expertise in financial services management.

FINCA Bank Georgia has played an important role in establishing and developing credit culture in the country – being a pioneer of microfinance for over 20 years FINCA Bank Georgia has been providing responsible financial services to entrepreneurs in all regions of Georgia. With more than 20 years of experience in the Georgian financial services sector and having impacted lives of tens of thousands of Georgian families, FINCA Bank Georgia strives for excellence and uniqueness to generate greater value to its more than 100 000 customer base.

**FINCA Bank Georgia intends to conduct a cybersecurity audit based on the Regulation of the National Bank of Georgia on the ‘Cybersecurity Management Framework of Commercial Banks’ Approved by Decree N56/04 of March 22, 2019 to evaluate cybersecurity controls.**

FINCA Bank Georgia invites Sealed Tenders for conducting Cybersecurity Audit from the firms/companies, who have prior experience of handling Cybersecurity Audit engagements

**AUDIT OBJECTIVES**

1. Provide management with an assessment of their cybersecurity policies and procedures and their operating effectiveness.
2. Identify security control concerns that could affect the reliability, accuracy and security of the enterprise data due to weaknesses in security controls.
3. Evaluate the effectiveness of response and recovery programs.

**THE ELIGIBILITY CRITERIA ARE AS UNDER:**

1. The vendor should have at least 3 years of experience in information security.
2. The vendor must provide the number and scope of cybersecurity audits conducted in the last year. The company must also provide at least one letter of recommendation on the successful completion of such an audit
3. The vendor must provide a list of certifications and the number of certified professionals on staff, as well as, resumes of employees who will conduct the cybersecurity audit in FINCA Bank Georgia
4. Audit team should have technical experience (verified technical qualification of audit team leader/team members in a form of CISA / CISSP certification would be considered as advantage).

**CYBERSECURITY AUDIT SCOPE**

**Cybersecurity audit must cover all requirements Regulation of the National Bank of Georgia on the ‘Cybersecurity Management Framework of Commercial Banks’ Approved by Decree N56/04 of March 22, 2019.**

Audit must cover risks associated with confidentiality, integrity and availability of systems. The scope of the audit must include all systems and assets of the Bank. The audit program should be based on the following five critical cybersecurity Functions:

|  |  |
| --- | --- |
| **Sub processes** | **Category** |
| **IDENTIFY - an organizational understanding to manage cybersecurity risk to systems, people, assets, data, processes and capabilities.** | **Asset Management** - The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy. |
| **Business Environment** - The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. |
| **Governance** - The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. |
| **Risk Assessment** - The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. |
| **PROTECT: appropriate safeguards to ensure delivery of critical services.** | **Access Control** - Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. |
| **Awareness and Training** - The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements |
| **Data Security** - Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. |
| **Information Protection Processes and Procedures** - Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. |
| **Maintenance** - Maintenance and repairs of information system components is performed consistent with policies and procedures. |
| **Protective Technology** - Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. |
| **DETECT: appropriate activities to identify the occurrence of a cybersecurity event.** | **Anomalies and Events** - Anomalous activity is detected and the potential impact of events is understood. |
| **Detection Processes** - Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. |
| **RESPOND: appropriate activities to take action regarding a detected cybersecurity incident.** | **Response Planning** - Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events |
| **Communications** - Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. |
| **Analysis** - Analysis is conducted to ensure adequate response and support recovery activities. |
| **Mitigation** - Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. |
| **Improvements** - Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. |
| **RECOVER: appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.** | **Recovery Planning** - Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents |
| **Improvements** - Recovery planning and processes are improved by incorporating lessons learned into future activities. |
| **Communications** - Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). |

More detailed scope will be provided to tender applicants through Email

**DELIVERABLES**

Cybersecurity Audit report should be in English and in Georgian languages. The report must include, but not limited to:

* Executive Summary
* Findings
* Risks analysis
* Recommendations
* Description of the methodology used
* Detailed description of the work done

The company must also make a presentation to the FINCA Bank Georgia about the identified deficiencies, risks and recommendations at the head office of the Bank.

**TIMING**

Audit should be conducted approximately within 3-4 weeks, Final report should be prepared no later 25 Dec 2020.

**CONTACT INFORMATION**

Contact information and submission of the bids

During the RFP process your contacts will be:

|  |  |  |  |
| --- | --- | --- | --- |
| **First Name** | **Last Name** | **Position** | **Email** |
| Natalia | Gochiashvili | Procurement Specialist | [Natalia.Gochiashvili@finca.ge](mailto:Natalia.Gochiashvili@finca.ge) |
| Giorgi | Dvali | Information Security Manager | [Giorgi.Dvali@finca.ge](mailto:Giorgi.Dvali@finca.ge) |
| Vladimer | Gordadze | Senior Auditor | [Vladimer.Gordadze@finca.ge](mailto:Vladimer.Gordadze@finca.ge) |

\*Please include all contacts when sending e-mails;

The bidder is free to provide any additional relevant information not covered by the RFP or an alternative proposal if he considers them more tailored to the client. Such items will be submitted as attachments to the proposal.

**The bids (in English) shall be received not later than November 6, 2020 via sealed envelope at HO of FINCA Bank Georgia at 71 Vazha Pshavela avenue, III Floor, office N12, 0186, Tbilisi, Georgia, during the working hours from 9:00 a.m. to 6:00 p.m.**

**PROPOSAL VALIDITY**

Tender Proposal must remain open and valid for consideration for a period of 2 (two) weeks from the date it was received by FINCA Bank Georgia.

Shortlisted Candidates will be invited for an interview.

**CONFLICT OF INTEREST**

JSC FINCA Bank Georgia operates in accordance with the highest ethical and professional standards and in accordance with the Bank's internal rules, the Bank employee and / or its related person may not have a direct or indirect financial interest in any of the Bank's counterparties (conflict of interest). In view of the above, there should be no conflict of interest between the company participating in the tender and the bank employee and / or their related parties.

**TENDER LANGUAGE**

The Proposal must be prepared in English. The documents obtained from the officials, can be in Georgian. Also, the questions and the answers can be in Georgian or bilingual.

**NOTE: FINCA Bank Georgia reserves the right to discontinue the Tender Process at any time with no financial compensation and makes no commitment that this process will result in a business transaction with one or more third parties.**