

TERMS OF REFERENCE

CYBERSECURITY CONSULTANT TO SUPPORT THE CENTRAL BANK OF SÃO TOMÉ AND PRÍNCIPE

1. Background

The Central Bank of São Tomé and Príncipe (BCSTP) is currently carrying out reforms to improve the country's financial infrastructure. Nonetheless, BCSTP payment systems are still underdeveloped and unreliable to support the growth and modernization of the economy. The country's limitations on payment infrastructure and access channels restrict access to payment services - particularly in rural areas and on the island of Príncipe - including the payment and collection of taxes, the payment of public service bills, salaries and pensions, and the disbursement of social benefits. Due to poor infrastructure reliability, BCSTP and bank employees spend considerable time manually resolving system errors, which discourages the use of bank cards and other electronic means in STP.

A critical aspect of the BCSTP Payments Oversight function is to ensure that evolving nature of technology is constantly monitored and meets the growing payment needs of the population, particularly the provision of digital payments. The existing payment infrastructure still has vulnerabilities since there is no central data center in STP and shared digital infrastructure and interoperability are non-existent, with individual servers and databases scattered across government ministries. Moreover, civil servants rely on public e-mail domains to conduct official government business, which can lead to considerable cybersecurity and data protection risks. While the BCSTP Oversight Unit is building its capacity to develop policies and procedures to ensure that the payments system is efficient, safe, fair and transparent, cybersecurity and data protection remain a concern since the technology and processes required to operationalize digital guardrails have yet to be implemented.

The Institutional Capacity Building Project, funded by the World Bank, is financing BCSTP's investments in new information technology systems, particularly a new core banking system, and is seeking a cybersecurity expert to assist the BCSTP in strengthening its cybersecurity framework. Any recommendations will take into consideration that operational and cybersecurity risks are identified and addressed by market participants and by the BCSTP in a timely manner.

2. Objective

The Consultant will assist the BCSTP in strengthening its cybersecurity framework.

3. Scope of the assignment

The Consultant shall:

- Assist the BCSTP in drafting a complete set of regulations for the financial industry to supplement the existing legal framework for cybersecurity;



- Provide support to the BCSTP in preparing a SWIFT compliant Plan to respond and monitor cybernetic attacks;
- Assess the existing security infrastructure and provide recommendations to update firewalls and introduce real-time monitoring
- Help organize and participate in meeting and information requests;
- Consult with relevant public and private sector stakeholders to better understand the context;
- Incorporate to the regulations feedback and comments from the technical team, public and private sector stakeholders, peer reviewing and others;
- Systematically capture global trends, practices and lessons learned;
- Provide comprehensive notes and analysis of mission meetings; and
- Assist in presentations of the regulations, if required;
- Design a training program to BCSTP staff on best cybersecurity practices in the financial sector, particularly those applied by Portuguese speaking countries.

4. Deliverables, Timeline, Payment

The Consultant will receive lump-sum payments upon completion of the following deliverables:

Deliverable	Date	Payment (%)
Draft regulations and SWIFT-compliant plan to respond and monitor cybernetic attacks	Month 1	50%
Final regulations (after incorporating comments) Final SWIFT-compliant plan to respond and monitor cybernetic attacks	Month 2	50%

The consultancy duration will be six months.

5. Reporting and location of the assignment

The Consultant will report to AFAP and the BCSTP. The Consultant will work remotely and is expected to carry out missions to São Tomé and Príncipe for discussions with stakeholders and to present documents. Mission travel will be decided in coordination with the BCSTP and AFAP. Mission costs are covered by AFAP. The documents to be sent to BCSTP and AFAP will be in Portuguese and English or French.

6. Required qualifications of Legal Expert

- Bachelor's degree in relevant areas such as IT, Law, Economics or Management with 12 years of relevant experience or equivalent combination of education and experience;
- Minimum of 5 years of experience in the provision of advice to governments and international financial organizations on the improvement of cybersecurity systems;
- Demonstrated knowledge of cybersecurity systems;
- Demonstrated experience in developing countries, particularly in Africa, in matters related

[Handwritten signature and official stamp of the Administration of Projects]

- to cybersecurity would be desirable;
- Fluency in Portuguese or French (written and spoken) are required.

7. Coordination and follow-up

The Consultant will work closely with the Information Security and Technology Innovation Department of the central bank.

