TC ABSTRACT

I. Basic Project Data

▪ Country/Region:	GUATEMALA/CID - Isthmus & DR
▪ TC Name:	Cyberattack Response and Cybersecurity Improvement at the Ministry of Public Finance of Guatemala
▪ TC Number:	GU-T1359
▪ Team Leader/Members:	NOWERSZTERN, ARIEL (IFD/ICS) Team Leader; PAZ GONZALEZ, SANTIAGO (IFD/ICS); RIVERA ARTEAGA, CESAR AUGUSTO (IFD/ICS); RESTREPO RESTREPO ANDRES DE JESUS (CID/CGU); FLORENCIA BAUDINO (IFD/ICS); MARTINEZ, YNTY KOYLLOR (IFD/ICS); CALDERON RAMIREZ, ANA CRISTINA (IFD/FMM); VILLAFUERTE MANZANO, ALBA CECILIA (CID/CID); SCHAEFFER CABRERA, MARIA JOSE (IFD/ICS); BARRAGAN CRESPO, ENRIQUE IGNACIO (LEG/SGO); LARRAZABAL, LUIS BERNAL (CID/CGU)
▪ Taxonomy:	Client Support
▪ Number and name of operation supported by the TC:	N/A
▪ Date of TC Abstract:	06 Feb 2024
▪ Beneficiary:	Ministry of Public Finance of Guatemala
▪ Executing Agency:	INTER-AMERICAN DEVELOPMENT BANK
▪ IDB funding requested:	US$400,000.00
▪ Local counterpart funding:	US$0.00
▪ Disbursement period:	30 months
▪ Types of consultants:	Individuals; Firms
▪ Prepared by Unit:	IFD/ICS - Innovation in Citizen Services Division
▪ Unit of Disbursement Responsibility:	IFD/ICS - Innovation in Citizen Services Division
▪ TC included in Country Strategy (y/n): ▪ TC included in CPD (y/n):	No No
▪ Alignment to the Update to the Institutional Strategy 2010-2020:	Institutional capacity and rule of law

II. Objective and Justification

2.1 The objective of this Technical Cooperation (TC) is to support the Ministry of Public Finance (MINFIN) of Guatemala in responding to cyberattacks and in strengthening its cybersecurity. The specific objectives of this TC are to provide technical assistance to the MINFIN in: (i) the technical response and analysis of recent cyberattacks, including the identification of potential evidence, its acquisition, forensic analysis, production and presentation of reports; (ii) strengthening MINFIN's cybersecurity through professional services and tools to analyze the current cybersecurity posture, protect and monitor systems, detect, respond and recover from cyber incidents.

2.2 The increasing use of ICT in LAC is a catalyst for economic and social progress; however, it introduces inherent cybersecurity risks which must be managed on a continued basis, else citizen safety and the public trust in ICT, including consumer faith in online transactions and access to digital public services, may be negatively affected. Thus, strengthening cybersecurity is essential to safeguard citizens' rights in the digital sphere, such as privacy and property, to promote citizens' trust in digital technologies, and to support economic growth through safe digital transformation. Citizens must be assured that the digital systems they use for their personal or

professional activities, as well as those that involve their personal data, possess adequate security measures to guarantee the integrity, confidentiality, and availability of their information and the services they depend on. In this context, being prepared, and knowing where we stand, is key. The Inter-American Development Bank (IDB) carries out assessments to capture the evolving capacities of its member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: "Risks, Progress and the Way Forward in Latin America and the Caribbean", developed in partnership with the Organization of American States (OAS), showed that countries were in varying stages of development in their preparedness to face cybersecurity challenges, but generally still had ample room for improvement. In the case of Guatemala, its maturity in cybersecurity public policy across 53 indicators was evaluated at less than 2.0 out of 5.0 points, on average. Specifically, Guatemala has approved a National Cybersecurity Strategy in 2018, however its objectives and action plan have not yet been fully realized. In 2019, Guatemala approved a Cybercrime Law. Guatemala does not have a national-level cybersecurity agency or a critical infrastructure protection plan. In this context, the government has limited capacity to prevent, detect and respond to cyberattacks. These underlying cybersecurity vulnerabilities occasionally result in high-profile cybersecurity attacks. In late November 2023, MINFIN announced it has suffered from a cyberattack, affecting the availability of some of its information and systems. Some of MINFIN's main information systems include SICOIN (Sistema de Contabilidad Integrada), used to manage government payments and accounts, GuateCompras, used to manage government purchases, and Guatenominas, used to manage government salaries. Needless to say, the reduced availability of such systems impacted the orderly realization of the government's financial processes, and the trust in their ongoing stability. The IDB has responded to cybersecurity challenges in LAC with a number of capacity building efforts, including loan operations and specific technical assistance.

III. Description of Activities and Outputs

3.1 **Component I: Cyberattack Response and Analysis (US$300,000).** This component will support the technical response, analysis and investigation of recently occurred cyberattacks.

3.2 **Component II: Strengthening MINFIN's Cybersecurity (US$100,000).** This Component will provide professional services and tools to analyze MINFIN's current cybersecurity posture, provide detailed diagnostics, recommendations, remediation and action plans and ongoing support to improve MINFIN's preventative capabilities.

IV. Budget

Indicative Budget

Activity/Component	IDB/Fund Funding	Counterpart Funding	Total Funding
Cyberattack Response and Analysis (US$300,000)	US$300,000.00	US$0.00	US$300,000.00
Strengthening MINFIN's Cybersecurity (US$100,000)	US$100,000.00	US$0.00	US$100,000.00
Total	**US$400,000.00**	**US$0.00**	**US$400,000.00**

V. Executing Agency and Execution Structure

5.1 This project will be executed directly by the Bank, through IFD/ICS, in coordination with the Guatemala country office and IFD/FMM.

5.2 IFD/ICS has extensive and recent experience in providing technical assistance to the public sector in LAC including in strengthening cybersecurity capabilities in organizations and with incident response and is therefore best equipped to manage this operation and to assure the coordination needed. The TC will be implemented over 30 months, with execution expected over a 24-month period. The IDB has responded to cybersecurity challenges in LAC with a number of capacity building efforts, including loan operations and specific technical assistance. In Guatemala, 5231/OC-GU,5232/KI-GU “Program for the Digital Transformation of Guatemala for Inclusive Access to Connectivity” (about to begin implementation) includes support for cybersecurity investment. Guatemala has also benefitted from regional capacity building activities such as the IDB-OAS regional cybersecurity maturity study, the IDB’s National Cybersecurity Leadership course, regional and subregional events and study courses dealing with cybercrime and cybersecurity such as for investigators, customs, prisons, among others. The IDB is in a unique position to support MINFIN’s cybersecurity capacity building, given our ongoing investment and technical assistance projects, and proven record leveraging technical support from the most advanced countries in cybersecurity worldwide. For example, the government of Israel has supported capacity in cybersecurity throughout Latin America since 2016 and is currently involved providing access for the region’s cybersecurity professionals to the most advanced training, knowledge, expertise and best practices worldwide (ATN/CF-15598-RG, ATN/CF-19154-RG). IDB is in a unique position to support MINFIN’s cybersecurity capacity building, given our ongoing investment and technical assistance projects, and proven record leveraging technical support from the most advanced countries in cybersecurity worldwide. For example, the government of Israel has supported capacity in cybersecurity throughout Latin America since 2016 and is currently involved providing access for the region’s cybersecurity professionals to the most advanced training, knowledge, expertise and best practices worldwide (ATN/CF-15598-RG, ATN/CF-19154-RG). The contexts of Japan, Korea and Spain also portend meaningful lessons and technical support in state capacity and the co-production of cybersecurity (ATN/JF-20080-TT, ATN/JF-19603-SU, ATN/KR-19795-RG, ATN/FG-16633-RG and ATN/FG-18691-RG).

VI. Project Risks and Issues

6.1 The main risk is linked to the unknown and variable scale of professional services required to achieve the project objectives, which would depend on the findings. To mitigate this risk, a modular phased contracting model would be adopted where work packages will be defined and approved gradually. There is also the risk to obtaining full access to the relevant information and systems to carry out the analysis and remediation. To mitigate it, the project will work closely with the managerial level and technical government counterparts to provide this assistance.

VII. Environmental and Social Aspects

7.1 This TC does not have applicable requirements of the Bank’s Environmental and Social Policy Framework (ESPF).