



USAID
FROM THE AMERICAN PEOPLE

USAID/GUINEA: INTERCONNECTION OF GOVERNMENT REVENUE AGENCIES IN GUINEA FINAL REPORT

JANUARY 2014

This document is made possible by the support of the American People through the United States Agency for International Development (USAID). The contents of this report were prepared by IBI International under contract number AID-675-TO-13-00001. The views expressed herein are the sole responsibility of IBI International and do not necessarily reflect the views of USAID or the United States Government.

USAID/GUINEA: INTERCONNECTION OF GOVERNMENT REVENUE AGENCIES IN GUINEA FINAL REPORT

JANUARY 2014

This document is made possible by the support of the American People through the United States Agency for International Development (USAID). The contents of this report were prepared by IBI International under contract number AID-675-TO-13-00001. The views expressed herein are the sole responsibility of IBI International and do not necessarily reflect the views of USAID or the United States Government.

TABLE OF CONTENTS

List of Acronyms and Abbreviations	iii
I. Introduction	1
II. Actions undertaken.....	3
Work plan	3
Deliverables.....	4
III. Observations.....	5
Documentation of Procedures.....	5
Means for Information Exchange	5
Status of the computerization	5
Information Security.....	5
Current interconnection between the General Directorate of Customs and the Central Bank of the Republic of Guinea.....	6
IV. Recommendations	7
Implement a Virtual Private Network, or "VPN".....	7
Software Aspects: Message Exchange System	7
Implement a Statistical Platform for Macroeconomic Analysis.....	7
Implement an Information Security Policy.....	7
Change Management.....	8
V. Provisional Planning.....	9
VI. Budget Estimates.....	11
VII. Overview of Proposed solutions	13
VIII. Conclusion.....	15
Appendix 1. List of Contacts.....	17
Appendix 2. Bibliography.....	21
Appendix 3. Organization for Implementation	23
Components of the Organization.....	23
Steering Committee.....	25
Technical Committee	25
Provisional Planning.....	25
Project Team	26

Appendix 4. Technical Specifications of an Information Exchange Environment.....	29
Technical Specifications of the Servers	38
Service Specifications	39
Budget Estimates.....	40
Appendix 5. Strategies for Establishing an Information Exchange Environment.....	41
Introduction	41
Incorporating the National Vision for E-government.....	41
Information Exchange Needs.....	42
Organizational Matters.....	43
Implementation of the Interconnection	43
Software— Message Exchange System.....	45
Implementation of a Statistical Platform for Economic Analysis	45
Information Security Issues	45
A few Examples in Africa	47
Appendix 6. Implementation of a Statistical Platform for Macroeconomic Analysis	49
Statistical Platform for Macroeconomic Analysis.....	49
Table of Information Flows	51

LIST OF ACRONYMS AND ABBREVIATIONS

ASYCUDAWorld	Automated System for Customs Data, World Version
ATN	Automatic Taxation Notifications
CAAT	Central Accounting Agency of the Treasury
CBRG	Central Bank of the Republic of Guinea
CCT	Central Collector of the Treasury
DGC	Directorate General of Customs
GRT	Guaranteed Restoration Time
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IMS	Integrated Monetary Situation
INANET	Inter-Administration Network
ISO	International Standards Organization
Java EE	Java Enterprise Edition
MFE	Ministry of Finance and the Economy
MSI	Maximum Service Interruption
NDIR	National Directorate of Internal Revenue
NDITS	National Directorate of IT Systems
NDTPA	National Directorate of the Treasury and Public Accounting
SLA	Service Level Agreement
SSTC	Special Series Treasury Check
UTM	Unified Threat Management
VAT	Value-Added Tax
VPN	Virtual Private Network

I. INTRODUCTION

The Republic of Guinea has requested assistance from USAID in order to improve the interconnection between the institutions involved in the management of the Treasury's current accounts. Assistance in designing the required system of interconnection was mobilized by USAID through a Public Financial Management task order contract with IBI International. The field team worked from October 19, 2013 through January 16, 2014, producing each of the contract deliverables and this final report. Translation and editing of both versions of the report continued through January 31.

The definition of an interconnection is a physical link and/or network organization, facilitating the exchange of information among different offices or organizations. The interconnection provides a means for each of the institutions involved to add real-time processing, accuracy of information, and simplification of procedures in their work processes. Therefore, the crux of the operation lies in the accurate definition of the information to be shared with others and of the expected information from other stakeholders. The technical aspects of the physical interconnection itself are rarely the problem, as there are numerous viable solutions/options.

This scope of work covered only the four key agencies involved in collecting and accounting for government revenues in Guinea:

- The National Directorate of Treasury and Public Accounting (Treasury)
- The Central Bank of the Republic of Guinea (Central Bank)
- The General Directorate of Customs (Customs)
- The National Directorate of Internal Revenue (Internal Revenue).

II. ACTIONS UNDERTAKEN

WORK PLAN

Only minor changes were made to the initial work plan, summarized in the table below. The black bullet points represent deliverables.

s		Oct			Nov				Dec			Jan	
Actions	Period covered: 12 weeks, from October 21, 2013 to January 16, 2014	1	2	3	4	5	6	7	8	9	10	11	12
		Action 1.1: On-location arrival of the IBI Team											
Action 1.2: First contact between USAID and stakeholders													
Action 1.3: Developing and submitting the work plan			◆										
Action 1.4: Starting the situation assessment													
Action 1.5: Clarifying the content of the interconnection and of the data exchanges for each stakeholder													
Action 1.6: Drafting the preliminary report on the situational assessment: flowcharts of current procedures					◆								
Action 1.7: Validating, with stakeholders, the situational assessment report including the flowcharts of current procedures						◆							
Action 2.1: Establishment of the Working Group													
Action 2.2: Validation of the situational assessment													
Action 2.3: Conceiving strategies for implementing an information exchange environment													
Action 2.4: Conceiving the technical specifications and implementation phases (costs, human resources, security)													
Action 2.5: Submission of the technical specifications and implementation phases (costs, human resources, security) to the Steering Committee													
Action 3.1: Submitting the preliminary version of the final report											◆		
Action 3.2: Submitting the final report containing the technical specifications and implementation phases (costs, human resources, security)											◆		
Action 3.3: PowerPoint presentation to the Steering Committee											◆		
Action 3.4: Submission of Final Report													◆

DELIVERABLES

Completing the initial commitments, the deliverables submitted are:

- situation assessment report
- PowerPoint presentation to the Steering Committee for the validation of this situational assessment report
- report inventorying information to be exchanged, with a focus on the recommendation that a statistical platform be established for macroeconomic analysis
- strategy document for establishing an environment of information exchange
- document presenting the architecture of the data system by asynchronous messaging
- document with the technical specifications and implementation phases (costs, human resources, security), budget estimates
- document presenting the general organization of the interconnection's implementation
- PowerPoint presentation to the Technical Committee on the recommendations, technical specifications, and implementation phases (costs, human resources, security), with budget estimates
- this final report

III. OBSERVATIONS

DOCUMENTATION OF PROCEDURES

The institutions covered by the proposed interconnection system generally do not have procedures manuals. The agents of these institutions know their different procedures well, but these procedures are rarely explicitly documented.

The team mapped existing and future processes through interviews with professionals in each structure to produce flowcharts for each.

MEANS FOR INFORMATION EXCHANGE

Many of these institutions' internal processes are currently computerized. However, apart from read-access made available to the DNTCP by the BCRG, all exchanges of information are in hard-copy. The result is that data often needs to be re-entered. This situation causes:

- arduous work and slow processing
- low productivity
- issues with the quality of the information in terms of reliability and security.

STATUS OF THE COMPUTERIZATION

The institutions covered by this study are at different levels of computerization.

The local networks of the Central Bank and Customs are of respectable dimensions given the duties of these two bodies. Reconfiguration and stabilization efforts are underway to improve their performance.

Internal Revenue has a local network, but all fields are not yet integrated into this network.

The Treasury is the least computerized structure, although it does have a connection allowing it to view Central Bank accounting.

The Treasury is the only structure with no information and communications technology (ICT) specialist.

INFORMATION SECURITY

The definition of information security used in this report is the ISO/IEC 27001: 2005 standard.

The ISO (International Standards Organization) and IEC (International Electrotechnical Commission) define information safety¹ as the protection of confidentiality, integrity, and availability of information. In addition, it specifies that other characteristics, such as authenticity, accountability, non-repudiation, and reliability, can also be included.

Confidentiality: characteristic of limiting access to specific information to authorized individuals, entities, and processes

Integrity: characteristic of protecting the accuracy and completeness of information assets

¹ http://www.iso.org/iso/fr/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103

Availability: characteristic of being accessible and usable on demand by an authorized entity.

The current situation on each of these criteria can be summarized as follows:

- Good protection of ICT equipment: accurate inventories of computer equipment are conducted and anti-virus policies are defined
- Doubtful reliability of computer systems: different networks and different resources on the networks suffer relatively long breakdowns, disrupting work
- Concerns about the confidentiality and integrity of processed information: currently, exchange of data in hardcopy and frequent data reentry compromise data integrity, resulting in accidental and intentional modifications, as well as creating opportunities for unauthorized access
- Lack of any formal information security policy: none of the covered institutions has an information security policy nor a "Director of Information Security." Information security is not coordinated by stakeholders with appropriate roles and functions
- No formal support for information security: managerial perspectives and past strategies do not show evidence of attention to information security.

CURRENT INTERCONNECTION BETWEEN THE GENERAL DIRECTORATE OF CUSTOMS AND THE CENTRAL BANK OF THE REPUBLIC OF GUINEA

With previous USAID support, an interconnection has been initiated between two of the organizations concerned, Customs and the Central Bank, and different commissioning tests have been completed.

This point-to-point connection by radio link is a temporary solution, chosen for quick implementation. It can become a backup system when the permanent fiber optic network proposed here is set up.

Data on the current link is initially exchanged through a shared table developed by Customs. Once a payment is made, the Central Bank updates this table with the appropriate information and shares it with Customs.

The long-term solution will facilitate the exchange of data by asynchronous messaging, as was suggested by earlier studies and further developed in this team's recommendations in the present report.

IV. RECOMMENDATIONS

IMPLEMENT A VIRTUAL PRIVATE NETWORK, OR "VPN"

As a first phase, the team recommends creating a Virtual Private Network (VPN), using the infrastructure of an existing internet service provider. An interconnection provided by a VPN using existing equipment of an Internet service provider, will allow one directorate's network to communicate with another directorate's network.

SOFTWARE ASPECTS: MESSAGE EXCHANGE SYSTEM

The principle of exchanging data through asynchronous messaging allows specific applications to exchange data. At the level of each structure, the specific application (the core banking business management solution for the Central Bank for instance, or ASYCUDAWorld for Customs) is operated as usual. When a sender has data to send, an external module takes the data to be sent and formats it as a message, which it then sends to the "mail server," also called provider or broker. An external module at the recipient's location connects to the "mail server" and removes the message; it pulls the information into a format supported by the specific local application and transfers it to the recipient.

This architecture brings together:

- a message processing module: packing the data as a message and unpacking the messages in order to retrieve the data. This module is specific for each site
- a "mail server" for the distribution of messages: it is an intermediary that stores messages as well as routes and redirects them to their recipients.

IMPLEMENT A STATISTICAL PLATFORM FOR MACROECONOMIC ANALYSIS

One of the advantages of interconnection is that it can facilitate better economic analysis. The institutions involved in the interconnection produce, distribute and use a lot of economic data. Since it passes through the implemented interconnection, this data provides an opportunity to build an exceptional statistical platform that can be used for the purpose of economic analysis. The goal is to have access to quality data to better manage and monitor development results.

This platform may become the provider for other national knowledge management systems and become the basis for an integrated system of macroeconomic analysis.

IMPLEMENT AN INFORMATION SECURITY POLICY

The deficiencies found in information security will be corrected by:

- developing safety objectives within the various directorates
- getting the primary leaders of these directorates to take ownership of security objectives and implement them effectively
- fine-tuning the current situation analysis to specify the organizational responsibilities and measures to be implemented
- drafting a national data security policy

- drafting procedures for the security policy
- establishing an action plan to implement the security policy
- creating security-monitoring dashboards
- producing guidelines for good use of computer resources
- raising awareness and training users
- implementing and enforcing the measures identified.

More than all the other recommendations, implementing information security policy requires leadership by the heads of relevant directorates and agencies.

CHANGE MANAGEMENT

Given that the implementing the interconnection will involve structural and procedural changes in each organization, these changes must be modeled and evaluated. Although no major upheaval is expected, there will be notable changes in the organization of the involved institutions. Change processes rarely proceed without encountering some resistance. Therefore, they must be carried out in a cautious, participatory manner and carefully thought through. The elements that will be covered are, for example:

- defining the new procedures
- developing data exchange modules
- implementing the data exchange modules
- evaluating the performance of the new procedures
- updating and improving procedures
- producing the required specifications for the next phase of integrated systems.

V. PROVISIONAL PLANNING

Month Actions	01	02	03	04	05	06	07	08	09	10	11	12
Implementation of the VPN												
Change management												
Implementation of an information security policy												
Development of the exchange system by messaging												
Implementation of a statistical platform for the purpose of economic analysis												

VI. BUDGET ESTIMATES

Topics	Quantities	Unit price	Total
		US dollars	US dollars
VPN			
Firewall UTM (1 per site and 1 backup)	5	10 000	50 000
Monthly subscription fee (12 months for all four sites)	48	2 000	96 000
Servers			
Development	2	20 000	40 000
Production	2	20 000	40 000
Data warehouse	2	20 000	40 000
Statistical platform	2	20 000	40 000
Backup	2	20 000	40 000
Study trips to learn from the experience of countries such as Liberia, Ghana, or Rwanda			
Airfare	10	2 500	25 000
Accommodation, per diem	70	300	21 000
Training activities			
Global package			100 000
Human resources			
Team Leader, E-Governance Expert, Information Security Specialist			
Fee	252	650	163 800
Airfare	2	2 500	5 000
Accommodation, per diem, transport, and telecommunications	365	600	219 000
Java Enterprise Edition Developer			
Fee	168	500	84 000
Airfare	2	2 500	5 000
Accommodation, per diem, transport, and telecommunications	240	600	144 000
Economist - Statistician			
Fee	168	600	100 800
Airfare	2	2 500	5 000
Accommodation, per diem, transport, and telecommunications	240	600	144 000
Database engineer			
Fee	168	500	84 000
Airfare	2	2 500	5 000
Accommodation, per diem, transport, and telecommunications	248	600	148 800
Backstopping support, logistical backup by a firm	12	15 000	180 000
Total			1 780 400

VII. OVERVIEW OF PROPOSED SOLUTIONS

Elements	Descriptions
What information will be exchanged in the interconnection?	At first, it is recommended that the information to be exchanged is that which is currently manually exchanged in hard-copy. The full list of relevant information is provided in the document called <i>“Implementation of a statistical platform for the purpose of economic analysis”</i>
How to find your way through a large amount of information?	Properties such as tax registration numbers, payment slip numbers, and payment order numbers are key elements that will be used to link data from different databases
How to ensure the reliability of these key elements?	The entities responsible for the allocation of these key numbers are able to address this concern
How the data will enter into the interconnection?	<p>Exchange scenario between the Central Bank and Customs</p> <ul style="list-style-type: none"> -an economic operator pays import tax at a Central Bank counter -the information is recorded in the Central Bank system -on the basis of the Customs account number, the Central Bank computer system activates the sending of the information to Customs -the Central Bank computer system sends all the information (payment slip, tax registration number, amount paid, etc.) to the interface module that handles the messages -this interface module (at the Central Bank) constructs a message for Customs and deposits it with the mail server -the next time that the similar Customs interface module connects to the mail server, it retrieves this message -the Customs interface module translates the received message in a format that is usable by Customs’ computer system and transfers it to the latter -once the message is retrieved by the interface module of the recipient, this message is sent to the statistical platform which acts as a data storage center -the message is deleted from the mail server
How many interface modules will there be then?	<p>There will be as many interface modules as entities participating in the interconnection.</p> <p>Each interface module will need to develop messages in the direction of all the other partners depending on their needs.</p> <p>Also, each module will have to interpret messages received from all partners and make the information available on its own computer system</p>
Who is responsible for sending the data?	<p>Each partnering entity is responsible for the data it exchanges with the others, respecting legal and administrative requirements and the needs of others.</p> <p>Therefore, each body has a major responsibility for the development and maintenance of the interface module</p>
At what level of detail will data be transmitted?	The exchanged data will have to be dispatched in its full detailed original format. It is up to each body to select and aggregate data it receives to suit its needs

Elements	Descriptions
How will the development of the interface module proceed?	<p>External expertise in Java Development will be required to implement the system. The internationally recruited experts will set up local teams based on available expertise in the various bodies, and will conduct major training and skills-transfer activities. Only then will the development of the interface module start. This approach ensures that local capacity is built from the start to enhance system sustainability.</p> <p>The interface module is a fundamental element of any interconnection. It should be designed with maximum strength in terms of information quality, and the flexibility to build new message types.</p>
How will the interface module function, who will operate it?	<p>The interface module will be an independent and automatic process on a specific machine. No human intervention will be necessary for daily operation. The module will receive data from the entities' applications and will send it to the mail server. It will also automatically retrieve messages from the mail server and send data to the applications of its entity</p>
What about entities that use multiple applications?	<p>An interface module can serve multiple applications, receive data from these applications in order to make messages, process messages, and send the data they contain to these applications</p>
How will exchanged data be saved?	<p>The data is temporarily stored on the mail server until the recipient modules recover them</p> <p>The data is then stored on the statistical platform which serves as data storage center</p> <p>The data will be then erased from the mail server</p> <p>The statistical platform will have an interface that presents the information to the user</p>
What economic analyses will be performed with the available data?	<p>In addition to providing a set of indicators, the presentation interface of the statistical platform will facilitate simple data retrieval and complex research and analyses, in compliance with the best practices for statistical platforms</p>
What information is relevant and why?	<p>All information which is currently manually held in hard-copy is relevant. Everyday use will surely produce more data, hence the need for flexible interface modules and available Java programming resources internally and throughout the interconnection</p>
What is the implementation road-map of this interconnection?	<p>Implement the VPN</p> <p>Develop the interface modules</p> <p>Conduct training and measure skills-transfer</p> <p>Install the mail server</p> <p>Install the modules</p> <p>Implement the statistical platform</p> <p>Manage the various necessary changes</p> <p>Implement an information security policy</p> <p>The documents produced have indicated a schedule for implementation over time, the human resources profiles that will have to contribute, the technical specifications of all the components, and an estimated budget.</p>

VIII. CONCLUSION

The interconnection between the institutions responsible for the Guinean public revenues sector stems from a desire to improve the administration's performance. Implementing this project will constitute an important step towards establishing a performance-based and results-oriented culture in public service. This achievement will also contribute, in conjunction with the national e-government strategy, to establishing a modern data exchange framework, to improve the efficiency and transparency of the public sector.

APPENDIX I. LIST OF CONTACTS

N	Last Name and First Name	Occupation/Function	Address
1.	Steven Brown	Economist/M&E Specialist USAID/Guinea & Sierra Leone	American Embassy B.P. 603, Conakry, Guinea
2.	Almany Boubakar Bah	USAID/Guinea Financial Analyst	American Embassy B.P. 603, Conakry, Guinea
3.	Mrs. Mayaki Mariama Barry	Chief Executive Officer	Treasury
4.	Dr. Mamadi Diané	Deputy National Director	Treasury
5.	Mr Ousmane Bah	Division Manager, Regulations Division	Treasury
6.	Mr. Thomas Macauley	Division Manager, CCCD	Treasury
7.	Mr. Ismaël Sangaré	Paymaster General of the Treasury	Treasury
8.	Mr Yagouba Cissé	Central Accountant Agent of the Treasury	Treasury
9.	Mr. Fodé Oussou Diané	Treasury Services Inspector	Treasury
10.	Mrs. Fanta Keita	Section Manager, CAAT Accounting	Treasury
11.	Mr. Mourana Soumah	Manager of Central Deposit Accounting Agency	Treasury
12.	Mr. Hassane Camara	Section Manager, Management Accounts, Regulations	Treasury
13.	Mr. Thierno Ibrahima Barry	CAAT Assistant	Treasury
14.	Colonel Toumany Sangaré	General Director	Customs
15.	Lt Col Oubou Zézé Guilavogui	Customs Inspector - Deputy General Director	Customs
16.	Lt Colonel Camara Moussa	Director/Informatics and Statistical Directorate	Customs
17.	Lt Col Bah Ibrahim Izi	Customs Inspector - Service Manager, Tariff, Value, and International Relations	Customs
18.	Captain Mory Diané	Customs Inspector - IT Specialist - Network Administrator	Customs - IT & Statistics Directorate

N	Last Name and First Name	Occupation/Function	Address
19.	Abdoulaye Yéro Balde	First Vice-Governor	Central Bank
20.	Sekou Ahmed Soumah	General Director Director of Information and Telecommunications Systems	Central Bank Information and Telecommunications Systems Directorate
21.	Kindy Sylla Baldé	Service Manager, Studies and Development	Central Bank Information and Telecommunications Systems Directorate
26.	Malick S. Sawadogo	GTMFP Secretariat	Ministry of Finance and the Economy
31.	Monemou Ouou Ouou Waita Balao	General Director of Internal Revenue	Internal Revenue
32.	Youssef Camara	Service Manager, Large Business	Internal Revenue - Large Business Office
33.	Abdoul Rahamane Kandé	Service Manager, Computers - IT Engineer	Internal Revenue
35.	Bah Amadou Oury	General Inspector of Fiscal Services	Internal Revenue
36.	Severin Monemou	Division Manager, VAT Credits Collection	Internal Revenue - Large Business Office
37.	Ibrahima Kalil Diané	National Director	National Directorate of IT Systems
38.	Fidel Leno Tamba	Director/Jurist	Presidency of the Republic - General Secretariat of the Government - National Directorate of Governmental Work
39.	Antoine Haba	IT Specialist	Presidency of the Republic - General Secretariat of the Government - National Directorate of Governmental Work
42.	Georges Aimé Konaté	Assistant Director - Service Manager, Network and Telecommunications	Central Bank Information and Telecommunications Systems Directorate
43.	Thierry Samnyck	Executive Director	NEXYME Corporation Consultant for the master plans mission
44.	Lambert Tchuenteu	Country Manager - Republic of Guinea	NEXYME Corporation Consultant for the master plans mission
45.	Ibrahima Khan Diallo	Pre-Sales Engineer	SkyVision Conakry - Guinea
46.	Mamadou Diallo		National Directorate of IT Systems
47.	Oueret Ernest Guilavogui	Deputy National Director	National Directorate of IT Systems
48.	Mamadou Oury Sakho		National Directorate of Posts and Telecommunications Pan-African Interconnection

N	Last Name and First Name	Occupation/Function	Address
49.	Dr. Fodé Soumah	General Secretary	Ministry of Posts and Telecommunications and New Information Technologies
50.	Sékou Oresto Bangoura	Deputy National Director	National Directorate of Posts and Telecommunications
51.	Bernard LAFORGUE	Managing Director	Consultant of the EU mission for customs auditing
52.	Dr. M. Dian Diallo	National Coordinator	Ministry of Economy and Finances/Project Coordination and Implementation Unit (UCEP, <i>Unité de Coordination et d'Exécution des Projets</i>) PARCGEF/PAPEGM-BAD EGTACB/SFP – World Bank Targeted supports – PNUD/BAD

APPENDIX 2. BIBLIOGRAPHY

1. NATIONAL DIRECTORATE OF INTERNAL REVENUE "Guinea - General Tax Code. Edition Updated on June 1st, 2011 - Followed by the major Guinean tax legislation texts," Nimba Council, June 2011
2. REPUBLIC OF GUINEA "The financial and accounting information system. European Union - Enhancing the Management of Public Expenditure Project," International Monetary Fund, May 2012
3. MINISTRY OF FINANCE AND THE ECONOMY "Order A/2012/ /MEF containing the State Accounting Plan," 2012
4. PRESIDENCY OF THE REPUBLIC OF GUINEA/GOVERNMENT'S GENERAL SECRETARIAT "Joint order No/2011/6795/PRG/SGG establishing the Organic Framework of the National Directorate of Treasury and Public Accounting of the Ministry of Economy and Finances," November 2011
5. MINISTRY OF FINANCE AND THE ECONOMY "Order No 2011/6868/MEF/CAB containing the attributions and organization of the National Directorate of Treasury and Public Accounting," November 2011
6. MINISTRY OF FINANCE AND THE ECONOMY - NATIONAL DIRECTORATE OF PUBLIC TREASURY AND ACCOUNTING "Order 2011/071/MEF/DNTCP containing the accounting instruction (2011 year-end closing of accounts and balance recovery for 2012 management): Central Accountant Agent of the Treasury, Paymaster General of the Treasury, Central Collector of the Treasury, Special Collector of Internal Revenue, Special Collector of Customs, Regional Treasurers, Prefectorial Treasurers, Municipal Collectors, Accounting Agents, February 2012
7. NATIONAL DIRECTORATE OF PUBLIC TREASURY AND ACCOUNTING - NATIONAL DIRECTORATE OF BUDGET "Public Finance Dashboard," June 2012
8. PRESIDENCY OF THE REPUBLIC OF GUINEA "Decree D/2011/117/PRG/SGG of April 14, 2011 containing the attributions and organization of the Ministry of Economy and Finances," April 2011
9. PRESIDENCY OF THE REPUBLIC OF GUINEA "Decree D/2011/118/PRG/SGG containing the attributions and organization of the Delegated Ministry of Budget under the Ministry of Economy and Finances," February 2013
10. MINISTRY OF FINANCE AND THE ECONOMY - NATIONAL DIRECTORATE OF INTERNAL REVENUE, IT DIVISION "The project to overhaul the National Directorate of Internal Revenue's information system, granted to the ETI Company according to government contract no. 2009/329/329/1/6/3/1/G," November 2009
11. REPUBLIC OF GUINEA - EU/National Transition Council "Law L/2012/No 012/CNT containing Organic Law relating to the State Finance Law," IMF, August 2012

12. REPUBLIC OF GUINEA - CENTRAL BANK OF THE REPUBLIC OF GUINEA
"Memorandum on the BCRG's information system," February 2012
13. MINISTRY OF FINANCE AND THE ECONOMY - DELEGATED MINISTRY FOR THE BUDGET "Order A/8136/MEF/CAB/SGG containing the attributions and organization of the National Directorate of Internal Revenue," December 2011
14. SkyVision "Official receipt statement for the installation of the BCRG - DGD connection," October 2013
15. MINISTRY OF FINANCE AND THE ECONOMY, "Order 000668./MEFP/CAB/DND containing Procedures for the Management and Clearance of Goods in Computerized Offices," November 2007
16. USAID "Trip Report, Ministry of Finance and the Economy - National Directorate of Treasury and Public Accounting," Michael Ablowich, April 2013
17. PRESIDENCY OF THE REPUBLIC "Draft-Project of the National Strategy for the Development of IT Governance in the Administration," ANGEIE

APPENDIX 3. ORGANIZATION FOR IMPLEMENTATION

COMPONENTS OF THE ORGANIZATION

The elements necessary for the success of the interconnection each comprise several sub-components.

Implementation of the VPN

VPN implementation will proceed according to the following phases:

- Request for Proposals for the VPN
- Analysis
- Procurement
- Installation and configuration of the equipment
- Testing
- Beginning of VPN service

The work of the selected contractors will occur under the supervision of the Team Leader/E-Governance Expert, who will ensure compliance with all technical specifications. He will also ensure that adequate training is provided so that the technical teams of the interconnected institutions are able to fully manage the system (hardware and software).

Change management

Change management will be facilitated by the Team Leader/E-Governance Expert. He will work closely with the Directors of stakeholder institutions and assist in:

- Definition of new procedures
- Development of data exchange modules
- Implementation of the data exchange modules
- Evaluation of the new procedures
- Improvement of procedures
- Development of requirements for eventual integrated systems.

Information Security Policy Implementation

The Team Leader/E-Governance Expert will also be responsible for implementing an information security policy. He will work closely with the Directors of stakeholder institutions and assist in:

- Development of security objectives for the institutions
- Acquisition of approval from the Directorates, validating these objectives
- Analysis of the current state of affairs to identify what measures should be implemented

- Creation of a security policy
- Development of security policy procedures
- Creation of action plans necessary for the implementation of a security policy
- Creation of security-monitoring dashboards
- Production of guidelines for good use of IT resources
- Promulgation and user training.

Message exchange system development

A Java Enterprise Edition Developer will be involved in the development of the message exchange system by messaging. His involvement will be a combination of training, supervision of implementation, and Java application development. The objective is to ensure from the outset that the technical teams of the interconnected institutions fully master the entire software solution and can ensure its sustainability. This development process will produce:

- Technical records of message management modules, specific modules for each stage (Analysis, Design, Implementation, Testing, Deployment, Maintenance, Progress Measurement and Monitoring, Updating)
- Definitions of messages
- Implementation of a "mail server," a service provider managing the connections, sessions, destinations and messages.

The Team Leader/E-Governance Expert will ensure compliance with security standards throughout the process.

Statistical platform implementation

The implementation of the statistical platform will involve an Economist/Statistician and a Database Engineer. The implementation of the statistical platform must generate the following products:

- A directory of the basic data which is currently exchanged
- A directory of the data which is produced and/or collected by each of the interconnected institutions
- A directory of the basic data potentially available for exchange
- A collection of indicators, each with a description of its variables, how it is calculated, its history and any other useful information
- A list of necessary components for the open data portal
- The technical records of the open data portal (Analysis, Design, Implementation, Testing, Deployment, Maintenance, Progress Measurement and Monitoring, Updating)
- The open data portal, incorporating all basic data
- A list of necessary components for the statistical platform

- The technical records of the statistical platform (Analysis, Design, Implementation, Testing, Deployment, Maintenance, Progress Measurement and Monitoring, Updating)
- The statistical platform, incorporating all selected indicators.

The organization necessary for the implementation of such a project requires collaboration between a Steering Committee, a Technical Committee and a competent Project Team.

STEERING COMMITTEE

At the launch of the project, a Steering Committee, composed of the primary leaders of the stakeholder institutions, was established in order to ensure a strict project management in accordance with the established objectives. The members of the Steering Committee are decision makers who are capable of making the necessary decisions to drive the project (allocating resources, revising the scope of the project, changing deadlines, etc.).

TECHNICAL COMMITTEE

The Technical Committee's mission is to handle the technical complexity of all components of the project in terms of equipment, services, and module development. It also assists in the establishment of new organizations and working methods and in facilitating the exchange between structures.

The Technical Committee brings together ICT managers and the primary users of the exchanged data.

PROVISIONAL PLANNING

Month Actions	01	02	03	04	05	06	07	08	09	10	11	12
Implementation of the VPN												
Change management												
Implementation of an information security policy												
Development of a message exchange system												
Implementation of a statistical platform for economic analysis												

PROJECT TEAM

The Project Team will comprise the following positions:

- Team Leader/E-Governance Expert/Information Security Specialist (present throughout the entire 12-month duration of the project)
 - Engineer by training, solid experience (more than 10 years) as a consultant in e-governance, information and security systems
 - ICT Specialist - Project Manager
 - ICT project managing and evaluation, application auditing
 - Information system auditing
 - General technical knowledge of methods and techniques for analyzing problems related to information security and the information system
 - Proven experience in applying risk analysis methodologies to Information System Security
 - In-depth knowledge of standards, norms, and methods pertaining to Information System Security, including ISO 27001/27002/27005
 - Overall technical mastery of information systems
 - Strong writing skills
 - Ability to work independently to conduct missions.
- Java Enterprise Edition Developer (an initial 6-month mission and a second 2-month mission)
 - A minimum 3-year college degree in computer science
 - A minimum of 3 years of experience in the same job
 - Good working knowledge of Java, Spring, Oracle
 - Qualities:
 - *sense of customer service, compliance with client needs (deadlines, quality of delivered goods, etc.);*
 - *teamwork;*
 - *analysis, synthesis, and listening skills;*
 - *good initiative;*
 - *training ability.*
- Economist/Statistician (a first 6-month mission and a second 2-month mission)
 - A minimum 5-year college degree in statistics, econometrics, economy

- At least ten (10) years professional experience with relevant references in producing economic analyses
- Good initiative and the ability to perform analysis, synthesis, and writing tasks in French
- Database Engineer (an initial 6-month mission and a second 2-month mission)
 - Over 5 years experience in developing and administering Websites and Open Source software (Apache, MySQL, PostgreSQL, etc.)
 - Ability to apply the security rules for systems and networks to the development of the databases
 - Experience in the design and administration of high-availability architectures.

APPENDIX 4. TECHNICAL SPECIFICATIONS OF AN INFORMATION EXCHANGE ENVIRONMENT

After much deliberation, it was decided that it would be best to establish a connection using equipment already established by a third party, such as an Internet service provider. This requires creating a virtual private network (VPN). In a VPN, a directorate's network can communicate with another directorate's network using the pre-existing infrastructure from the Internet service provider.

The recommendations include four points:

- a virtual private network (VPN)
- software aspects: information exchange by messaging
- a statistical platform for economic analysis
- an information security policy

VPN TECHNICAL SPECIFICATIONS

Interconnecting the local networks of the Treasury, Internal Revenue, the Central Bank, and Customs enables these structures to electronically exchange data amongst themselves. The needs expressed and identified can be summarized as follows:

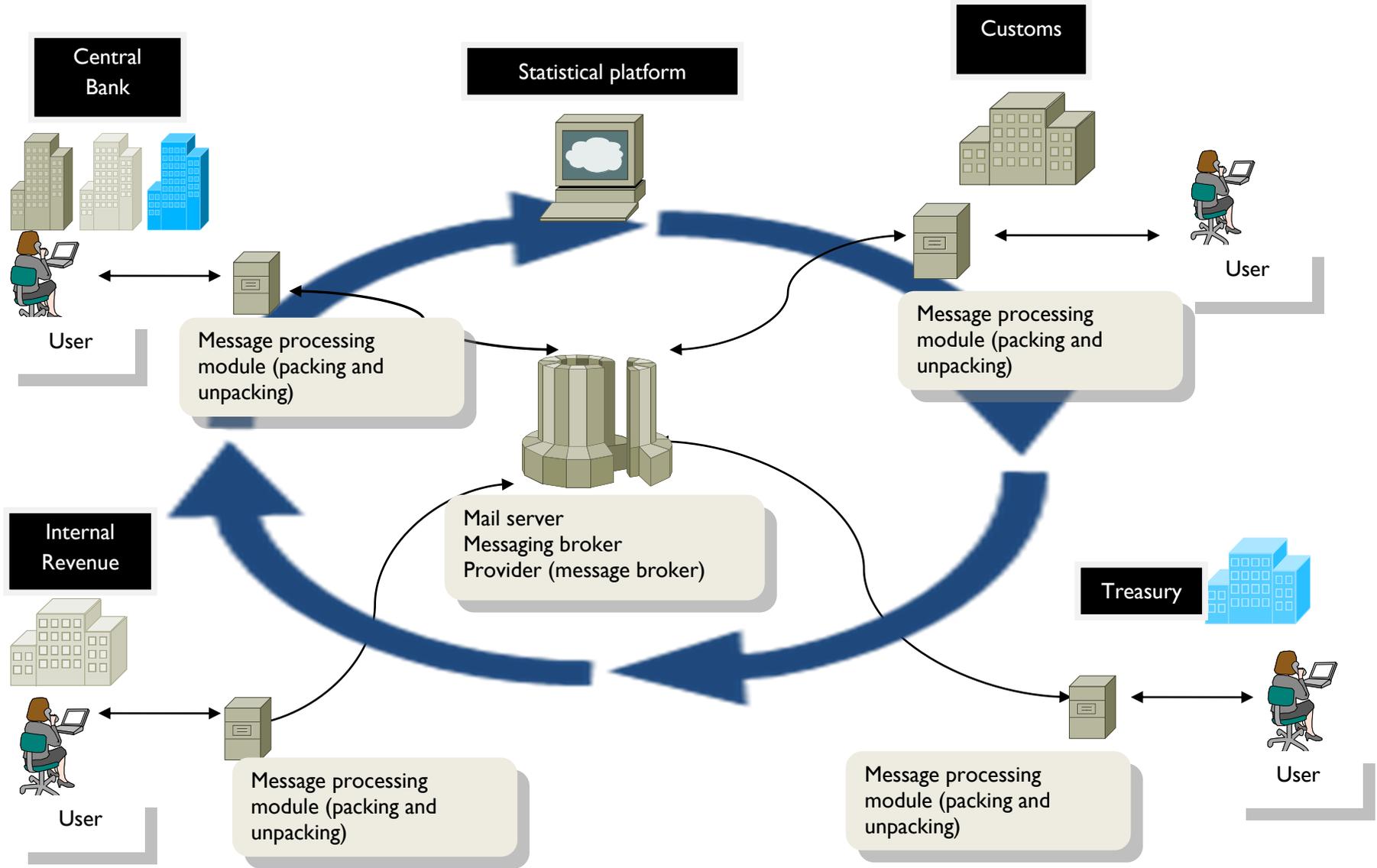
- The reduction of processing times
- Increased productivity
- Increased information reliability

To answer this list of needs, an interconnection is expected to achieve the following benefits:

- Instantaneous transactions
- The elimination of redundancy
- Lower paper costs (print, mail, envelopes, etc.)
- Greater data reliability
- Increased process automation
- Greater exchange security.

The hardware and software will have to be structured in a VPN (Virtual Private Network). The currently existing connection by radio link between Customs and the Central Bank will need to be integrated into this VPN. Each of these sites has an antenna with an auto injector, a CISCO 1941 router and a CISCO ASA 5510 firewall.

Planned software organization



Components of the general architecture

The general architecture, presented above, contains similar elements in each directorate. All of these directorates are in direct exchange with a common space, the message provider, or mail server.

The principle of exchanging data through asynchronous messaging allows specific applications to exchange data. For each institution, the specific application (the core banking business management solution for the Central Bank for instance, or ASYCUDA World for Customs) is operated as usual. When a sender has data to send, an external module takes the data to be sent and formats it as a message, which it then sends to the "mail server," also called the provider or broker. Another external module at the recipient's location connects to the "mail server" and retrieves the message; it converts the message into a format compatible with the local software before transferring it to the recipient.

This architecture includes:

- a message processing module: packing outgoing data as messages and unpacking incoming messages to retrieve data
- a "mail server" for the distribution of messages: it is an intermediary that stores messages and routes them to their recipients.

The "mail server" is the same for the entire network but the message processing modules are specific to each site. Indeed, at each site, this module is in charge of creating messages (on the basis of the content and recipients: for instance, determining what data from the Central Bank should be sent to Customs, to Internal Revenue, and to the Treasury) and correctly processing received messages.

Furthermore, the plan is to take advantage of this interconnection in order to build a statistical platform that will (i) provide quick access to reliable data, (ii) ensure electronic archiving of information, and (iii) create reliable and integrated databases, for ministerial departments and macroeconomic analysis services.

The implementation of a secure interconnection solution between the different institutions is mainly based on appropriate UTM (Unified Threat Management) appliances that will control the interfacing with the Internet access and manage exchanges between sites through VPN (Virtual Private Network) tunnels. Each site has at least two Internet access points.

A UTM appliance is a multi-function device for the protection of corporate information systems. It integrates security services (network firewalling, anti-spam, antivirus, URL filtering), routing functions (managing VLANs, dynamic routing) and service quality functions (bandwidth management, load balancing).

The solution to be acquired for this interconnection, in addition to the expected benefits of the interconnection itself, is expected to:

- secure Internet access against any intrusions or viruses
- control and protect web navigation
- protect the e-mail service from any kind of danger (spam, virus, etc.)

The solution must be designed around the following components:

- a firewall at each site, as an appliance integrating a powerful UTM engine, installed and configured for high availability
- a directory architecture within the Central Bank which will act as the central site, authenticating all processes and servers using the interconnection
- a virus protection solution for workstations and servers

The solution must be accompanied by all the relevant services:

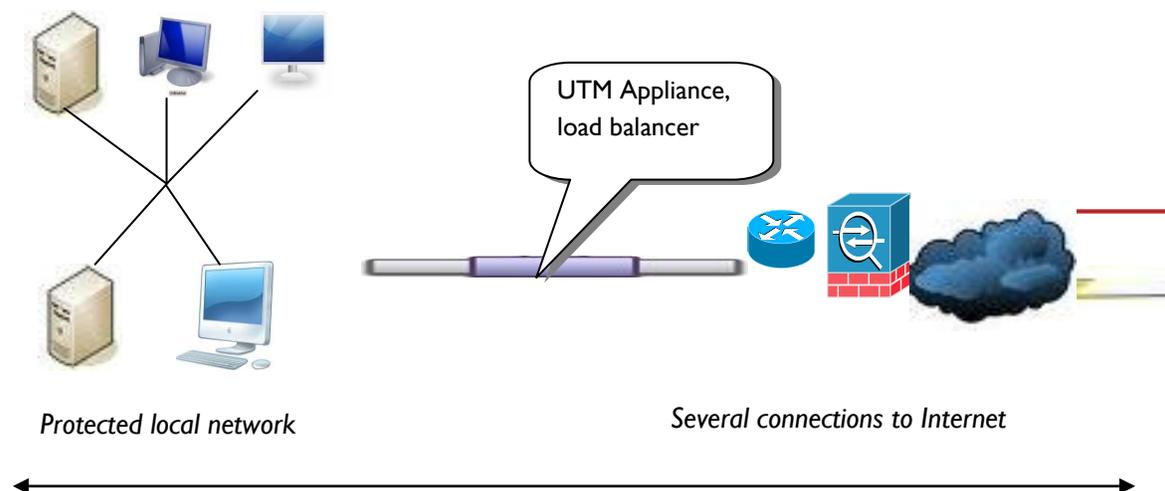
- engineering, installation, and implementation
- support and maintenance of suggested hardware and software components
- training the team to ensure system maintenance
- The processes and servers using the interconnection must authenticate and connect to the resources of the central site by secure IPSEC/SSL VPN tunnels.

VPN ARCHITECTURE AT EACH SITE

Architecture at each site

The planned security architecture must comply with the diagram below:

Each site shall have a firewall appliance to control all exchanges between the different sites. It must be installed for high availability.



Internet connections

Each site has at least two Internet access-points from different providers:

1. a main permanent and unlimited connection with a minimum downstream rate of 2 Mbps
2. a permanent and unlimited backup connection with a minimum downstream rate of 256 Kbps.

The upstream rate should be at least 256 Kbps, except for the central site at the CBRG which will have to have a minimum upstream rate of 2 Mbps.

Equipment for setting up the VPN

Firewall

To meet technical specifications, the firewall must:

- have a default blocking filter: anything that is not authorized is prohibited
- meet compliance with safety standards: FCC or CE and certified by ICESA, WestCoastLabs or equivalent
- have the ability to filter based on source address, destination address, user, service, protocol, input interface, time and date of access, etc.
- support the creation of firewall rules based on user identity in addition to other criteria: Source/Destination, IP/Subnet, Source/Destination port, etc.
- allow management of address ranges, IP groups (machines, networks, address ranges), user groups, service groups, etc.
- allow administrators to view and disable the implicit rules
- be able to enforce and associate antivirus/anti-spam, content or QoS filtering rules with firewall rules (ACL)
- be able to manage several intervention levels in the filtering policy depending on the specific permissions of each administrator
- be able to manage bandwidth by application
- support the BasedRouting Policy (routing based on all the criteria of a rule: IP source, IP destination, interface, protocol, input interface, application)
- contain a tool to test the consistency of the rules (to verify that there are no identical or conflicting rules in the policy)
- permit naming rules (to facilitate monitoring in the logs over long periods)
- integrate the intrusion prevention module (IPS)
- manage automatic security updates from the manufacturer for all functions (Full)

Network Configuration

To meet technical specifications, the network must:

- balance loads and manage backup for several operators by Source/Destination, User, or Protocol/Application
- have at least 6 10/100/1000 Ethernet interfaces available
- be able to configure interfaces in routed mode, bridge mode, or mixed mode (combination of routed mode and bridge mode)
- support vlans management (Tag VLAN 802.1q) and bridge mode with the vlans
- support IPV6

- support access via 3G or 4G modems on a USB port (offered by Guinean service providers) for fault tolerance
- be able to configure in transparent mode with a bypass in case the appliance suffers a failure

Intrusion Prevention System (IPS)

To meet technical specifications, the IPS must:

- have an IPS signature-based module and anomalies based on protocols
- be able to make behavioral analyses of any traffic
- be able to create its own signatures
- update IPS signatures automatically
- create and allocate IPS policies by type of area or interface
- be able to temporarily or permanently authorize or block, send an alarm, send an email, and/or automatically quarantine for any attack;
- be able to manage IPS profiles in combination with certain traffic in the filtering policy (IP source, IP destination, service, protocol, network, etc.)

Administration

- To meet administrative requirements, the operations capacity of the solution must:
 - allow administration through a secure web interface
 - allow administration in CLI (Command Line Interface) via a Console
 - be simple, user-friendly, and ergonomic graphical interface
 - allow backup, restoration, import and export of the configuration
 - grant access to the secured administration interface with the directory being integrated
 - support a multilingual console (minimum: French and/or English)
 - support Simple Network Management Protocol (SNMP)
 - define administrative profiles according to predefined access levels
 - support configuration of different policies and different modules in "object" mode (machines, networks, services, protocols, etc.) with the ability to make groups
 - contain dashboards with equipment supervision (with visual indicator) and monitoring of alarm levels
 - be able to perform, in a centralized way, the update, the backup, the policy deployment, or the sending of a configuration script of all or part of the system
- To meet administrative requirements, the production of reports must:
 - be composed in accordance with best practices in the industry
 - integrate several predefined types of reports

- make logged data, including alarms, weaknesses, connections, visited websites, and antivirus and spam measures, accessible
- integrate highly detailed monitoring reports detailing username, IP address, application, destination, port/protocol, etc.
- generate graphical reports automatically
- generate an activity report detailing e-mail, antivirus, web applications, etc.
- To meet administrative requirements, monitoring capabilities must:
 - be able to conceive general graphic dashboards presenting the overall condition of the equipment
 - provide real-time visualization, including:
 - system status (CPU, RAM, License),
 - alarm reports,
 - weaknesses,
 - output from each of the interfaces,
 - authenticated users,
 - status of VPN tunnels,
 - active sessions,
 - quarantine status,
 - monitoring updates on IPS, antivirus, anti-spam, etc.
- To meet administrative requirements, authentication capabilities must:
 - allow internal user authentication
 - provide authentication for all protocols (authentication request integrated to the filtering rule)
 - support interconnection with an external directory such as an LDAP, Active Directory, or RADIUS
 - produce certificates for infrastructures with PKI public keys with regards to the X509 standard

UTM functionalities

- URL filtering and Applicative filtering needs include:
 - Web filtering by site categorization based on predefined categories
 - filtering HTTPS flows based on the URL
 - ability to block URLs based on common expressions

- ability to grant unique permissions for each user
 - ability to filter and control the protocol and/or applications
- Anti-spam needs include:
 - support for SMTP, POP3, and IMAP protocols.
 - detection technology by RBL database for effective detection
 - analysis by DNS blacklists or by heuristics
 - a quarantine list for processing incoming emails
- Antivirus needs include:
 - an effective antivirus scanning engine
 - antivirus scanning for HTTP, HTTPS, FTP, SMTP, IMAP, and POP3 protocols
 - the ability to analyze compressed files
 - the ability to refuse encrypted files
- Web Application Firewall (Reverse Proxy) needs include:
 - protection from attacks
 - load balancing across multiple servers
 - routing and control of HTTP and HTTPS flows
 - protection against SQL Injections, Cross-site Scripting (XSS), Session Hijacking, URL Tampering, Cookie Poisoning
 - secure and control encrypted connections in servers and user accounts
 - status dashboards for remote applications
- VPN IPSEC/SSL needs include:
 - support for IPSEC VPN connections (site to site, client to site) and L2TP
 - integration of the SSL VPN
 - support for encryption algorithms: DES, 3DES, AES, TwoFish, Serpent, and Blowfish
 - integration of a PKI (Public Key Infrastructure)
 - the ability to serve as a certification authority or to integrate an external certification authority

Minimum connectivity and performance needs:

- 6 10/100/1000 interfaces that can be configured as LAN/DMZ/WAN
- 40,000 concurrent sessions
- 40 Mbps antivirus flow

- 80 Mbps IPS (Intrusion Prevention System) flow
- console port 1
- USB port 1
- licenses (antivirus and anti-spam) for unlimited users
- retrievable backup configuration with graphical administration tools
- ability to schedule security updates (antivirus, anti-spam, weakness analysis, IPS, etc.) according to the administrator's needs and convenience

Centralized management

To meet technical specifications, the management of the proposed system must be centralized. This centralized management should enable the simultaneous on-line monitoring of the activity of all deployed appliances. It must furthermore have the following features:

- centralized management and configuration (configuration, object definitions, NAT, firewall rules, web/application filtering, anti-spam, etc.)
- synchronized configuration of different firewalls from the central console
- the ability to implement policies on multiple devices
- configuration backup
- centralized reports and logs to view the system status of all deployed equipment
- web interface and ability to administer in command line interface
- definition of access profiles as administrator and auditing log files (access, changing the configuration, etc.)
- management of e-mail alerts.

Tolerance and recovery in case of failure

In addition to the two Internet access points, the required appliances have the ability to access the Internet using 3G or 4G USB keys. For all sites, there will be at least one on-site backup generator that can provide power immediately in case of power failure.

Each one will also have a recovery procedure in case of an accident, a procedure which may include the ability to quickly assemble a workstation outside of the usual work space. This workstation will be an "occasional" mobile user that can access the interconnection through an IPSec or SSL VPN tunnel; VPN clients must therefore be provided in unlimited number with no additional license fees.

Public key infrastructure

Associated with the directory, the interconnection solution shall:

- develop a public key infrastructure;
- deploy a Certification Authority using the Certificate Services;
- conceive and publish one or more certificates using the certificate templates installed with the Certificate Services;
- select one or more distribution methods (also called certificate registration methods) to install the certificates on computers and distribute them to users.

TECHNICAL SPECIFICATIONS OF THE SERVERS

A central site will host all the servers:

- the messaging broker,
- the directory,
- the statistics platform.
- These servers will be machines that meet the following specifications:
- Processor: 2 or 4 processor sockets
- Processors: Intel ® Xeon ® 7500 series or 6500 series, up to eight cores
- shared memory (DDR3) of 256 GB
- 20 TB of striped disks
- Two SAS/SSD DASD (Direct Access Storage Device) controllers
- One SATA controller
- 3 USB (Universal Serial Bus) ports
- 2 HMC (Hardware Management Console) ports
- 2 SPCN (system power control network) ports
- Operating System
 - Ubuntu Server 12.04 LTS 64-bit or other stable Linux distribution with long-term support

The Java Enterprise Edition platform used will be Apache Geronimo of the Apache Software Foundation or GlassFish from Oracle.

SERVICE SPECIFICATIONS

In addition to the providing the equipment, some of the other expected services are listed below.

The services cover the following areas:

- delivery and installation:
- Providers will have to offer an integrated solution for the supply and full installation of hardware and software. They will therefore have to prove their expertise working in this context and provide detailed information on the procedures for delivery, installation, and commissioning of the proposed hardware and software
- training teams in the participating institutions:
- Through an appropriate combination of training and support documents, the provider shall help prepare teams in the participating institutions to use all hardware and software effectively.
- configuration:
- Providers shall configure and test all hardware and software
- acceptance tests:
- Providers shall perform acceptance tests and all test procedures must be specified
- warranty:
- During the 2-year (24-month) warranty period starting on the date of the acceptance tests, the warranty service shall cover preventive maintenance, failure diagnostics, and troubleshooting in case of hardware or software failure with the replacement of the failing components or equipment
- documentation:
- All equipment and software must be supplied with documentation in French, covering technical and operational aspects, system administration and support, user manuals, and any other helpful documents.

BUDGET ESTIMATES

Topics	Quantities	Unit price	Total
		US dollars	US dollars
VPN			
Firewall UTM (1 per site and 1 backup)	5	10,000	50,000
Monthly subscription fee (12 months for all four sites)	48	2,000	96,000
Servers			
Development	2	20,000	40,000
Production	2	20,000	40,000
Data storage	2	20,000	40,000
Statistical platform	2	20,000	40,000
Backup	2	20,000	40,000
Study trips to learn from the experience of countries like Liberia, Ghana, or Rwanda			
Airfare	10	2,500	25,000
Accommodation, per diem	70	300	21,000
Training activities			
Global package			100,000
Human resources			
Team Leader, E-Governance Expert, Information Security Specialist			
Fee	252	650	163,800
Airfare	2	2,500	5,000
Accommodation, per diem, transport, and telecommunications	365	600	219,000
Java Enterprise Edition Developer			
Fee	168	500	84,000
Airfare	2	2,500	5,000
Accommodation, per diem, transport, and telecommunications	240	600	144,000
Economist - Statistician			
Fee	168	600	100,800
Airfare	2	2,500	5,000
Accommodation, per diem, transport, and telecommunications	240	600	144,000
Database engineer			
Fee	168	500	84,000
Airfare	2	2,500	5,000
Accommodation, per diem, transport, and telecommunications	248	600	148,800
Backstopping and logistical support by a firm	12	15,000	180,000
Grand total			1 780,400

APPENDIX 5. STRATEGIES FOR ESTABLISHING AN INFORMATION EXCHANGE ENVIRONMENT

INTRODUCTION

The analysis of work processes for the institutions concerned focused on processing payments made to the Central Bank on diverse Treasury Accounts, specifically clearance of goods through Customs and payment of taxes.

The situation assessments at Customs, Internal Revenue, and the Treasury have revealed the channels by which information is exchanged, as well as the current means and frequency of these exchanges.

To develop a strategy for effectively implementing an interconnection between these different institutions, it is important to start with the national options for e-government in general and for integration of public financial management in particular.

This document on the interconnection strategy follows the same dynamic. It gives an overview of the national vision for e-government, then goes on to the specific needs of the stakeholder institutions of this project. It will then outline the necessary reorganization that will occur. The technical infrastructure options are covered first before discussing the software issues.

INCORPORATING THE NATIONAL VISION FOR E-GOVERNMENT

The Republic of Guinea has decided to make efforts to boost its national e-government strategy. This strategy, approved on November 23, 2013, "aims to create a national consensus around the broad objectives of e-governance, namely: improving the efficiency and transparency of public administration." The administration is expected to emphasize the four pillars below, with the last two comprising the key success factors of the first two:

1. applications;
2. networked user interaction;
3. institutional framework;
4. awareness and training.

At the very least, this interconnection project is in line with this vision, if not ahead of it.

The applications pillar and the networked user interaction pillar represent the needs of this project's stakeholder institutions. The applications will implement modern tools that will contribute to the efficiency of the administration and the transparency of its management. The interconnection will strengthen these two elements while improving information reliability and security.

Although integrating all revenue activities is not specifically on the agenda, the various initiatives already in place will almost inevitably cause significant changes in 2014 to the current environment of these revenue activities:

- The Delegated Ministry of Budget, through the services of the National Directorate of ICT Systems, is currently conducting a master plan for all the bodies within the Ministry.

- Internal Revenue has been pursuing a project since 2009 to overhaul its entire ICT system. Assuming this project can be completed in time², it is expected that this overhaul project will provide, among other benefits, various on-line tax return services.
- In 2014, Customs will migrate its computer system to the new version of ASYCUDA, called ASYCUDAWorld.
- As part of the National Payment System (NPS) project, the Central Bank will deploy in 2014 a core bank management solution.

Therefore, in 2014 each actor will have more powerful tools and a better ICT environment. A successful interconnection will therefore pave the way for full integration of all revenue activities.

INFORMATION EXCHANGE NEEDS

As they appear today, the stakeholders' information exchange needs can be assessed in terms of volume and especially frequency. The volume of data exchanged is generally not very large, the larger parts being bank statements produced each morning: thirty or so pages with about fifty lines per page. Exchanges are made at various intervals, with monthly exchanges being most common, followed by daily and weekly exchanges.

However, it should be noted that daily information exchange is far from being ideal and is something that the directorates have accepted because they cannot do any better. Indeed, daily statements are used to verify receipt of payments made by traders on the public treasury accounts from the Central Bank. This is a tedious task of painstaking research through printed listings. Eliminating the strenuous aspects of this task is a priority need, as the search has to be completed on-demand and traders may come to verify at any time within the hours of operation. With interconnection, when a company has made a tax payment to the Central Bank, which is submitted to Internal Revenue, it will be able to verify immediately that the payment was made and received.

The needs that have been identified to this point represent only a portion of the stakeholders' information exchange needs. In fact, each of the directorates involved is located centrally in Conakry. They all have local units, agencies, bodies, etc., which are distributed throughout the entire Guinean territory. An efficient solution for centralized interconnection would pave the way for the integration of other sites, both inside and outside of Conakry.

The needs expressed and identified can be summarized as follows:

- reduced processing times
- increased productivity
- improved reliability of information

To meet these needs, an interconnection is expected to achieve:

- instantaneous transactions
- elimination of redundancy

² There are many uncertainties about this project

- reduced paper costs (print, mail, envelopes, etc.)
- greater data reliability
- process automation
- increased exchange security.

ORGANIZATIONAL MATTERS

In response to the above needs, the implementation of an interconnection will make certain tasks and positions obsolete. The most obvious case of this is the required daily trip to the Central Bank to retrieve bank records. Not only will this task now be unnecessary, but the production of payment records by the Central Bank and the tedious research within these records will be unnecessary as well. Upon completion, the applications involved in this interconnection will make it possible to retrieve desired information instantly, accurately, and without the strenuous efforts that these operations currently require.

The removal of these tasks and positions, with all their implications, should be modeled and assessed before the interconnection is implemented. Although there should not be major upheavals, there will be notable changes in the organization of stakeholder institutions. The role of change management in this project is very important.

In order to successfully manage a series of changes within an organization, strong leadership, diligence, and sufficient time are required. Changes rarely occur without some resistance. It is precisely for this reason that they must be carried out in a cautious, thoroughly considered, and participatory manner.

IMPLEMENTATION OF THE INTERCONNECTION

Establishing an interconnection between the stakeholders of the project requires that workstations in different local networks be able to exchange information directly. It will be necessary to establish a major city-wide network with an architecture capable of linking the local networks of several sites.

Customs and the Central Bank have already established a point-to-point radio link connection. This connection was a first step to solving problem of data exchange. Data is exchanged through a shared table developed by Customs. Once a payment is made, the Central Bank updates this table with the appropriate information.

Virtual private network

This “hardware - software - organization” package is an asset that will need to be integrated into the proposed infrastructure.

Implementation of the interconnection is projected to be performed by using a third party infrastructure. The use of such an infrastructure offers many advantages, the most important of which are almost instantaneous availability and the concentration of efforts on the stakeholders’ core business. Granted, the risk of becoming “hostage” to the provider is not negligible, but this possibility can be controlled with backup solutions and especially with quality contracts that are closely monitored.

Establishment of an interconnection using the existing equipment already established by a third party, such as an Internet service provider, will necessitate the use of a virtual private network,

or "VPN." In a VPN, a directorate's network can communicate with another directorate's network using the internet service provider's pre-existing infrastructure.

Specifications of the VPN

The recommended VPN organization is in the form of a star; the shared resources will be on a central, virtual site through which the various institutions will communicate. In fact, the message exchange system and the statistical platform are resources that will be managed directly in one site.

In this star configuration, the VPN will establish a "tunnel", a virtual network connection whose traffic is directed to a different network interface after undergoing the process of encapsulating and encrypting the information. Encapsulation allows data to travel across the Internet to a network that uses private addresses, and encryption ensures the confidentiality of exchanged information.

The proposed solution will be built on the Internet access points which are available at each site. Each one will have two Internet access points, one being used as backup in case of failure. The main access point will provide a minimum 2 Mbps of bandwidth. The equipment of the proposed solution will include the following components:

- an "appliance" firewall at each site, incorporating a UTM (Unified Threat Management) engine that will control interfacing with the Internet access and manage exchanges between sites through VPN (Virtual Private Network) tunnels; the firewall must be installed and configured for high availability
- a directory architecture within the Central Bank which will act as the central site, authenticating all processes and servers using the interconnection
- a virus protection solution for workstations and servers

This construction will also use a PKI (Public Key Infrastructure).

Internet provider's service level

For a VPN to make the expected benefits of an interconnection possible, mainly instantaneous transactions, it is important that the Internet provider(s) comply with several commitments in a service level agreement (SLA), such as:

- **Guaranteed Restoration Time (GRT):** a contractual obligation which determines how quickly the network must be restored if it is down
- **Maximum Service Interruption (MSI):** annual maximum, expressed in cumulative hours, during which the network may suffer interruptions
- **Network Performance (latency):** low elapsed time (in milliseconds) between the time information is sent and when it is received.

Several service providers in Conakry offer solutions fulfilling the VPN requirements for this project's interconnection, such as, for instance, MTN, Orange, SkyVision, and ETI S.A.

SOFTWARE — MESSAGE EXCHANGE SYSTEM

Once the different offices can communicate beyond their local networks, the next priority will be software. The key question is: "How will different applications exchange information?"

As part of the implementation of the interconnection between the Central Bank and Customs, these two structures have begun establishing a shared Oracle table. This table is created by Customs. It records the information pertaining to the tax payment records. Once a payment is made, the Central Bank inputs the payment information in the same table.

This simple and quick solution is used on a temporary basis. The long-term preference involves the establishment of a data exchange system with asynchronous messaging. Exchanges will be done through JAVA interfaces developed by the Central Bank and Customs.

It is with this same system of asynchronous message exchange that the entire interconnection will be established between the four stakeholder institutions: The Treasury, Internal Revenue, Customs, and the Central Bank.

IMPLEMENTATION OF A STATISTICAL PLATFORM FOR ECONOMIC ANALYSIS

The stakeholder institutions produce, spread, and use a lot of economic data. Since the data will pass through the implemented interconnection, it provides an opportunity to build an exceptional statistical platform for economic analysis. The goal is to have access to quality data which is required for the management and monitoring of development results.

In order to achieve this goal, the platform could collect data and statistical information that is not currently exchanged. Indeed, to conduct research on pressing (as well as long-term) development problems and to perform analyses of policies, both current and potential, it is important to have statistical data in several areas covering several decades. It will then be essential to integrate as many statistics as possible to the various exchange processes in order to achieve the platform's objectives.

This platform may become the model for other national interfaces or the basis for an integrated system of macroeconomic analysis.

INFORMATION SECURITY ISSUES

Issues pertaining to information security are an important part of interconnection. It is the quality of the information exchanged which gives value to this interconnection. It is therefore crucial that information security be a chief concern of the primary leaders of the stakeholder institutions.

Indeed, among other responsibilities, the leaders of large institutions such as those involved in the project are aware that they must:

- fully understand the various threats facing their activity
- ensure that all measures are taken to address all identified risks in the best way possible.

Unfortunately, when it comes to information security, the technical jargon, the speed of change, and the complexity of the topics can be a major handicap for leaders. As a result, they take

shortcuts which amount to more than just delegating: they abandon their responsibilities and hand them to information security professionals.

This kind of neglect from the directorates for information security issues is potentially harmful. Instead, leaders at the highest level must maintain leadership in the following areas:

- making resources available;
- governance and decision-making;
- establishing an organizational culture with clearly defined and followed responsibilities.

The most recommended approach for any organization is to understand six key dimensions, which together comprise a mature information security policy.

1. Leadership and Governance

Obvious interest from the highest leadership levels (and even the Board) and the assumption of risk management responsibilities.

2. Human Factors

Integration of an information security culture which is strong enough to ensure that the organization has the appropriate skills and awareness for information security to be a priority for the entire staff

3. Information risk management

Implementing information risk management in a comprehensive and effective manner, all the way to level of the providers, clients, and other partners.

4. Maintaining activity and crisis management

The capacity to cope with information security incidents and the ability to limit their impact through successful crisis management and good stakeholder management.

5. Administration and Technology

Measures taken to address the identified risks and limit the impact of their potential effects.

6. Respecting the law and complying with norms and standards

Emphasis on respecting the law and complying with international norms and standards.

Taking these six key dimensions into account leads to implementing a holistic model of information security. Such a model ensures that the entire staff and all parts of an institution fulfill their roles in preventing information security incidents and maintaining uninterrupted activity in the event of such an incident.

A FEW EXAMPLES IN AFRICA

N	Country	Type of organization	IT system for customs	IT system for taxes	Sites' interconnections infrastructure
	Tanzania ³	Customs and taxes within a single unit	ASYCUDA++	Integrated system	Wired connections Use of GSM service providers
	Zimbabwe ⁴	Customs and taxes within a single unit	ASYCUDA World		Optical fiber
	Burundi ⁵	Customs and taxes within a single unit	ASYCUDA World	Integrated system	Very Small Aperture Terminal
	Ivory Coast ⁶	Separated units	Sydam World ⁷		
	Burkina Faso	Separated units	ASYCUDA	Integrated system	Inter-Administration Network (INANET) on fiber optic Extension with wimax
	Liberia ⁸	Customs and taxes within a single unit but they are currently in the process of setting up two separate units	ASYCUDA World	The USAID-GEMS project has developed an interface between the tax application and ASYCUDA World	VPN with provider, but there will soon be a switchover to an optical fiber belt

³ Yuda Julius Chatama, The impact of ICT on Taxation: the case of Large Taxpayer Department of Tanzania Revenue Authority, ISSN 2224-607X (Paper) ISSN 2225-0565 (Online), Vol.3, No.2, 2013

⁴ http://www.zimra.co.zw/index.php?option=com_content&view=article&id=1489:zimra-upgrades-network-infrastructure&catid=4:story&Itemid=85

⁵ Burundi Revenue Authority, Quarterly Report April - June 2011, http://english.obr.bi/images/stories/download/April-June_Report.pdf?ml=4&mlt=system&tmpl=component

⁶ <http://www.douanes.ci/sydamworld/>

⁷ The ASYCUDA World project, renamed SYDAM World in the context of the Ivory Coast, began June 13, 2005.

⁸ USAID-GEMS project

APPENDIX 6. IMPLEMENTATION OF A STATISTICAL PLATFORM FOR MACROECONOMIC ANALYSIS

STATISTICAL PLATFORM FOR MACROECONOMIC ANALYSIS

The stakeholder institutions produce, spread, and use a lot of economic data. Since it passes through the implemented interconnection, this data provides an opportunity to build an exceptional statistical platform for economic analysis. The goal is to have access to quality data to better manage and monitor development performance and results.

The realization of this digital platform will (i) provide quick access to reliable data, (ii) ensure electronic archiving of information, and (iii) create reliable and integrated databases, for ministerial departments and macroeconomic analysis services.

In the interconnection among the four institutions involved, the statistical platform paves the way for integration with the sector bases of the different institutions producing statistical data for the National Statistical System.

This platform may become the provider for other national interfaces or become the basis for an integrated system of macroeconomic analysis.

The procedure for implementing the statistical platform must provide the following products:

- a directory of the basic data which is currently exchanged
- a directory of the data which is produced and/or collected by each interconnected structure
- a directory of the basic data which could potentially be subject to exchanges
- a compendium of indicators; each indicator will be described with its variables, its calculation method, its history and any other information allowing for its calculation, dissemination, and understanding
- the required specifications of the open data portal
- the technical records of the open data portal (Analysis, Design, Implementation, Testing, Deployment, Maintenance, Progress Measurement and Monitoring, Updating)
- the open data portal, incorporating all basic data
- the required specifications of the statistical platform
- the technical records of the statistical platform (Analysis, Design, Implementation, Testing, Deployment, Maintenance, Progress Measurement and Monitoring, Updating)
- the statistical platform, incorporating all selected indicators

The following table shows the aggregated documents and the first-level elements they contain.

Global Flow of information between the stakeholders

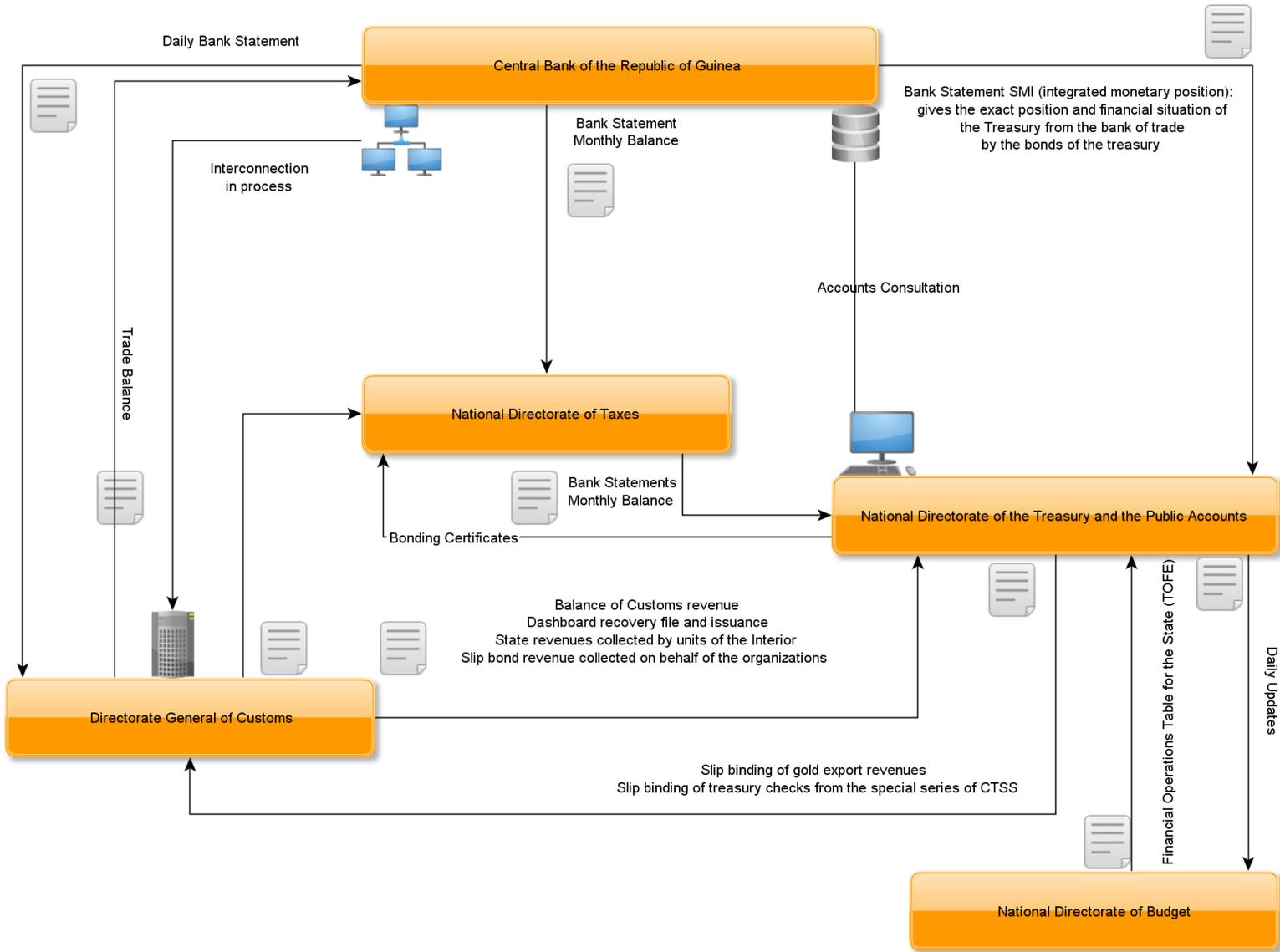


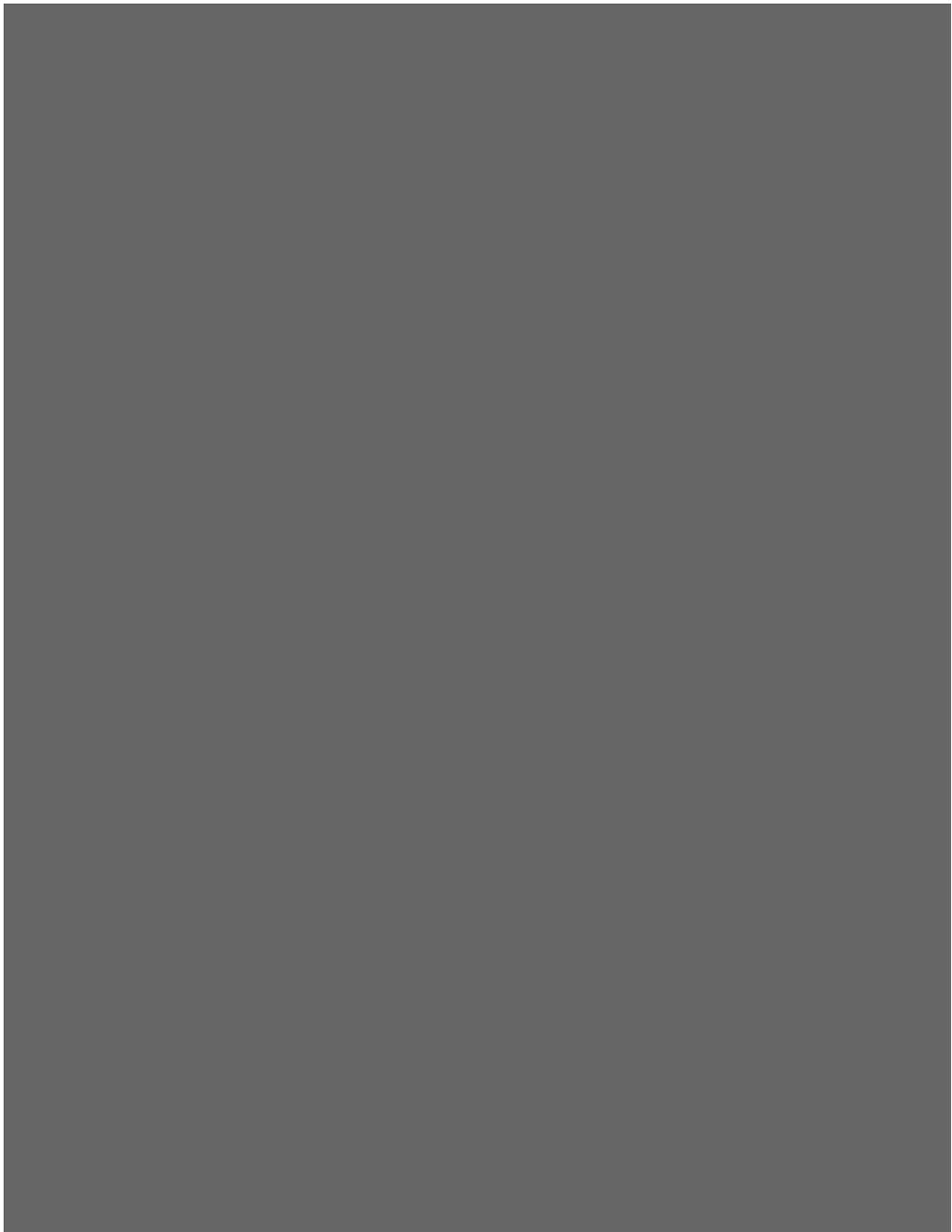
TABLE OF INFORMATION FLOWS

	Title and description	Source	Destination
1.	<p>Daily or monthly bank records</p> <ul style="list-style-type: none"> • Validation date • Code (department, year, serial No.) • Caption • GNF Debit amount • GNF Credit amount • GNF Progressive balance 	CBRG	DGC, NDIR, NDTPA
2.	<p>IMS (Integrated Monetary Situation): situation that gives an account of the Treasury's Net Position and of the Treasury's financing with commercial banks through the Treasury bonds</p> <ul style="list-style-type: none"> • Net foreign assets <ul style="list-style-type: none"> – Central Bank – Deposits Bank • Net domestic assets <ul style="list-style-type: none"> – Central Bank Net domestic assets – Net domestic credit – Claims on the public sector – Net claims on the State – Claims on the public enterprises – Claims on the private sector • Other net positions • Monetary supply <ul style="list-style-type: none"> – Monetary base • Inflation rate 	CBRG	NDTPA
3.	<p>Trade balance</p> <p><i>By product category:</i></p> <p>A. IMPORTS (Products, Net Weight, Customs Values)</p> <p>B. EXPORTS (Products, Net Weight, Customs Values)</p>	DGC	CBRG
4.	<p>Balance of customs revenue</p> <ul style="list-style-type: none"> • Accounts • Captions • Debit movements (Input Balance on the..., Previous, Operations of the month, Total) • Credit movements (Input Balance on the..., Previous, Operations of the month, Total) • Accounts balance (debtor, creditor) 	DGC	NDTPA
5.	<p>Centralizing collection dashboard file and Centralizing emissions dashboard file</p> <ul style="list-style-type: none"> • Deductions • Topics • Captions • Amounts 	DGC	NDTPA

	Title and description	Source	Destination
6.	Status of the collected revenue by internal units <ul style="list-style-type: none"> • Units • Annual quotas • Monthly collection • Total • Rate 	DGC	NDTPA
7.	Liaison slip for revenue which was collected on behalf of organizations Liaison slip between specialized accountants A. Recipient: Central Accountant Agent of the Treasury (CAAT) <ul style="list-style-type: none"> – Topics – Credited account with the Special Collector of Customs <ul style="list-style-type: none"> • Captions • Current slip • Previous • Total – Debited account with the receiving accountant – Topics – Debited account with the Special Collector of Customs <ul style="list-style-type: none"> • Captions • Current slip • Previous • Total – Credited account with the receiving accountant B. Recipient: Special Collector of Internal Revenue <ul style="list-style-type: none"> – Credited account with the Special Collector of Customs <ul style="list-style-type: none"> • Captions • Current slip • Previous • Total – Debited account with the receiving accountant – Debited account with the Special Collector of Customs <ul style="list-style-type: none"> • Captions • Current slip • Previous • Total – Credited account with the receiving accountant 	DGC	NDTPA

	Title and description	Source	Destination
8.	<p>Monthly Balance:</p> <ul style="list-style-type: none"> • Account No. • Account title • Debit: <ul style="list-style-type: none"> – Input balance – Previous – Month – Total • Credit: <ul style="list-style-type: none"> – Input balance – Previous – Month – Total • Balance: <ul style="list-style-type: none"> – Debtors – Creditors 	NDIR	NDTPA
9.	<p>Liaison slip for gold exports revenue</p> <ul style="list-style-type: none"> • Liaison slip for CAAT/Centralizing and Specialized Accountants • Credited Account with CAAT <ul style="list-style-type: none"> – Debited account with the receiving accountant • Debited Account with CAAT <ul style="list-style-type: none"> – Credited account with the receiving accountant • Monthly revenue budget breakdown <ul style="list-style-type: none"> – Folio – Date – Notice No. – Units (USD, EUR) – Budget allocation – Amount (GNF) – Amount (USD) – Amount (EUR) – Paying parties 	NDTPA	DGC

	Title and description	Source	Destination
10.	Liaison slip for Special Series Treasury Checks (SSTC) DFI and VAT duties and taxes status <ul style="list-style-type: none"> • ORI • Market reference • Supervisory Ministry • Projects • Purpose of expenditure • Amount excluding tax • Duties and Taxes Division • SSTC amount • Requested payment DFI • Requested payment VAT • Beneficiary 	NDTPA	DGC
11.	Everyday situation and instances: (a) Daily status of the Treasury at the BCRG <ul style="list-style-type: none"> – Caption – Previous operations – Operations of the day – Aggregate operations – Cash Flow Forecasting – Remains to be done – Execution rate (b) Summary of income received / ACCT <ul style="list-style-type: none"> – Title – Grand total of revenue DNT/ACCT (in GNF, USD, EUR) (c) Summary of Expenditures <ul style="list-style-type: none"> – Date – Title – Caption – ACCT – Paymaster General of the Treasury – Total 	NDTPA	DNB
12.	Liaison slip <ul style="list-style-type: none"> • Credited with the issuing accountant • Debited with the receiving accountant • Name of the debtor • Address • Amount • Nature of revenue • Reference • Accountant who made the revenue • Assignee accountant of the revenue 	NDTPA	NDIR



IBI International
2101 Wilson Blvd
Suite 1110
Arlington VA 22201- USA
Phone: 1-703-525-2277
www.ibi-usa.com