GOVERNANCE AND THE DIGITAL ECONOMY IN AFRICA
TECHNICAL BACKGROUND PAPER SERIES

Vulnerabilities of ICT Procurement to Fraud and Corruption

WORLD BANK GROUP

DIGITAL DEVELOPMENT PARTNERSHIP

The World Bank
1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

GOVERNANCE AND THE DIGITAL ECONOMY IN AFRICA
TECHNICAL BACKGROUND PAPER SERIES

Vulnerabilities of ICT Procurement to Fraud and Corruption

Hunt LaCascia and Michael Kramer

WORLD BANK GROUP

DIGITAL DEVELOPMENT PARTNERSHIP

Acknowledgments

This Background Note was prepared by Hunt LaCascia (Senior Procurement Specialist, Governance Procurement) and Michael Kramer (Consultant) under the direction of James Anderson (Lead Governance Specialist). It benefitted from comments from Maria Delfina Alcaide (Governance Data Consultant), Justin Valentine (Valent – Procurement Consultant), and Travis Mells (Valent – Procurement Consultant).

The report benefited from the inputs of the following World Bank colleagues who kindly agreed to serve as peer reviewers: Walid Dhouibi, Knut Leipold, Khalid Bin Anjum, Rajesh Kumar, Hiba Tahboub and Carey Kluttz from the Open Contracting Partnership.

The Background Note benefited immensely from the participation, assistance, and insights from other experts. The team is especially grateful for the support of the Global Governance Practice (GGP), the and the prior work of governance, finance, and procurement colleagues in both the GGP and Operations Policy and Country Services (OPCS).

We are grateful to Maria Lopez for cover design.

Common Abbreviations and Defined Terms

This section explains the common terms and abbreviations used in this paper.

Abbreviation / Term	Full Terminology / Definition
FCPA	Foreign Corrupt Practices Act
HP	Hewlett Packard
IBM	International Business Machines
ICT	Information and Communications Technology
IFMIS	Integrated Financial Management Information System
OCCRP	Organized Crime and Corruption Reporting Project
SEC	Security and Exchange Commission
U.K.	United Kingdom
US	United States

Table of Contents

1 Introduction

Information Communication Technology (ICT) contracts are prone to fraud, corruption, bid rigging and collusion. The OECD Foreign Bribery Report which shows that in 2014, 10% of the foreign bribery cases occurred in ICT sector.[1]

Integrated Financial Management Systems (IFMIS) and other ICT systems play important roles in improving transparency and accountability and reducing the opportunities for fraud and corruption in developing countries. The procurement and implementation of such systems, however, present significant opportunities for abuse.[2] The main reasons include:

a. The systemic corruption in many parts of the developing world where many such systems are procured, ironically in an attempt to reduce the impact of corruption and improve governance;

b. The large scale and complexity of such systems, which provide many opportunities to improperly rig contract specifications, manipulate implementation and inflate prices, and which make it difficult to detect such abuses;

c. The expense and potentially large profit margins of such systems, which provide ample margins to offer and pay substantial bribes to corrupt officials;

d. The relatively low risk of vendors or officials being caught and sanctioned, which is virtually non-existent in many developing countries.

[1] https://www.oecd-ilibrary.org/docserver/9789264226616-en.pdf?expires=1635533981&id=id&accname=guest&checksum=3D0743FE477E089CD599FCFB83DE05A0

[2] Installed IFMIS and other ICT systems also can be misused to facilitate procurement, payment and implementation frauds, as discussed in more detail in the paper "Reaching the Potential for the Digital Economy in Africa - Addressing Governance and Corruption Risks."

2 Examples of Actual Cases of Corruption, Bid Rigging, Collusion and Fraud in the Procurement of ICT Systems

2.1 Corruption Cases

2.1.1 Publicized Cases

2.1.1.1 Africa

2020 Semlex in Africa - Biometric Bribery: Inside Semlex's Global Playbook – an active Brussels-based company in Africa providing supplies biometric documents such as passports and driving licenses to governments and international bodies. Investigations by OCCRP have found the use of bribes, kickbacks and insider dealing to secure contracts around the world, inflating the cost of vital documents for ordinary citizens while lining the pockets of the wealthy.[3]

2.1.1.2 China and South Korea

2011 International Business Machines Corp. – SEC charged IBM for providing improper cash payments, gifts, and travel and entertainment to government officials in China and South Korea in order to secure the sale of IBM products. IBM agreed to pay $10 million to settle the SEC's charges.

2.1.1.3 India

2012 Oracle - SEC charged the California-based computer technology company with violating the FCPA by failing to prevent a subsidiary from secretly setting aside money off the company's books to make unauthorized payments to phony vendors in India. Oracle agreed to pay a $2 million fine.

2.1.1.4 Russia, Poland and Mexico

2014 Hewlett-Packard – The US SEC charged the Palo Alto, Calif.-based technology company with violating the FCPA when subsidiaries in three countries made improper payments to government officials to obtain or retain lucrative public contracts. HP agreed to pay $108 million to settle the SEC charges and a parallel criminal case.

According to the SEC, in a case in Russia, HP:

> … created excess profit margins to finance [a] slush fund through an elaborate buy-back deal scheme. [Company] subsidiaries first sold the computer hardware and other technology products called for under the contract to a Russian channel partner, then

[3] https://www.occrp.org/en/biometric-bribery-semlex/

> bought the same products back from an intermediary at a nearly €8 million mark-up and an additional €4.2 million in purported services, then sold the same products to the Office of the Prosecutor General of the Russian Federation at the increased price.
>
> The payments to the intermediary were then largely transferred through multiple layers of shell companies, some of which were directly associated with government officials. Proceeds from the slush fund were spent on travel services, luxury automobiles, expensive jewelry, clothing, furniture and various other items.
>
> To keep track of and conceal these corrupt payments, the conspirators … kept two sets of books: secret spreadsheets that detailed the categories of bribe recipients, and sanitized versions that hid the bribes from [outsiders].
>
> They also entered into off-the-books side agreements to further mask the bribes. As one example, [a company executive] executed a letter agreement to pay €2.8 million in purported "commission" fees to a U.K.-registered shell company, which was linked to a director of the Russian government agency responsible for managing the Office of the Prosecutor General of the Russian Federation project.

2.1.1.5 Panama

2016 SAP SE - The software manufacturer agreed to give up $3.7 million in sales profits to settle SEC charges that it violated the FCPA when its deficient internal controls enabled an executive to pay bribes to procure business in Panama.

2.1.1.6 Hungary, Thailand, Saudi Arabia, and Turkey

2019 Microsoft Corporation - The company agreed to pay more than $24 million to settle SEC charges related to FCPA violations in Hungary, Thailand, Saudi Arabia and Turkey and criminal charges related to Hungary.

2.1.1.7 Saudi Arabia, China, Djibouti, Vietnam, Indonesia and Kuwait

2019 Ericsson - The multinational telecommunications company agreed to pay more than $1 billion to the SEC and DOJ to resolve charges that it violated the FCPA by engaging in a large-scale bribery scheme involving the use of sham consultants to secretly funnel money to government officials in multiple countries.

2.1.2 Publicly Reported Investigations

2.1.2.1 Romania, 2019 Investigation of Oracle subsidiary

https://business-review.eu/news/oracle-romania-ceo-questioned-by-anti-corruption-prosecutors-on-bribery-allegations-203832

2.1.2.2 South Africa, 2020 Investigation of SAP

https://www.reuters.com/article/us-sap-se-safrica-exclusive/exclusive-south-africa-tries-to-recover-over-23-million-from-sap-for-unlawful-contracts-idUSKCN2531MX

2.1.3 World Bank Sanctions Case

2017 - The World Bank Group announced the debarment for six months of FreeBalance, Inc., a Canadian provider of financial-management-related software, in relation to sanctionable misconduct under the Integrated Financial Management Information System (IFMIS) Project for Liberia. The debarment, which precludes the company from participating in World Bank-financed projects, is part of a Negotiated Resolution Agreement (NRA) under which the company did not contest a fraudulent practice of failing to disclose the identity and payment terms of a local agent in Liberia. https://www.worldbank.org/en/news/press-release/2017/11/09/world-bank-group-announces-settlement-with-freebalance

2017—The World Bank Group announced the debarment for 2.5 years of Oberthur Technologies SA (Oberthur), a French digital security company (now part of a company called Idemia). The sanction relates to corrupt and collusive practices under the Identification System for Enhancing Access to Services Project (IDEA), a project designed to establish a secure, accurate and reliable national ID system in the People's Republic of Bangladesh.[4]
https://www.worldbank.org/en/news/press-release/2017/11/30/world-bank-announces-settlement-with-oberthur-technologies-sa

2.1.4 Other Unpublished Cases

A number of cases involved ICT vendors providing their products at steep discounts to their local resellers, who then sell the product to the final customer at the full price. The resellers use the extra profits from their discounts to fund and pay the bribes, often through other intermediaries and shell companies. See, e.g., https://www.gibsondunn.com/wp-

[4] https://www.worldbank.org/en/news/press-release/2017/11/30/world-bank-announces-settlement-with-oberthur-technologies-sa

content/uploads/documents/publications/Hanna-Farhang-Soto-Peters-Channeling-the-Channel-Partner-Risk-Addressing-Anti-Corruption-Risk-FCPA-Report-6-21-2017.pdf

In Africa, an ICT vendor agreed to pay multi-million-dollar bribes through the award of bogus maintenance contracts to government officials. The scheme was revealed by the vendor's project manager who worked for several years on the project before being removed just weeks before the contract award because he objected to the payment of bribes demanded by the government officials. As a result, he lost the substantial bonus he would have earned on the award of the contract. The bonus was instead paid to an outside "consultant" who quickly negotiated the terms of the contract award and the corrupt payments.

In another case, an ICT vendor deliberately incurred financial penalties for the late delivery of contracted services; the penalties were then used to fund the agreed bribe payments.

A major European ICT vendor had a roster of hundreds of unused offshore shell companies in Liechtenstein, a secrecy jurisdiction, to which funds intended for bribes could be transferred in payment of fictious invoices. A representative of the shell company in Liechtenstein would then convert the proceeds to cash and deliver them directly to the officials involved in Nigeria and elsewhere.

Other common methods to fund and pay bribes in ICT cases include the payment of inflated fees and commissions to sales agents, the payment of fees to shell companies for non-existent goods and services, payments to offshore shell companies controlled by corrupt officials, the payment of bribes in cash, literally delivered in suitcases, gifts in kind, such as vacation travel, the payment for the education of children of corrupt officials or the offer of jobs to them, and so on.

2.1.4.1 Bid Rigging Cases (Unpublished case):

A competitor for a substantial ICT contract award in Pakistan was permitted by the project manager, in exchange for a corrupt payment, to write the specifications for the contract in a manner that, of course, favored the competitor.

2.1.4.2 Collusion Cases (Unpublished cases):

In several projects in Central Asia and elsewhere, several major ICT vendors systematically colluded in the award of contracts by agreeing on which companies would bid and win on which projects, often even before the request for bids were formally announced. The firms also agreed to divide work on the contracts, e.g., one company agreeing to submit a bid only on the software component and another company to bid only on the hardware component, thereby increasing prices and defeating competition.

The relatively few companies that are qualified to bid on major ICT contracts made it easy to arrange for such collusion. A former senior executive of one of the companies advised that the companies would

routinely meet before major procurements to determine whether the companies would collude in the competition, or bid separately, or at all.

In most developing countries, government and procurement officials are aware of the collusion, even suggest and facilitate it, to raise prices and increase margins for the payment of bribes.

2.2 Fraud Cases

Unpublished case:

In a case in Africa, an ICT vendor, in collusion with procurement officials, in order to fund bribes, deliberately and unnecessarily inflated the scope and price of the contract, and then delivered fewer features than called for in the contract.

In several other cases, ICT vendors charged for but deliberately failed to install products and features called for in the contract.

2.3 Procurement Abuses

It is not uncommon for ICT vendors to sell unnecessary and often unused features to inflate fees and profit margins.

"Horizontal collusion:" ICT vendors can provide reasonably priced initial system and then promote the addition of other high-priced products and features, again often unnecessary and unused, which only the vendor can provide.

3 Best Practices to Reduce the Vulnerability of IT Procurements to Corrupt Practices

There are various best practices to reduce the vulnerability of IT procurement to corrupt practices. Here we include examples of best practices used in countries who succeeded in combatting corruption in ICT contracts. For example, Queensland State (Australia)seems to be doing well in mapping and monitoring corruption risks in ICT contracts and in establishing a standard Information Technology Contracting (QITC) framework.

To reduce corruption in ICT contracts in Queensland State, all agencies should:

- Ensure procurement and contracting practices are transparent, accountable and meet obligations in accordance with legislation, codes and policies.

- Have a detailed planning process which includes risk identification and assessment adequate to the level of value, complexity and sensitivity of the procurement.
- Be alert to the possibilities of "grooming" of staff by potential vendors or other interested parties.
- Proactively anticipate and explore conflicts of interest and increase disclosure obligations.
- Scrutinize applications for secondary employment carefully to identify potential conflicts of interest.
- Find out how frequently "urgency" is given as a reason for taking shortcuts with the proper procurement process, and why it is happening.[5]

In general suggested recommendations for improvements include:

1. Closer scrutiny on needs deliverables and costs in ICT procurement
2. Closer scrutiny on agent fees
3. Wider use of eProcurement systems
4. More aggressive WBG "Client Management:" promptly address possible irregularities in Bank ICT procurements

4 ANNEX

Below are the definitions of the most common corruption and fraud detection techniques are listed below. For a more detailed list please refer to the report: Finding Fraud: GovTech and Fraud Detection in Public Administration.

4.1 Conflicts of Interest

Project or government officials can take undisclosed financial interests in companies or suppliers that provide goods, works and services to the project. Such firms often are shell companies, without permanent staff or significant assets, that operate out of residences or other business fronts.

4.2 Bid Rigging

The bid rigging schemes are linked to corruption, as corrupt parties often seek to rig the bidding process to favor the corrupt payer and to exclude other legitimate bidders. As such, bid rigging schemes are both red flags of corruption and evidence of corrupt influence. Click on each scheme for more information.

In some cases, corrupt project officials will not tamper with the selection process by the methods and will select what they believe to be the best bid or proposal. They will then demand a bribe

[5] https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Prevention-in-Focus-ICT-procurement-2018.pdf

from the selected firm before they will sign a contract. In this case the price of the bids or proposals may rise, but the other red flags of bid rigging will be largely absent.

4.3 Collusive Bidding

Collusive bidding refers to agreements by contractors or suppliers in a particular trade or area to cooperate to defeat the competitive bidding process in order to inflate prices to artificially high levels. It can occur in large and small contracts. Where collusive bidding is well established prices can rise substantially, in some cases by as much as several hundred percent.

Collusion in international projects often involves corruption, in which government officials and procurement personnel under their direction sponsor or facilitate the collusion in exchange for bribes. All or part of the corrupt payments often end up in the coffers of local political parties where they are used to offset campaign and other expenses.

4.4 False, Inflated and Duplicate Invoices

A contractor or supplier can commit fraud by knowingly submitting false, inflated or duplicate invoices with the intent to defraud, either acting alone or in collusion with contracting personnel as the result of corruption.

"False invoices" refer to invoices for goods or services not rendered. "Duplicate invoices" are fraudulent if issued knowingly with the intent to defraud.

Duplicate, false or inflated invoices often are used to generate funds for bribe payments.

"Knowingly" typically is defined as:

- Actual knowledge of falsity
- Deliberate ignorance of truth or falsity ("willful blindness")
- Reckless disregard of truth or falsity

Knowledge and intent can be proven directly, for example, by the admission of the subject, the testimony of a co-conspirator or other witness with direct personal knowledge, or by documentary evidence, such as an incriminating email.

Knowledge and intent also can be proven circumstantially, by, for example, showing that the subject knowingly altered or forged supporting documentation, lied to investigators, attempted

to obstruct the investigation (e.g., by intimidating witnesses) or refused to produce pertinent records.

A pattern of prior similar "errors" or misrepresentations, beneficial to the subject also can be used to show willfulness and rebut the typical defense of accident or mistake.

4.5 Fictitious Contractor (Phantom Vendor)

A project or government official can create a fictitious contractor, consultant, vendor or supplier that does not provide any actual goods or services in order to embezzle project funds. The fictitious companies often purportedly provide consulting or other hard to verify services, such as repair work or the delivery of consumables, rather than more tangible goods or services that can more easily be verified.

In similar schemes, project or government officials can set up and control "middleman" companies that are used to purchase goods or services from legitimate companies for resale at higher prices, or shell companies that subcontract all work received to other firms. Such "companies" often operate out of residential addresses or other non-business locations and cannot be found on the internet or in business or telephone directories.

Contractors also can set up fictitious companies to submit complementary bids in collusive bidding schemes.

5 Bibliography

Business-Review. 2019. “Oracle Romania CEO facing bribery charges in investigation by anti-corruption agency”. https://business-review.eu/news/oracle-romania-ceo-questioned-by-anti-corruption-prosecutors-on-bribery-allegations-203832

Crime and Corruption Commission, Queensland, Australia. 2018. “ICT procurement — what are the corruption risks?”. https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Prevention-in-Focus-ICT-procurement-2018.pdf

FCPA Report. 2017. Volume 6, Number 12. “Channeling the Channel-Partner Risk: Addressing Anti-Corruption Risk with Channel Partners in the Technology Sector”. https://www.gibsondunn.com/wp-content/uploads/documents/publications/Hanna-Farhang-Soto-Peters-Channeling-the-Channel-Partner-Risk-Addressing-Anti-Corruption-Risk-FCPA-Report-6-21-2017.pdf

OCED. 2014. “OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials” https://www.oecd-ilibrary.org/governance/oecd-foreign-bribery-report_9789264226616-en;jsessionid=J3BjTmUoLNGpUxvysJfiWcrq.ip-10-240-5-89

Reuters. 2020. “Exclusive: South Africa tries to recover over $23 million from SAP for 'unlawful' contracts” https://www.reuters.com/article/us-sap-se-safrica-exclusive/exclusive-south-africa-tries-to-recover-over-23-million-from-sap-for-unlawful-contracts-idUSKCN2531MX

World Bank. 2017. “World Bank Group Announces Settlement with FreeBalance, Inc.”. https://www.worldbank.org/en/news/press-release/2017/11/09/world-bank-group-announces-settlement-with-freebalance

World Bank. 2017. “World Bank Announces Settlement with Oberthur Technologies SA”. https://www.worldbank.org/en/news/press-release/2017/11/30/world-bank-announces-settlement-with-oberthur-technologies-sa

GOVERNANCE AND THE DIGITAL ECONOMY IN AFRICA

MAIN REPORTS

VOLUME 1 Digital for Governance: Reaching the Potential for the Digital Economy in Africa—Digital Tools for Better Governance

VOLUME 2 Governance of Digital: Regulating the Digital Economy in Africa—Managing Old and New Risks

TECHNICAL BACKGROUND PAPERS

- ICT Procurement in Africa
- Adoption of eGP in Africa
- Vulnerabilities of ICT Procurement to Fraud and Corruption
- Regulating Digital Data in Africa
- Taxes and Parafiscal Fees on Digital Infrastructure Services in Africa
- Corporate Governance and Transparency of State-Owned and State-Linked Digital Enterprises in Africa
- State-Owned Enterprises in Digital Infrastructure and Downstream Digital Markets in Africa
- Competition Advocacy for Digital Markets in Africa
- Competition Policy in Digital Markets in Africa

WORLD BANK GROUP

DIGITAL DEVELOPMENT PARTNERSHIP