Public Disclosure Authorized

Public Disclosure Authorized

GovTech
Putting people first

# FINDING FRAUD: GOVTECH AND FRAUD DETECTION IN PUBLIC ADMINISTRATION

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Economic Affairs SECO**

Report No: AUS0001581

# World

# CMC - GovTech Partnership

## Finding Fraud: GovTech and Fraud Detection in Public Administration

July 2020

GOV

© 2020 The World Bank
1818 H Street NW, Washington DC 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

Some rights reserved

This work is a product of the staff of The World Bank. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Executive Directors of The World Bank or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

**Rights and Permissions**

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given.

**Attribution**—Please cite the work as follows: "World Bank.2020. Finding Fraud: GovTech and Fraud Detection in the Public Administration. © World Bank."

All queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, The World Bank Group, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2625; e-mail: pubrights@worldbank.org.

# Acknowledgements

This Report was prepared under the leadership of Hunt LaCascia (Senior Procurement Specialist, Governance Procurement) with contributions from Izzah Akram Malik (Public Sector Specialist), Michael Kramer (STC Consultant), Eduardo Vicente Goncalves (E T Consultant) and Yasodara Maria Damo Cordova (E T Consultant). Overall guidance for the report was provided by Vinay Sharma, Ed Olowo-Okere, Tracey Lane and Adenike Oyeyiola.

This report was financed by the State Secretariat for Economic Affairs SECO of Switzerland and forms part of a preparatory phase preceding its broader engagement with the GovTech Trust Fund.

The Report benefited immensely from the participation, guidance and insights from other experts. The team is especially grateful for the support of Governance Procurement, Governance Public Sector and the prior work of the procurement colleagues in both Governance Procurement and Operations Policy and Country Services (OPCS).

# Table of Contents

Acknowledgements ..... 4
Table of Contents ..... 5
List of Figures ..... 6
I. Executive Summary ..... 7
II. Key points, challenges, and recommendations ..... 11
III. Background Information: ..... 13
IV. Terms and Definitions ..... 17
V. "Analog" Complements to Digital Reform ..... 18
VI. Legal and Policy Challenges ..... 21
VII. Political Will and Economy ..... 23
VIII. International Transparency Initiative ..... 24
IX. Digital Fraud Detection and Prevention in Procurement ..... 30
X. Country Digital Fraud Detection Initiatives in Procurement ..... 36
XI. Toward Ex Ante Fraud Detection and Prevention: e-Procurement Systems ..... 42
XII. Digital Fraud Detection in IFMIS Systems ..... 45
XIII. Digital Detection of Fraud and corruption in Human Resources ..... 49
XIV. Other Sectors of Possible Digital Fraud Detection and Prevention ..... 54
XV. Summary of Challenges to the Successful Implementation of Digital Anti-Fraud Solutions ..... 54
Annex A: Detailed Information on Procurement Fraud Red Flags, Data Requirements, and Follow-Up Steps ..... 56
Annex B: Information on IFMIS Fraud Detection Applications ..... 63
Annex C: Information on Human Resources Fraud Detection Applications ..... 69
References ..... 73

# List of Figures

Figure 1 - Control of Corruption and Good Governance ..... 14
Figure 2 - Perception of Corruption and Citizen Trust ..... 14
Figure 3 - Progress Against Corruption ..... 15
Figure 4 - E-Government and Government Effectiveness ..... 16
Figure 5 - E-Services and Perception of Corruption ..... 16
Figure 6 - Data Protection and Privacy Legislation around the World ..... 20
Figure 7 - Follow the Money ..... 28
Figure 8 - E-Saram ..... 50
Figure 9 - Sierra Leone case example ..... 52
Figure 10 - Percentage of People Who Paid a Bribe to Access Public Services, 2013 ..... 53
Figure 11 - Same Graphic Reports of Collusive Bidding Indicators ..... 57

# I. Executive Summary

This paper examines the most promising current and new technologies that can be applied to detect and prevent fraud and corruption in public administration, with a focus on procurement, integrated financial management information systems (IFMIS) and human resource (HR) systems. The paper is intended to be a practical guide for practitioners, policy makers and government officials. The paper also addresses the important related "analog" (non-technical) legal, policy and political requirements for the success of digital anti-fraud measures. Other issues, such as needed capacity building and institutional reforms, are outside the scope of this paper, and are treated in more detail elsewhere.

According to the United Nations every year an estimated US$1 trillion is paid in bribes and US$2.6 trillion stolen through corruption. Together, this sum represents 5 percent of annual global GDP. Further, in developing countries, funds lost to corruption are estimated to be 10 times the amount of overall Official Development Assistance (ODA)[1].

The inverse link between corruption and successful development outcomes has been well established: corruption deters investment and impedes economic growth, exacerbates income inequality, increases the cost of government services, lowers trust in government and increases political instability.

The impact of corruption and fraud worsens under emergency conditions and in times of economic distress, such as the COVID 19 crisis. The increased demand and time pressures for the acquisition of remedial goods and services lead to the relaxation of procurement and inspection procedures, creating an increased risk of the selection of unqualified of fictitious suppliers (well-known and reliable suppliers being overwhelmed) and the delivery of poor quality or non-existent goods and services.

Effectively responding to such conditions requires the services of highly qualified, diligent and ethical development professionals, ideally trained in anti-fraud measures and equipped with tools to detect and prevent it, including the measures discussed in this paper. Also required are the development of effective emergency procurement procedures, more intensive background checks on suppliers and more intensive, independent inspections of received goods and services.

## The advantages of digital fraud detection

In recent years, breakthroughs in digital technologies have expanded the scope of reform possibilities and provided an array of new tools to governments to help them improve governance outcomes and control corruption. e-Government tools and e-Services are closely related to improved outcomes in government effectiveness and perceptions of corruption. Together, these digital tools present an exciting new frontier in the fight against corrupt practices.

As highlighted in this report, there are significant opportunities for and benefits from using digital tools to tackle fraud and corruption in the public sector, benefits that extend beyond just detecting corruption. Studies show that capturing the full potential of government digitization can free up US$1 trillion annually in global economic value through lowered costs and improved operational performance

[1] United Nations, "International Anti-Corruption Day," https://www.un.org/en/observances/anti-corruption-day.

(Dilmegani, Korkmaz, and Lundqvist 2014). The UK Government Digital Service (GDS), for example, saved the UK government £4.1 billion between 2011 and 2015 (Filer 2019).

At the same time, digital tools are not a panacea. As the country case studies in the following sections of the report illustrate, technology is most effective when it is paired with traditional fraud detection and prevention methods and integrated with "analog" components of reform.

## Analog complements of digital reform

The following analog factors are important for the successful implementation of digital anti-fraud measures.

### Data availability

Fraud detection algorithms require, of course, access to the relevant electronic data: bids and purchasing information for procurement transactions, financial information for IFMIS systems and employee information for HR systems. Quick, easy and reliable access to such data is the number one requirement for the successful implementation of digital anti-fraud measures.

### Data privacy and protection

Governments must regulate who can access confidential public sector data and how this data will be used and keep data security at the forefront in all digital efforts to detect fraud and corruption.

Efforts also must be made to prevent government actors from using digital systems to selectively target their political opponents and to guard against inherent biases built into algorithms and data (Aarvik 2019). Parties must be able to "defend their interests against the reasoning of an algorithm, just as they should be able to appeal the reasoning of a human."

### Digital infrastructure and data sharing

Governments in many developing countries continue to work in silos, with minimal institutional and technical coordination. To make full use of digital systems (once they have been set up) governments need to develop formal roles and business procedures to enable data sharing across government entities as well as put in place incentives to ensure that they are followed.

### Digital literacy and institutional capacity

Studies have shown that there is a "skills and resources gap" when it comes to technology and data analytic tools in the public sector (CFRR 2017). In addition to building existing public administration capacity, governments can partner with academic institutions to ensure that the curriculum focuses on essential digital skills and the use of technology to address public administration challenges (Filer 2019).

### Link to government decision making

Sanctions must be present and enforced to deter the misconduct detected by digital systems. This requires regular monitoring and reporting and links to responsible government decision makers willing to take remedial action, which is often lacking. Public disclosure of information and citizen engagement tools may help spur such action.

### Adapting to the local context

Governments should focus on improving existing digital systems, in incremental steps, rather than importing systems that may be overly ambitious and not fit.

No technology or digital tool can guarantee success when it comes to government reform efforts (Pathways for Prosperity Commission 2019). The 2016 World Development Report notes that many public sector digital technology projects fail: various estimates suggest that about 30 percent are total failures, with the project abandoned before completion and 50 to 60 percent are partial failures. Fewer than 20 percent are successes. A widely quoted study blames inadequate regulatory, political, management, process, and skill realities. (World Bank 2016, 165–6).

# Legal and policy challenges

## Barriers to successful implementation of digital anti-fraud strategies

The primary impediments include:

a. Poor infrastructure, such as intermittent internet connection or the lack of computing power to process the data and applications involved in the FMIS ecosystem
b. Poor public financial management (PFM) strategy resulting in reduced usage and the minimal standards
c. Corrupt fiscal reporting practices, the automation of bad practices, out of date institutions and even lack of translated materials
d. The common problems found in digital transformation projects, such as low capacity and skills, or the absence of an official authority in charge of implementing usage and development of international standards

## Grievance mechanisms: the right to human revision

Big data technologies and Artificial Intelligence can "learn" distortions and biases from the underlying data sources. Access to grievance redress mechanisms, is therefor, important. "Access to redress" means that a human should review the results of a questioned algorithm. See European General Data Protection Regulation (GDPR).

## Questions regarding the admissibility of digital evidence in the legal system

A report by the U.S. Department of Justice, predicted that "legal issues concerning the admissibility of digital evidence will nearly always arise" (NIJ 2007, 39) which impact the utility of information collected digitally. For example, a computer might identify a pattern of bids that to an experienced practitioner strongly indicate collusive bidding; such information may be admissible in one legal system and not in others.

# Political will and economy

The political will to install digital anti-fraud systems and to follow up on the results with appropriate sanctions is absent in many countries where the systems are needed most.

If implemented, however, GovTech reforms may increase civil society's trust in government and demands for more transparency and accountability, which in turn may increase the political will to implement further reforms.

# International transparency initiatives

A number of ambitious international transparency initiatives promote increased transparency and accountability in government procurement systems. The open databases allow civil society and other groups to analyze the data for fraud and corruption risks and indicators, waste and inefficiencies.

## Digital fraud detection and prevention in procurement

Combating fraud and corruption in procurement is a central focus of digital fraud detection: it is where most major fraud and corruption cases and losses occur and where governments spend the most money, often financed by international donors. According to the OECD:

> Governments around the world spend an estimated $9.5 trillion on goods and services each year. This accounts for roughly one third of government expenditures (29.1 percent on average in OECD countries) and ten to twenty percent of total gross domestic product ("GDP") in many nations - more than 14% in low income countries. (Djankov, Islam, and Saliola 2016)

Below is a brief description of the most common and costly fraud and corruption schemes that occur in procurement and their primary Indicators ("red flags") that can be detected electronically. More detail on the schemes, their red flags, detection methods, data requirements and follow-up steps can be found in the main text and Annex A, and at https://guide.iacrc.org/proof-of-common-schemes/.

## Toward ex-ante fraud detection and prevention: eProcurement systems

Most current procurement fraud detection programs are ex-post (after the fact) efforts to identify fraud indicators in previous procurements, after the misconduct has occurred and losses have been sustained. eProcurement systems would appear to offer the best opportunity to move to the far superior ex-ante (proactive) fraud detection programs, given eProcurement's immediate, easy access to the masses of relevant data that such systems collect and store.

Surprisingly, it appears that few eProcurement systems currently include ex-ante detection programs - referred to as "Governance Filters" - in routine purchasing transactions, and it appears that there are no such programs that monitor large scale tender transactions, where serious losses are routinely incurred.

## Digital fraud detection in IFMIS systems

IFMIS systems can be vulnerable to a number of fraud and corruption schemes, such as the misallocation of budget items, processing of inflated payments to shell companies or phantom vendors and payments to offshore accounts as part of a money laundering scheme.

There are a number of robust commercial anti-fraud systems that can be installed in or linked to commercial IFMIS systems. These systems can provide continuous monitoring and ex-ante alerts of potential fraud, many related to accounts payable transactions. Similar functions may be programed in homegrown systems, but the expense and technical difficulty of doing so may raise issues.

## Challenges to the successful implementation of IFMIS platforms

In the best of circumstances, IFMIS platforms are expensive, complex and difficult to install, operate, and maintain. A 2009 paper by the U4 Anti-Corruption Resource Center cited the "almost universal failure to implement and sustain IFMIS systems in developing countries" and attributed it to a number of factors, including unsound project design, the lack of the necessary underlying financial reforms, inadequate digital readiness and inadequate financial management skills. U4 Anti-Corruption Resource Center, "The Implementation of Integrated Financial Information Management Systems," U4 Expert Answer, April 8, 2009, https://www.u4.no/publications/the-implementation-of-integrated-financial-management-systems-ifmis/

## Digital detection of fraud and corruption in human resources

To date there has been limited use of anti-fraud digital technologies in the HR sphere compared to their use in procurement and IFMIS platforms. HR information systems and the data they collect do, however, present a novel opportunity for governments to expand the digital fight against corruption.

## Next steps

Moving forward there are a few next steps that could be taken to further introduce the advantages of digital anti-fraud technology. The creation of a prototype ex-ante digital fraud detection program that would demonstrate how such a system could be installed in an eProcurement system. This would provide a necessary, tangible illustration of the design, operation and benefits of such a program. A similar tool might be developed for operation in an HR system. Furthermore, research should be conducted to identify the appropriate location for such a demonstration, in which the necessary political will, digital infrastructure, capacity and enthusiasm is present.

# II. Key points, challenges, and recommendations

## The promise and importance of moving to ex ante fraud detection

The ability to apply fraud detection and prevention algorithms to detect and prevent fraud ex-ante – before contracts are awarded or payments are made – has obvious, enormous advantages.

Most current fraud detection systems are ex post, identifying possible misconduct only after the fact. There are some ex ante (proactive) fraud detection programs in IFMIS platforms, but few if any in e-Procurement and none in systems that monitor tenders, where the benefits of ex ante detection would be the most significant, as discussed below.[2]

New e-Procurement systems could be designed to incorporate ex ante programs (known as "Integrity Filters" or "Governance Filters"), and current systems can be modified to do so without undue technical difficulty or expense, although other challenges remain, as discussed below.

Overcoming these challenges and broadly incorporating ex ante fraud detection and prevention programs in e-Procurement, IFMIS, and HR systems should be a top priority in anti-fraud strategies.

## The need for stronger fraud detection algorithms

Many if not most of the current digital detection programs, from those run by individual agencies to country systems and large-scale transparency initiatives, suffer from weak fraud detection algorithms. The indicators often are too ambiguous and imprecise to be effective and generate too many false positives.

For this reason, this paper includes comprehensive lists of the proven, most effective indicators to identify possible misconduct in procurement, IFMIS, and HR systems in Appendices A, B, and C.

[2] Research has revealed no current ex ante detection or prevention programs in HR systems.

## Fraud detection algorithms should be tailored to the country in which they are installed

Contrary to many assumptions, fraud schemes in procurement and other sectors do not frequently change, but they do differ by country and region. To be effective, fraud detection algorithms should be tailored to the schemes and red flags as they occur in the location where installed and should include new indicators "learned" by the operation of such systems.

AI systems, which can find unique and previously unknown fraud patterns and indicators in large data sets, can be most useful in this regard.

## Fraud detection technology is most effective when integrated with traditional detection and prevention methods

Even with better algorithms and tailored applications, automated systems are most effective when incorporated with traditional fraud detection and prevention methods.

Automated fraud detection systems, for example, work best when linked to whistleblower systems that provide useful focus, and even strong fraud indicators must be followed by traditional investigative steps to conclusively resolve the issues.[3]

For example, computer generated indicators of corruption usually identify possible instances of corrupt influence, such as high-priced contracts or favorable treatment of certain contractors; proof of corrupt practices requires the further evidence of a related illegal payment, usually provided through traditional investigative means. Similarly, computers may identify unusual bid patterns that indicate collusive bidding, but proof may require evidence of an actual, confidential agreement to collude, again usually obtained by traditional means. And indications of false or inflated invoices, such as invoice amounts that exceed purchase order terms and prices, must be followed by proof that the invoices were submitted knowingly and willfully, and not by accident or mistake. See more information on the combination of traditional and digital investigation steps in collusive bidding at https://guide.iacrc.org/potential-scheme-collusive-bidding/.

Anti-corruption strategies should therefore continue to seek to improve traditional detection, investigation, and prevention methods even with the advent of promising new technologies.

## Automated fraud detection systems should be extended to the project implementation stage

Most current digital fraud detection systems focus on the procurement stage—bids and contract awards—and largely ignore misconduct in the implementation stage, where most losses occur, particularly in construction and infrastructure projects.

Current IFMIS programs can be linked to e-Procurement systems to identify potential misconduct in invoicing and payment transactions, but research has revealed no programs that identify indicators of

---

[3] For examples of traditional fraud detection methods, see International Anti-Corruption Resource Center (IARC), "Guide to Combating Corruption and Fraud in Development Projects," IARC, Washington, DC, 2020 (online), https://guide.iacrc.org/10-steps-of-complex-fraud-and-corruption-investigation/.

more serious implementation frauds, such as product substitution, the failure to meet contract specifications, or corruption in the supervisory function.

Current procurement fraud detection programs should be extended, and new programs developed, to identify misconduct in these areas, as discussed below.

### Expense and complexity of installing anti-fraud systems in homegrown IFMIS platforms

The impressive features of commercial IFMIS fraud management systems and add-ons theoretically could be incorporated in homegrown systems. The expense and difficulty of accomplishing this, however, could be substantial and may represent a major impediment to implementation. On the other hand, homegrown solutions may be better tailored to the risks, needs, and capacities of local users.

### Issues regarding the expense and complexity of installing anti-fraud systems in homegrown IFMIS platforms

The impressive features of commercial IFMIS fraud management systems and add-ons theoretically could be incorporated in homegrown systems. The expense and difficulty of accomplishing this, however, could be substantial and may represent a major impediment to implementation. On the other hand, homegrown solutions may be better tailored to the risks, needs, and capacities of local users.

### Challenges to implementing anti-fraud technology: lack of IT capacity, resources, political will, and other factors

Many of the countries where digital fraud detection systems would be most useful lack the capacity, resources, or political will to implement them. Research for this paper revealed a great many projects that failed for these reasons; in fact, many of the papers that purported to describe digital fraud prevention initiatives instead discussed almost exclusively the difficulty in implementing them.

Some of the difficulties in installing ex ante anti-fraud programs in country e-Procurement systems might be addressed by installing the systems to run remotely in independent oversight organizations, such as the World Bank, the EU, or other donor organizations.

## III. Background Information:

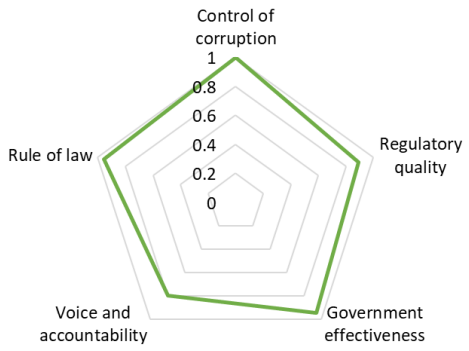
### The impact of corruption on governance

According to the United Nations (UN), every year, an estimated US$1 trillion is paid in bribes and US$2.6 trillion stolen through corruption. Together, this sum represents 5 percent of annual global GDP. Further, in developing countries, funds lost to corruption are estimated to be 10 times the amount of overall Official Development Assistance (ODA).[4] Collectively, these statistics demonstrate the scale of the challenge of corruption confronting governments around the world.

[4] United Nations, "International Anti-Corruption Day," https://www.un.org/en/observances/anti-corruption-day.

**FIGURE 1 - CONTROL OF CORRUPTION AND GOOD GOVERNANCE**

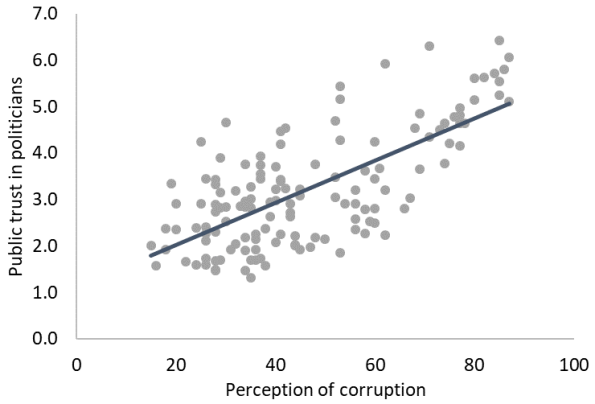
WGI pairwise correlations, 1996–2017




*Source*: Chuah, Loayza, and Myers (2020).
*Note*: Based on Worldwide Governance Indicators data.[5]

**FIGURE 2 - PERCEPTION OF CORRUPTION AND CITIZEN TRUST**

2017–2018 GCI data, 2019 CPI data




*Source*: Global Competitiveness Index (GCI); Corruption Perceptions Index (CPI).[6]
*Notes*: GCI: 1=low, 7=high; CPI: 0=corrupt, 100=clean; based on 137-country sample.

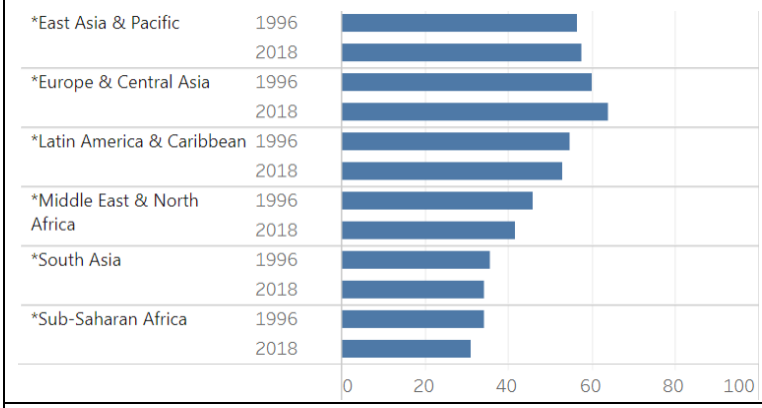
A vast body of literature has clearly demonstrated the inverse link between corruption and successful development outcomes. For instance, it has been shown that corruption deters investment and impedes economic growth. Empirically, one standard deviation change in measured corruption leads to a decrease of 1 percentage point in GDP (Chuah, Loayza, and Myers 2020, 2). Similarly, corruption can exacerbate income inequality. A standard deviation change in measured corruption can lead to an increase of 11 percentage points in inequality, as measured by the Gini co-efficient (Chuah, Loayza, and Myers 2020, 2). The prevalence of corruption also affects government interactions with citizens. For example, studies have shown that corruption increases the cost of public services and can therefore impede citizen access to basic service delivery (World Bank 2019a). In turn, corruption's negative impact on the provision of services can lower citizen trust in government and lead to increased levels of political instability. Figures 1 and 2 above demonstrate the close link between corruption and various dimensions of good governance and public trust.

[5] World Bank, "Worldwide Governance Indicators," https://info.worldbank.org/governance/wgi.
[6] World Economic Forum, "Global Competitiveness Index: Public Trust in Politicians," https://govdata360.worldbank.org/indicators/h5c4a5dee?country=BRA&indicator=666&viz=line_chart&years=2007,2017; Transparency International, "Corruption Perceptions Index," https://www.transparency.org/research/cpi/overview.

Despite this recognition of the underlying importance of curbing corruption to make broader gains in development, countries have had mixed results when it comes to actual reform efforts. As figure 3 shows, over the past two decades, although states in the East Asia and Pacific and Europe and Central Asia regions have made some progress in controlling corruption, (based on perception data and survey results), countries in other parts of the world have seen average outcomes deteriorate.

**FIGURE 3 - PROGRESS AGAINST CORRUPTION**

1996 and 2018 WGI data




*Source*: Worldwide Governance Indicators.[7]

*Note*: Percentile Rank: 0=lowest, 100=highest.

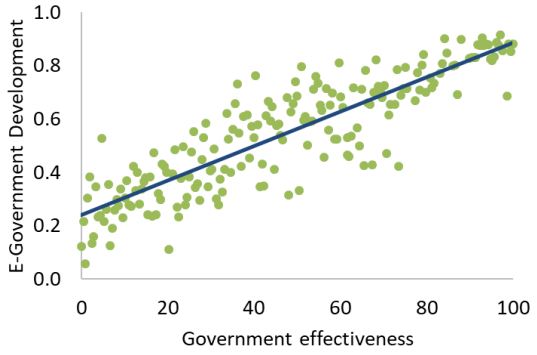
## Digital tools and the fight against corruption

In recent years, breakthroughs in digital technologies have expanded the scope of reform possibilities and provided an array of new tools to governments to help them improve governance outcomes and control corruption. As figures 4 and 5 below illustrate, e-Government tools and e-Services are closely associated with improved outcomes in government effectiveness and perceptions of corruption. Together, these digital tools present an exciting new frontier in the fight against corrupt practices.

[7] World Bank, "Worldwide Governance Indicators: Control of Corruption," https://info.worldbank.org/governance/wgi.

**FIGURE 4 - E-GOVERNMENT AND GOVERNMENT EFFECTIVENESS**

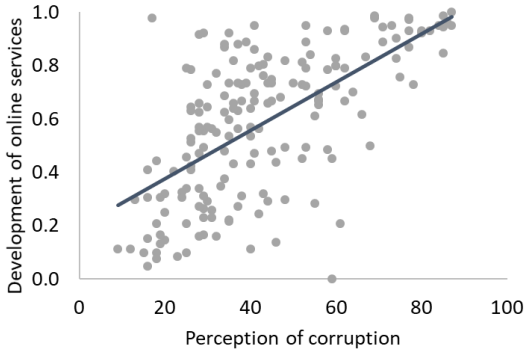
2018 UN data, 2018 WGI data




*Source*: E-Government Development Index (EGDI); Worldwide Governance Indicators (WGI).[8]
*Notes*: EGDI: 0=low, 1=high; WGI Percentile Rank: 0=low, 100=high; based on 191-country sample.

**FIGURE 5 - E-SERVICES AND PERCEPTION OF CORRUPTION**

2018 UN data, 2019 TI data




*Source*: E-Government Development Index (EGDI); Corruption Perceptions Index (CPI).[9]
*Notes*: EGDI: 0=low, 1=high; CPI: 0=corrupt, 100=clean; based on 176-country sample.

**FIGURE 6 - DIGITAL TOOLS AND CORRUPTION**

In **Afghanistan**, the government tested the rollout of mobile salary payments for local policemen in 2009. The testing revealed that under the previous cash payment system, 10 percent of salary payments never reached their recipients, as they were diverted to ghost employees or siphoned off by middlemen. "Most policemen assumed that they had been given a significant raise in salaries, while they were simply receiving their full pay for the first time."[10]

In **Albania**, the government put in place an SMS-based system for citizens to provide feedback on any challenges related to accessing public services and to report if they were asked for a bribe. The program focused on the health sector and property registration services—two areas that were particularly prone to corruption in the country.[11] Since then, the government has been able to reach 187,000 citizens and has investigated 189 corruption complaints. These efforts have been seen to be instrumental in fighting corruption and improving citizen trust in government.[12]

---

[8] United Nations, "e-Government Development Index", https://publicadministration.un.org/publications/content/PDFs/UN%20E-Government%20Survey%202014.pdf; World Bank, "Worldwide Governance Indicators: Government Effectiveness," https://info.worldbank.org/governance/wgi.

[9] United Nations, "e-Government Development Index: Online Service Component", https://publicadministration.un.org/publications/content/PDFs/UN%20E-Government%20Survey%202014.pdf; Transparency International, "Corruption Perceptions Index," https://www.transparency.org/research/cpi/overview.

[10] M. Mumford, "M-Paisa: Ending Afghan Corruption, One Text at a Time," Techcrunch, October 17, 2010 (online), https://techcrunch.com/2010/10/17/m-paisa-ending-afghan-corruption-one-text-at-a-time.

[11] J. Kunicova and Z. Bhatti, "Building Trust in the Government One Text at a Time," World Bank (blog), June 9, 2015, https://blogs.worldbank.org/governance/building-trust-in-government-though-mobile-messaging.

[12] R. Seligmann, "Is GovTech the Missing Ingredient to Curb Corruption?" World Bank (blog), December 11, 2018, https://blogs.worldbank.org/governance/govtech-missing-ingredient-curb-corruption.

In **Ukraine**, the government launched an e-Procurement system called ProZorro in 2015. By 2017, the system was handling US$14.4 billion in contracts and had generated estimated savings of US$1.5 billion, a figure equivalent to 1.4 percent of the country's GDP (Chuah, Loayza, and Myers 2020).

This report looks at novel approaches to harnessing big data, artificial intelligence (AI), and digital technologies to address the challenge of fraud and corruption in public administration. It does so by focusing on three key areas that have not received as much comprehensive focus: (1) public procurement, (2) financial management, and (3) human resource management. The report makes an important contribution to this topic by describing the cutting-edge technologies that can be applied to tackle corruption in government systems and by providing actionable insights for policy makers, development practitioners, and government officials. This is done through the use of country case studies and a complementary discussion of the non-digital (or "analog") drivers that can make or break digital reform efforts in the area of public sector fraud and corruption.

# IV. Terms and Definitions

## Definition of fraud as used in this paper

The terms "fraud" and "irregularities" as used in this paper include the schemes listed below in the sections on Procurement, Expense Reporting (IFMIS), and HR systems, as well as waste, abuse, and costly errors. References to "fraud" include corruption and vice versa.

## Definition of digital fraud detection

As used in this paper, digital fraud detection refers to data analytics, AI, and machine learning programs.

In fraud detection, data analytics refers to "rules-based" analysis of data to identify indicators of fraud. The "rules," or algorithms, are defined by domain experts based on lessons learned from prior cases or risk assessments. These programs look for known indicators, such as procurement agency employees who share the same address as a vendor or bids from different bidders that are an exact percentage apart.

The indicators are then matched to the potential scheme or schemes that, depending on the strength of the indicators, are subject to further investigation to determine if they are in fact present.

Data analytics includes "big data" and "small data" analytics.

In fraud detection, "big data" analytics refers to the examination of very large data sets to identify broad trends and patterns associated with potential risks. An example would be the discovery that the award of government contracts to certain contractors by members of certain political parties increased dramatically shortly before an election cycle. The transparency initiatives described below, such as the Open Contracting Partnership and EU DIGIWHIST programs, are examples of big data programs.

Big data analytics typically do not look for specific indicators of fraud. That task is usually accomplished by "small data" analytics. These programs look for indicators of wrongdoing in individual procurements that can be matched to identifiable contractors or suppliers and procurement personnel. An example would be the detection of bid-rigging indicators in the selection of a contractor for a specific contract,

approved by certain procurement officials. The purpose of such analysis would be to identify and assign responsibility for specific wrongdoing and enforce remedial measures or apply sanctions.

The recommended fraud indicators set out below and in Appendices A, B, C, and D are examples of the red flags that would be employed in rules-based, small data analysis programs.

AI in fraud detection refers primarily to "cognitive machine learning" programs in which computers are programmed to find previously unknown indicators or patterns in large data sets, without reference to predetermined rules.

In fraud detection, AI programs can be particularly useful in finding patterns and indicators of complex frauds in new environments, such as sophisticated cartel activities that were not previously recognized and would therefor elude rule-based detection.

AI programs also can be deployed to read and analyze the written content of contract documents, invoices, and other records to identify indicators of bid rigging, false invoices, and other offenses. Examples of pattern recognition and AI text reading programs are discussed below.

# V. "Analog" Complements to Digital Reform

As highlighted in this report, there are significant opportunities for and benefits from using digital tools to tackle fraud and corruption in the public sector, benefits that extend beyond just detecting corruption. Studies show that capturing the full potential of government digitization can free up US$1 trillion annually in global economic value through lowered costs and improved operational performance (Dilmegani, Korkmaz, and Lundqvist 2014). The UK Government Digital Service (GDS), for example, saved the UK government £4.1 billion between 2011 and 2015 (Filer 2019) through its digitization efforts. Given these wide-ranging benefits, it is clear that digital technologies are here to stay when it comes to public sector operations.

At the same time, it would be a mistake to consider digital tools to be a panacea in and of themselves. As the country case studies in the following sections of the report illustrate, technology is most effective when it is paired with traditional fraud detection and prevention methods and integrated with "analog" components of reform. Some of these critical "analog" complements to digital reform are discussed in greater detail below.

## Data availability

Digital technologies that are used to detect fraud and corruption in the public sector ultimately need underlying databases that are centralized, comprehensive, accurate, timely, and accessible. This prerequisite is not a given in many countries around the world. For example, most governments outside the Organization for Economic Co-operation and Development (OECD) lack a central IFMIS or HRMIS. Many have decentralized procurement systems that are not integrated and are thus unable to "speak" to each other. As governments pursue and push for digital measures to curb corruption in public administration, parallel efforts would need to be put in place to automate internal systems for managing procurement, finances, and human resources. At the same time, governments need not wait for a "perfect" data system to realize reform gains. Country evidence shows that officials can begin with sample surveys in targeted areas that are particularly prone to fraudulent practices to analyze patterns

and identify fraud. These can then be expanded to cover the full scope of the public sector once centralized data systems have successfully been put in place.

## Data privacy and protection

This is an umbrella topic that covers several dimensions, each critical in its own right. For instance, (1) the right to individual privacy is intrinsic and must be protected.[13] Many countries have set out regulations to do just that[14] (see figure 6). Governments around the world must similarly set boundaries and regulate who can access public sector data with regard to fraud and corruption, and how this data will be used. (2) Governments must also ensure that this confidential public sector data is safe from cyber threats. For instance, reports that personal data linked to India's universal ID system *"Aadhaar"* were being sold in alternate markets for as little as INR 500 (or US$7.27) set off alarms for the government.[15] In recent years, most major developed countries have created national cybersecurity strategies and developed information-sharing mechanisms to detect and respond to cyber threats (Dilmegani, Korkmaz, and Lundqvist 2014). There is a similar need to keep data security at the forefront in any and all digital efforts to detect fraud and corruption. (3) Efforts must also be made to prevent government actors from using digital systems to selectively target their political opponents. Robust regulations and mitigation measures would need to be put in place to ensure this. Finally, (4) governments must guard against inherent biases built into algorithms and data (Aarvik 2019). They can do so by regularly retraining and auditing their algorithms. Employees must also be able to "defend their interests against the reasoning of an algorithm, just as they should be able to appeal the reasoning of a human" (Pathways for Prosperity Commission 2019b).

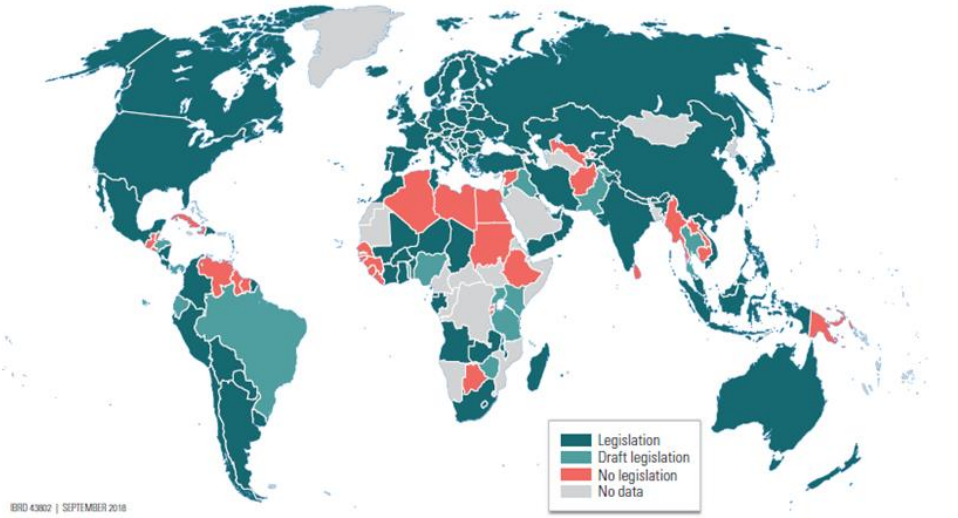
---

[13] See, for example, an article in the *Financial Times* that states that "McKinsey produced a document analyzing public perceptions of austerity measures introduced in the Kingdom of Saudi Arabia in 2015. It concluded that negative sentiment outweighed positive reactions on social media and cited three Twitter users with large followings who were influencing the debate — one of whom was later arrested." See A. England, "McKinsey 'Horrified' Saudi Arabia Could Have Used Report in Crackdown," *Financial Times*, October 21, 2018, https://www.ft.com/content/5d5fa556-d523-11e8-a854-33d6f82e62f8.

[14] See, for example, the European General Data Protection Regulation (GDPR) that determines how citizen data is to be used.

[15] J. Pandya, "Nuances of Aadhaar: India's Digital Identity, Identification System and ID," *Forbes*, July 16, 2019, https://www.forbes.com/sites/cognitiveworld/2019/07/16/nuances-of-aadhaar-indias-digital-identity-identification-system-and-id/#4e4852bc209d.

**FIGURE 7 - DATA PROTECTION AND PRIVACY LEGISLATION AROUND THE WORLD**




*Source*: World Bank (2019b).

## Digital infrastructure and data sharing

In addition to the availability of data, digital efforts to curb fraud and corruption in the public sector also require an underlying infrastructure of multiple, interoperable digital systems and data-sharing protocols and standards. This is both an IT challenge and a call for a cultural shift in how public sectors operate. Governments in many developing countries continue to work in silos, with minimal institutional and technical coordination. To move past this and make full use of digital systems (once they have been set up), governments will need to develop formal roles and business procedures to enable data sharing across government entities as well as put in place incentives to ensure that they are followed.

## Digital literacy and institutional capacity

Governments will also need to devote significant resources and policy effort to building up the skills and capacity of their staff to be able to fully utilize these digital tools and systems. Studies have shown that there is a "skills and resources gap" when it comes to technology and data analytic tools in the public sector (CFRR 2017, 7). In addition to building existing public administration capacity, governments can also work toward setting up a pipeline of digitally savvy future employees by partnering with academic institutions and ensuring that the curriculum design focuses on essential digital skills and the use of technology to address public administration challenges (Filer 2019). In order to do this, policy makers will need to think of what the "future of government" looks like and develop their workforce development plans accordingly. For example, greater use of technologies in the future may necessitate hiring more data scientists in government jobs or employees with coding and AI skills.

## Link to government decision making

Governments can spend vast resources developing digital systems and still not make progress against corruption if sanctions are not prescribed against employees on the basis of fraudulent practices (see box 2). Efforts to use digital tools to detect fraud and corruption must therefore be accompanied by regular monitoring and reporting and be linked to decision making at the highest levels of government. This may require making changes to local regulations to ensure that the government can sanction civil servants. In addition, public disclosure of information and citizen engagement tools may also help add pressure on governments to take strict action.

**FIGURE 8 - GOVERNMENT SANCTIONS AND THE FIGHT AGAINST CORRUPTION**

In **Pakistan**, under the Punjab Citizen Feedback Model, a government call center sends SMS messages and voice calls to public service users to make targeted inquiries about satisfaction with 16 services. The system has been deployed on a very large scale, with more than 250,000 citizens contacted per month. The government has taken more than 6,000 administrative actions against officials based on the feedback. However, given the protections afforded to staff under civil service rules, the actions have mostly resulted in warnings and formal apologies from concerned officials to citizens, and only a handful of cases have resulted in suspensions or dismissals (World Bank 2016).

In **Brazil**, the Office of the Comptroller General developed a machine learning application to estimate the risk of corrupt behavior among civil servants using data from criminal records, education registries, political affiliation, business relations, etc. The team found that the AI tool was effective in uncovering and predicting fraud and corruption. However, it faced challenges with regard to taking offenders to court as Brazilian law does not allow sanctions on the basis of AI predictions (Aarvik 2019). (See following section for detailed discussion on 'Digital evidence in the legal system'.)

## Adapting to the local context

Digital reforms work best when they build on an underlying knowledge of fraud risks and their indicators in the local socioeconomic and political environment (CAPI 2017). Governments should focus on using technology to improve existing systems rather than importing digital systems that may not fit. In addition, focus should be on taking incremental steps to ensure sustained improvement over time and on changing the broader public sector culture to promote ethical employee behavior.

No technology or digital tool can guarantee success when it comes to government reform efforts (Pathways for Prosperity Commission 2019b). The 2016 *World Development Report* notes:

> Many public sector digital technology projects fail. Although the evidence is limited, various estimates from surveys of government officials, audit reports, and country cases suggest that about 30 percent of these projects are total failures, with the project abandoned before completion. Another 50 to 60 percent are partial failures, with significant budget and time overruns and only a limited number of the project objectives achieved. Fewer than 20 percent are successes. … e-government scholars provide numerous explanations for these stark numbers. A widely quoted study blames a large gap between the regulatory, political, management, process, and skill realities in government and the ambitions of e-government projects. (World Bank 2016, 165–6)

To manage these risks, governments should put in place an underlying "analog" framework to complement their digital reform priorities and ensure that digital tools are used as a means to an end (in this case, controlling fraud and corruption in public administration) rather than an end in and of themselves.

# VI. Legal and Policy Challenges

## Barriers to successful implementation of digital anti-fraud strategies

Poor infrastructure, like an intermittent internet connection or the lack of computing power to process the data and applications involved in the FMIS ecosystem, will likely be a critical barrier to the successful implementation of digital anti-fraud strategies. A poor public financial management (PFM) strategy will

be reflected in reduced usage and the minimal adoption of standards, which will have an impact on the application as well. In addition to the common problems found in digital transformation projects, such as low capacity and skills, poor or no connection, or even old institutional arrangements, the application of digital anti-fraud efforts can be disrupted or impaired by the lack of translations to local languages, corrupt fiscal reporting practices, the automation of bad practices, or the absence of an official authority in charge of implementing the usage and development of international standards. As one of the remedies for these issues, recent World Bank Research concludes that "a proper focus on interoperability and reusability/expandability of application software and infrastructure elements plays an important role in the development of effective data exchange mechanisms and ensuring sustainability for integrated PFM information systems" (Dener, Watkins, and Dorotinsky 2011, 75). Underscoring that the implementation of digital FMIS ecosystems might take more than five years from inception to full operation, the projects need to include the adoption of standards as an important part of their development and deployment.

## Grievance mechanisms: the right to human revision

The AI Now Institute, an interdisciplinary research institute at New York University dedicated to understanding the social implications of AI and emergent technologies, has published a report that structures the main modern issues regarding automation and the use of these technologies to prevent and detect crimes in general. In the report, the AI Now researchers investigate the discriminatory practices that are sometimes embedded in AI algorithms, often creating loopholes in a country's labor and judicial information systems. By limiting the diversity of the data used to analyze the occurrence of flags, some platforms might be biasing their automation engines toward discrimination against vulnerable communities.

Cathy O'Neil makes the same case in her book, "Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy," arguing that, especially in the financial systems, big data technologies automate oppression and inequality by "learning" the distortions present in society and feeding a loop that keeps vulnerable communities at the margins (O'Neil 2016). Safiya Noble makes a case on how international biases might be introjected via the crowdsourcing of information, especially within public platforms that change according to the inputs made by users themselves (Noble 2018).

Research shows the importance of having grievance redress mechanisms in place when automating fraud detection. On the recommendation of the World Economic Forum, automated platforms should always be under the close monitoring and scrutiny of civil society, using four principles to guide their development: 1) active inclusion; 2) fairness; 3) right to understanding; and 4) access to redress (WEF 2018).

The last principle, "access to redress," recommends that a human should review the results, thus keeping the mechanized decisions from causing further damage through inappropriate actions (for example, by blocking the earnings of an employee before further investigation of the flagged wrongdoing).

## Digital evidence in the legal system

There is the possibility that the legal system might not be prepared to accept a piece of digital evidence. The report, *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors*, published by the U.S. Department of Justice, is categorical in affirming that "legal issues concerning the

admissibility of digital evidence will nearly always arise" (NIJ 2007, 39). Since the technology and its admissibility progress at different paces, the debate about the admission of digital evidence will probably not be resolved anytime soon (Romano 2005). Thus, it is crucial to ponder the weaknesses and strengths of the responses presented by the use of algorithms when dealing with fraud detection.

This probabilistic mechanism raises several concerns. For example, data privacy laws frequently mention the right of citizens to challenge algorithm-based decisions by invoking the right to human review. That is the case, for instance, in the European General Data Protection Regulation (GDPR).

Moreover, algorithm-based decisions are only part of the challenge. On a higher level, there is a need not only for legal reform but also for institutional change to accommodate these channels of communication, accountability, and citizen engagement. For instance, Brazil's access to information law, which focuses on transparency and accountability, created an institutional framework in the public sector that defines the proper channels through which citizens can file requests as well as the deadlines for doing so, thus establishing an appropriate pipeline for all stakeholders to track their requests and assuring citizens of a satisfactory and prompt response to their demands. The law also includes mandatory deadlines for a response from the public sector.[16]

# VII. Political Will and Economy

## Digital government and political will: the digital transformation opportunity

A government's digital transformation process represents an opportunity to use technologies to prevent fraudulent actions. Illegal activities, such as money laundering, bribery, embezzlement, and other types of corruption, were less preventable until technology started to play a central role in management. However, as the power might shift when anti-fraud technologies are put in place, digital transformation agendas can often prioritize government surveillance of citizens instead of citizen oversight of government (Lyon 2017, 19), even though the digitalization of the budgeting process has the proven potential to improve government efficiency and transparency. To create the political will to implement FMIS platforms in digital government ecosystems, trust is a key factor. The lack of trust in government, which includes local institutions, political parties, service delivery, and politicians, is often a problem for governance more generally and can worsen already fragile situations and reinforce existing social inequalities (Barro 1991). As Lee and Schachter (2019) explain, "citizens' endorsement of the overall performance of government" is an important component of trust, highly connected to low rates in the corruption perception measurement. The implementation of anti-fraud technology in digital transformation strategies, what is known as GovTech reforms, might be able to decrease citizen perception of corruption and thus increase trust in government. Another important factor that affects political will is civil society's support for the implementation of such technologies. As political stability is an essential part of political will, corruption perception and trust in politicians are connected elements that can be utilized by civil society. A general strategy to install anti-fraud measures and prevent corruption could thus help prevent fragile situations.

[16] Brazilian Federal Law number 12.527/2011.

If digital government is strengthened with high-quality technology and a systematic approach to its implementation, it could more effectively lower the levels of corruption in public administration. Strategies for trust-building outreach should include the implementation of FMIS ecosystems technology to increase transparency and keep civil servants and politicians accountable.

### International cooperation and sanctions

International cooperation on the implementation of technology to prevent fraud could have a positive impact on political will, potentially increasing trust among citizens and on global markets. International conventions have the power to harness the current need for technical anti-fraud platforms to improve the financial health of states. One example is the UN system aiming to counter transnational fraud, which includes such institutions as the Centre for International Crime Prevention, the Financial Action Task Force on Money Laundering, and the G8 Senior Experts Group on Transnational Organized Crime. Another example is the International Criminal Police Organization, or Interpol. These institutions set the standards on international norms and activities to combat fraud and crime and also establish frameworks for better implementation of systematic measures. As fraud perpetrators can sometimes have connections with international crime, using digital tools and platforms to facilitate illegal money flows, for example, it is important that international cooperation efforts use tools and platforms to prevent transnational fraud.

Sanctions as a tool to reinforce the adoption of basic standards, such as FMIS technical systems, are key to fighting international fraud. As an example,

> The WBG's sanctions system is designed both to protect the integrity of WBG development projects and to deter future wrongdoing, while at the same time incentivizing the remediation and rehabilitation of sanctioned entities. Among other measures, the sanctions system provides for the suspension and debarment of firms and individuals found to have engaged in sanctionable practices when competing for, or executing, Bank-financed contracts. (Dubois et al. 2019)

Such initiatives should be inserted into a framework that includes capacity building and executive education in order to guarantee implementation.

## VIII. International Transparency Initiative

When it comes to fraud detection, there is a multitude of initiatives that take advantage of transparency to allow civil society to keep the government accountable. In that scenario, standards play an essential role in guiding the strategy and implementation of policies to make government data open. A prominent example in this sense is the Open Government Partnership (OGP),[17] which supports governments in coordinating efforts to open data and ensures that members of civil society have the proper institutional framework to enjoy this as an asset for engagement. In a practical sense, OGP involves a minimum set of prerequisites for countries to become members and supports a two-year action plan of commitments focused on allowing citizens to oversee the public sector. The eligibility criteria include, for instance, the

[17] For more information, see https://www.opengovpartnership.org.

availability and accessibility of data (such as fiscal transparency and access to information), but also values that ensure that civil society organizations can freely and safely exercise their mandate.

OGP is a sort of generic standard, but there are also more specific, sectoral standards. The Publish What You Pay (PWYP) project, for example, focuses on the relationship between the mining, oil, and gas industries and their development. In their words, "PWYP calls for tax justice so revenues from extraction can be used to boost development, via measures such as registers of beneficial owners and companies publishing their payments to individual country governments."[18] In this way, they make relevant information accessible to interested actors in civil society, generating fiscal transparency and advancing development by strengthening the conditions for accountability. Another example that is specific to an area is the Open Contracting Data Standard (OCDS), which targets contracts in general. According to the official website, OCDS "enables disclosure of data and documents at all stages of the contracting process by defining a common data model." [19] By this means, the standard promotes transparency and allows citizens to have access to and analyze this data.

Undoubtedly, standards such as OGP, PWYP, and OCDS play a crucial role. However, they address the "supply" of open data. When it comes to the "demand" for open data, these protocols play only a minimum role. Other initiatives try to tackle capacity building at the demand side, that is to say, they invest in ways to facilitate and foster the engagement of civil society with open government data. These initiatives, even if technological in nature, can focus on non-technical or technical objectives.

On the non-technical side, Guaxi in Brazil and Alex in Australia[20] are chatbots designed to help citizens navigate through the jargon and intricate structure of the public sector. The first is a Facebook bot that teaches Brazilians about the Access To Information Law and how to exercise their rights in requesting government data. Alex is a virtual assistant from the Australian Tax Office that helps citizens do their taxes. Both chatbots offer a *quasi*-human interaction that enhances the perception of transparency, and indirectly, both build citizen capacity to use the transparency tools their governments put forward. Cases like these highlight that transparency is not only about data and technology, but also about offering tools for people to make sense of that data, understand the framework they work on, and comprehend their rights and duties in a democracy. Those tools do not need to be fancy and disruptive chatbots, but they should have enough clarity about the meaning of data and the legal framework to potentialize the engagement (and this is valid for engagement between the public sector and civil society as well as among different units of the public sector).

On the technical side, it is worth highlighting tools that have been making the manipulation of data accessible for people without an IT background. Examples in this category are Tableau and Microsoft Power BI.[21] Many journalists (without IT experience) use Tableau to organize, filter, and visualize large data sets and can therefore write data-driven stories without necessarily being or involving data engineers or data scientists. This approach is even encouraged in the curriculum of journalism schools, especially in the training of data journalists (Berret and Phillips 2016). Microsoft Power BI follows the

---

[18] For more information, see https://www.pwyp.org.
[19] More information on OCDS can be found at: https://standard.open-contracting.org.
[20] See https://www.facebook.com/gastosabertos; and https://cxcentral.com.au/advanced-technology/virtual-assistant-to-improve-self-service.
[21] See https://www.tableau.com; and https://powerbi.microsoft.com.

same trend, as it offers a portal focused specifically on journalists.[22] Assuming that a free press is essential in modern democracies, tools such as these strengthen the voice of civil society by empowering more individuals (in this case, the media) to handle open government data. Beyond journalism, these tools also make it possible for other groups to easily and quickly develop a prototype, design proofs-of-concept, and test what transparency portals can grant in terms of checks and balances.[23] This logic does not limit itself to civil society, however, as there is the potential to adopt these tools in the public sector, enabling public servants to better deal with data in the exercise of their mandates.

Thus far, in terms of transparency initiatives, this section has argued that standards provide a good background for policies that focus on accountability through engagement with data. Next are the tools that address the potential technical as well as non-technical barriers to engagement with transparency initiatives. Finally, some tangible cases will be outlined demonstrating how civil society can deal with this data by using different strategies to single out outliers and attempt to detect fraud using open government data.

Two Brazilians initiatives, for example, use financial data to compare how municipal governments collect and spend money from taxpayers. Focused on public managers, Meu Município[24] uses algorithms to provide a tool to identify optimal and suboptimal financial management strategies and public investments. It starts by "clusterizing" (that is, grouping) every one of the more than 5,000 Brazilian cities based on a multitude of indexes (inhabitants, GDP, education, urban and rural population, and so on). The result is that for any given city, the user has a small cluster that includes 10 similar municipalities. Within this cluster, there are different ways to compare data, and outliers become evident: how much each of these cities collects through every municipal tax, how much they spend in various sectors, and also some customized indexes proposed by the website. A very similar initiative is an Android app called As Diferentonas.[25] This platform departs from a clusterization of cities by similarity but focuses on the general public. It adopts a very accessible language, mimicking memes and catchphrases from the social media sphere to shed light on outliers. Another (minor) difference is that this app considers only funds transferred by the federal government to local governments (and not all municipal revenue and expenses).

These initiatives are examples of the use of algorithms to automate the analysis of big data sets made public by the government. The use of technology allows civil society to add a layer of meaning to this data, making the data appealing and, arguably, actionable. For example, in the case of Meu Município, public managers can rethink policies and set the agenda for the government in a data-driven tone; with As Diferentonas, citizens can ask their representatives about the specificities of their municipal government. In both cases, part of the explanation for outliers might be fraud and other wrongdoing. Moreover, in both cases, public-civic engagement is informed by data provided by transparency policies.

---

[22] See https://powerbi.microsoft.com/en-us/datajournalism.

[23] For instance, in the Data4Governance hackathon in Nigeria (February 2020), hosted by the ccHub, four out of eight finalists used Microsoft Power BI in their pitches to the judges. (Disclaimer about the source: as the World Bank was supporting the event, the authors made this observation *in loco.*)

[24] See https://meumunicipio.org.br.

[25] See https://play.google.com/store/apps/details?id=com.ionicframework.diferentonas906569&hl=pt_BR.

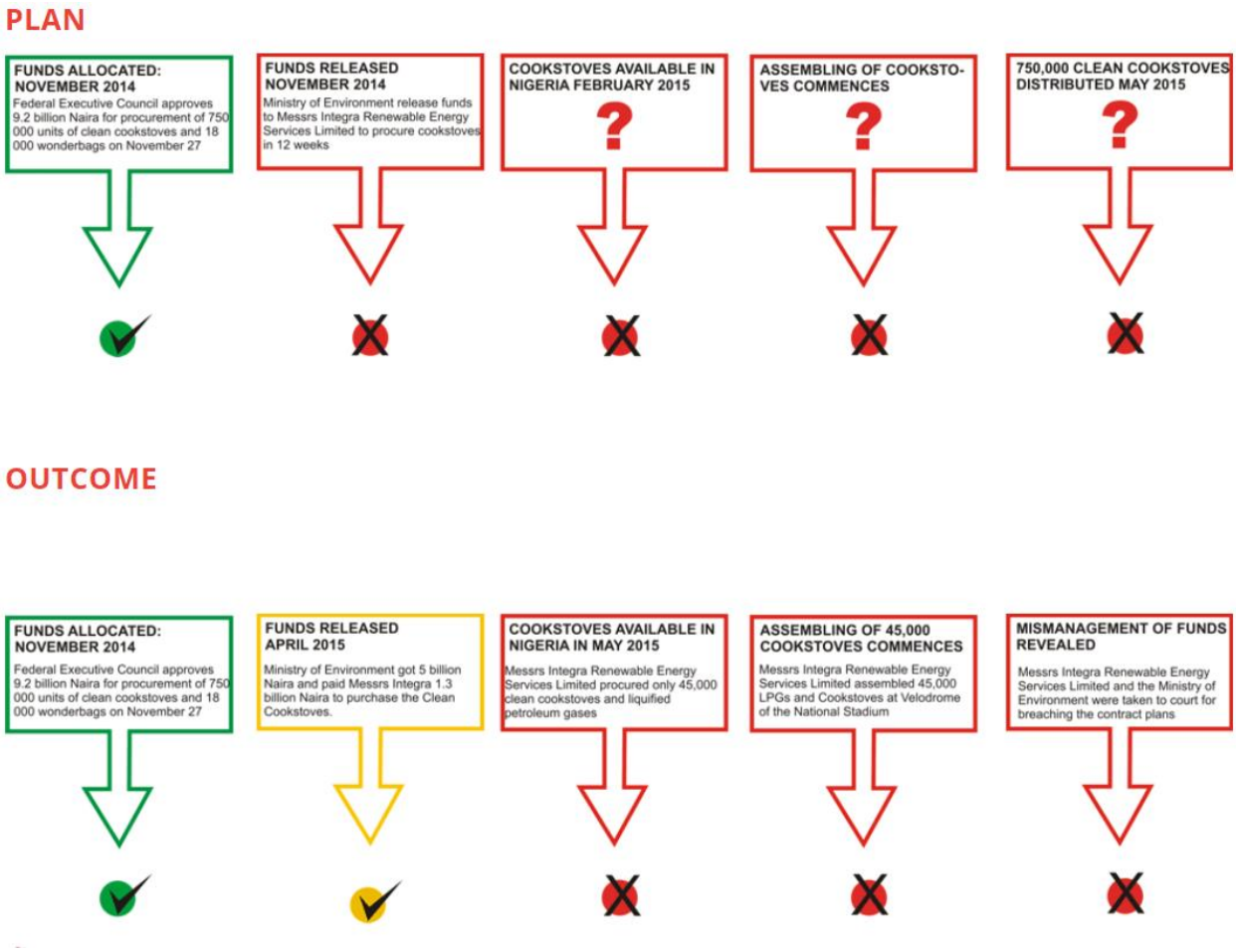
In sum, platforms like these are friendly interfaces, made possible by technology, to automate the data-driven detection of deviance.

Other initiatives count on engagement and feedback from the general public on open sources, such as social media. Operação Serenata de Amor[26] uses machine learning to uncover any suspicious activity related to public expenses. If the payment data involved includes mostly small amounts of money (for example, for meals, domestic flight tickets, taxis, and so forth), it would not be worthwhile to take those cases to court. Instead, social media provides an alternative means to call out public officials for any expenses flagged as suspicious by the algorithm. In that sense, transparency broadens its range even more in terms of engagement and thus takes accountability further.

Many initiatives follow this same roadmap. They start with open government data, use algorithms to flag suspicious practices, and finally, engage the general public (that is, engage people who are not necessarily experts in technology, financial management, and the like). This strategy is used widely in different countries. Interestingly, the engagement of the general public is usually strong enough to sustain projects that can afford a considerable impact even without involving advanced technologies, such as AI. In Nigeria, for instance, there are a number of cases of engagement with transparency through social media. Different platforms monitor public investments, taking transparency as a starting point and social media as a means. Tracka[27] describes itself as a "community of active citizens" that, via Twitter, provides space for a dialogue between citizens and official government agencies regarding the investments made (based on transparency policies) and the actual service delivery reported by local communities. A typical conversation on that feed is a report produced by a civil society initiative to which an official account responded with: a "thank you" for bringing the issue to the attention of the local government, an apology together with a justification for the problem, and a solution to the case. Follow The Money[28] provides a similar service but offers more detailed reports informing and engaging the public on the financial management flow. Among other communication strategies, this organization produces infographics such as the ones below to promote an easy rapport with the general public:

[26] See note 41.
[27] See https://tracka.ng.
[28] See http://followthemoneyng.org.

**FIGURE 9 - FOLLOW THE MONEY**




*Source:* Follow the Money.[29]

Not all examples described in this section focus on fraud detection per se. Nevertheless, they include a number of components that point to the value of adopting technical methods to identify potential fraud in the public sector. Moreover, all of these examples involve an *a posteriori* approach: first, the government expends a certain amount, which generates data in its financial management systems. This data becomes public, and only at that point can civil society act on it to try to detect fraud and other wrongdoing. A more proactive approach, taking advantage of technology in an FMIS, would instead involve an *a priori* method in which the public sector can adopt an algorithmic strategy internally and avoid fraud before it happens.

Yet, there are two other lessons from these transparency initiatives. First, that open data does not necessarily mean accessible data. The standards may help in finding better ways to share data, but extra work is often needed to help consumers of these resources to comprehend the data fully. This factor is

[29] Follow the Money, "How We Tracked 9.2 billion NGN Meant to Provide #WomenCookstoves," November 5, 2014, http://followthemoneyng.org/2014/11/05/how-we-tracked-9-2-billion-ngn-meant-to-provide-womencookstoves.

quite relevant even within the public sector; for example, one department might need data from another to implement a data-driven decision-making system. Therefore, making data open, readable, accessible, and understandable is critical even within and among agencies of the public sector. Second, if automatization leads only to indicators of fraud instead of the clear-cut identification of fraud,[30] a crowdsource architecture (with or without social media) can be used to verify the data from algorithmic decisions, as well as any other automatically generated data (for example, satellite images). In the case of the public sector adopting internal systems, this lesson demonstrates the importance of employing human labor to corroborate algorithmic results, rather than blindly following what the machine has reported. Standards, accessibility, and human engagement are great allies in the use of technology for automatic fraud detection.

## The European Union

DIGIWHIST, the "Digital Whistleblower," offers products devoted to fiscal transparency, risk assessment, and reviews of the impact of good governance policies (https://digiwhist.eu). The products include:

a. EuroPAM, The European Public Accountability Mechanism, a data collection effort to enhance the transparency of public administration and the accountability of public officials; http://europam.eu
b. Opentender, a platform that allows the user to search and analyze tender data from 33 jurisdictions; https://opentender.eu/start
c. MET, Monitoring European Tenders, another tool to assess the risks in European tenders; https://monitoringeutenders.eu
d. The Government Transparency Institute, which provides big data analytics to auditors to identify and prevent fraud and corruption in public procurement; http://www.govtransparency.eu; http://redflags.govtransparency.eu/

## The Open Contracting Partnership

The Open Contracting Partnership publishes data and documents from all stages of the procurement process from numerous countries and cities that can be analyzed for indicators of fraud, waste, and abuse. See https://www.open-contracting.org/.

The Partnership's Open Contracting Data Standard is a global, non-proprietary data standard structured to reflect the complete contracting cycle. The standard enables users and partners around the world to publish shareable, reusable, and machine-readable data, to join that data with their own information, and to create tools to analyze or share the data. Examples of the OCDS in action can be found in its global overview.

To facilitate the analysis of the contract data, the Partnership published an online resource, "Red Flags for Integrity: Giving the Green Light to Open Data Solutions," that provides a comprehensive list of indicators and a suggested methodology to examine the data. It can be found at: https://www.open-contracting.org/resources/red-flags-integrity-giving-green-light-open-data-solutions/. See also Measuring the Benefits of Open Contracting: Case Studies on Mexico, Paraguay, and Slovakia.

[30] See Legal and Policy Challenges above.

## The Open Contracting Explorer

https://www.developmentgateway.org/expertise/contracting

The Open Contracting Explorer is an open source tool for storing, disclosing, and analyzing procurement data. Data is taken directly from government sources, converted, and published in the OCDS, allowing it to be viewed through a suite of interactive tools for data visualization and in-depth analytics. The Explorer contains three distinct open-source tools:

### Monitoring and Evaluation (M&E) Dashboard

The M&E Dashboard aims to help procurement officials and citizens gain insight on the efficiency, competitiveness, and fairness of procurement practices using interactive charts, graphs, and web GIS. The flexible tool also helps users to understand where procurement creates value for money. For more information, see the collaboration with the Vietnam Public Procurement Authority.

#### Corruption Risk Dashboard

The Development Gateway's Corruption Risk Dashboard uses high powered analytics and global research to identify risk profiles for potential corruption in procurement. This red-flagging tool can assist governments in identifying procurement activities that merit in-depth auditing or public scrutiny and to view fluctuations in corruption risk, including fraud, collusion, and process rigging, over time.

#### Contract Explorer

To help citizens "follow the money," the Contract Explorer enables users to view each contracting process from program planning through the tendering, award, contract, and implementation stages. The unique search engine and repository ensures that citizens have access to full procurement data in an easily digestible format. They can also download the data to use it as they like.

See https://www.developmentgateway.org/expertise/contracting.

# IX. Digital Fraud Detection and Prevention in Procurement

Most major fraud and corruption cases occur in procurement, where governments spend the most money, often financed by international donors. According to OECD:

> Governments around the world spend an estimated $9.5 trillion on goods and services each year. This accounts for roughly one third of government expenditures (29.1 percent on average in OECD countries) and ten to twenty percent of total gross domestic product ("GDP") in many nations - more than 14% in low income countries. (Djankov, Islam, and Saliola 2016)

Fraud and corruption in procurement not only unfairly enrich corrupt officials but typically result in the selection of high-priced, unqualified contractors and the delivery of substandard goods, works, and services.

Bribes are usually paid as a percentage of the contract value and can be as high as the level of oversight—or more accurately, the lack thereof—allows. Payments can go directly to project or government officials or often to the reigning political party, or both. Smaller bribe payments may be paid to supervisory personnel to allow the contractors to cut back on quality.

Corruption of the supervisory function and fraud in implementation are much bigger problems than generally acknowledged, contributing greatly to crumbling roads, collapsed structures, invisible schools, and even entirely failed projects, all of which make anti-corruption efforts such a high priority.

For this reason, digital fraud detection and prevention procedures should be extended to the implementation stage of construction contracts, as discussed below.

For more information on fraud and corruption in procurement, see the International Anti-Corruption Resource Center's (IACRC) "Guide to Combating Corruption and Fraud in Development Projects" at https://guide.iacrc.org/. Refer to https://guide.iacrc.org/red-flags-listed-by-project-cycle/ to see the major red flags organized by project cycle; the site also links the red flags to the related schemes and follow up steps.

## The most common and costly corruption and fraud schemes in procurement

Below are brief descriptions of the most common and costly fraud schemes that occur in the procurement process and their primary red flags that can be detected electronically. More detail on the schemes, their red flags, data requirements, and follow-up steps can be found in Annex A and at https://guide.iacrc.org/.

### Collusive bidding

Collusive bidding refers to secret agreements by bidders or suppliers to divide work and artificially inflate prices, often with the complicity of government officials.

Digital detection methods can be particularly effective in detecting collusive bidding because many of the most useful indicators can be drawn from readily available bid data and the bidder's contact information.

#### Sample digital indicators:

a. Different bids from the same IP address
b. Bidders with the same contact information, such as addresses and telephone numbers
c. Unusual bid patterns, e.g., total or line item bids from different bidders that are an exact percentage apart
d. Sequential bid securities submitted by different bidders, indicating that they may have been purchased at the same time by the same person

For more information on collusive bidding, see that section of the IACRC's "Guide" at https://guide.iacrc.org/potential-scheme-collusive-bidding/.

### Bid rigging

As used here, bid rigging refers to efforts by corrupt bidders and procurement officials to improperly steer contracts to a favored bidder and to exclude others, often as the result of corruption.

Bid rigging includes several different schemes, listed below, that have different indicators. Each scheme is explained separately in the IACRC's "Guide" at https://guide.iacrc.org/potential-scheme-bid-rigging/.

a. Change order abuse
b. Exclusion of qualified bidders
c. Leaking of bid information

d. Manipulation of bids after receipt
e. Rigged specifications to favor certain bidders and exclude others
f. Split purchases to avoid upper-level review or competitive bidding
g. Unbalanced bidding: using information leaked by corrupt officials quoting unreasonably high or low line item bid prices to gain
h. Unjustified sole source awards

The primary indicators of bid rigging include violations of procurement rules and procedures to assist the favored bidder, such as not providing the required notice time to other bidders to submit bids, splitting contracts to avoid competition, or improperly awarding sole source contracts.

As bid rigging is frequently the result of corruption, its indicators are often the initial red flags that lead to the detection of bribes and kickbacks.

### Sample digital indicators:

a. Procurement official's contact information the same as the bidder's contact information
b. Shorter notice provided to submit bids than procurement rules require
c. Multiple purchases just below a procurement threshold to avoid competition
d. Award to other than the lowest evaluated bidder
e. Award to only one evaluated bidder

## Bribes and kickbacks

"Kickbacks" refer to corrupt payments, usually a percentage of the contract value, made incrementally during the contract period as the contractor is paid.

As noted above, bribes and kickbacks can be identified indirectly through bid-rigging indicators, or more directly through the "SPQQD" formula, explained below.

### Sample digital indicators:

a. Bid-rigging indicators, above
b. "SPQQD" factors:
    - Irregularities in the SELECTION of the contractor or vendor
    - The payment of unexplained high PRICES
    - The purchase of excessive QUANTITIES of goods, works, or services
    - The acceptance of low QUALITY goods, works, or services
    - The DELIVERY and acceptance of items that do not match the purchase order or contract requirements

For more information on bribes and kickbacks, see https://guide.iacrc.org/potential-scheme-bribes-and-kickbacks/.

## Shell company vendor

Shell company vendors refer to firms that are owned by procurement or agency officials employed by the procuring agency. Such schemes are typically classified as a conflict of interest under the general category of corruption.

Shell companies usually operate as unnecessary middlemen, buying and reselling readily available goods and services at a markup without providing any additional value. Many such shell companies are little more than a post office box and a bank account.

In a recent case, a national utility purchased several thousand electronic security badges for the equivalent of US$47 each through a shell company broker operated by the senior executive. The same badges were available from a legitimate online vendor for US$7 each.

The senior executive directed the purchasing department to source as many items as possible through his "company," including computer supplies, coffee, catering, and painting services, vehicle purchases and repairs, and so forth, all at unnecessarily high prices and often in unnecessary quantities.

Shell companies also can refer to schemes in which corrupt officials set up fictitious companies to act as purported suppliers or subcontractors in order to receive bribes or hide assets.

### Sample digital indicators:

a. Vendor located at a non-business address or not listed on the internet
b. Vendor corporate records or contact information linked to employee
c. HR employee record/vendor record match
d. SPQQD factors
e. Vendor provides a variety of disparate goods or services (per vendor and product codes)

For more information on shell company vendors, see https://guide.iacrc.org/potential-schemes-hidden-interests/.

## Phantom vendor

Phantom vendors, or ghost suppliers, refer to fictitious companies set up by insiders that submit false invoices as part of schemes to embezzle funds.

The fictitious transactions tend to focus on purchases that are hard to verify, such as commodities, repair and maintenance services, and consulting services.

### Sample digital indicators:

- Vendor not listed in corporate registries or directories or on the internet
- HR employee record/vendor record match
- "Fuzzy match" vendors with the same or similar names but different bank accounts
- High number or percentage of sequential invoice numbers
- Benford's Law violations[31]

Benford's Law states that in naturally occurring number sets, the number 1 will occur as the first digit about 30.4 percent of the time, the number 2 about 17 percent of the time, with the other digits

[31] Benford's Law states that in naturally occurring number sets, the number 1 will occur as the first digit about 30.4 percent of the time, the number 2 about 17 percent of the time, with the other digits descending in regular order until the number 9, which appears as the first digit about 4 percent of the time. Prices in invoices, quantities in reports, and so on that do not follow this pattern can indicate fabricated numbers and fraud. See https://en.wikipedia.org/wiki/Benford%27s_law.

descending in regular order until the number 9, which appears as the first digit about 4 percent of the time. Prices in invoices, quantities in reports, and so on that do not follow this pattern can indicate fabricated numbers and fraud. See https://en.wikipedia.org/wiki/Benford%27s_law.

For more information on phantom vendors, see https://guide.iacrc.org/potential-scheme-fictitious-contractor-2/.

## Purchases for personal use, resale, or diversion

This is a common abuse that can be quite costly if not adequately controlled, particularly if the improper purchases are used to supply inventory for side businesses, which is not uncommon.

### Sample digital indicators:

a. Purchase of inappropriate personal "consumer items"
b. Different "ship to" address
c. High number of purchases of certain items susceptible to personal use (laptops, tires, gas, vehicle repairs, etc.)
d. Unexplained spike in the purchase of such items
e. Employee has an outside business (used to resell or divert products)

## False, inflated, and duplicate invoices

This scheme can be committed by vendors or suppliers acting alone or in collusion with purchasing agency insiders. The latter are, of course, more difficult to detect.

Fictitious or inflated invoices can also be submitted by contractors and approved by insiders to generate funds for bribe payments.

### Sample digital indicators:

#### FALSE INVOICES:

a. Invoice information does not match the purchasing order, receiving, or payment information
b. Sequential invoice numbers
c. "Outlier" amounts in price and quantity
d. Benford's Law violations

#### INFLATED INVOICES:

a. Invoice price, quantities greater than the purchasing order price, etc.
b. Total payments greater than total invoice amounts

#### DUPLICATE INVOICES:

a. Invoices with the same:
    - Number, dates, and item descriptions
    - Price and quantities
    - Payment amount

For more information on false, inflated, and duplicate invoices, see https://guide.iacrc.org/potential-scheme-false-inflated-and-duplicate-invoices/.

## Other procurement reports that can be generated by small data analytics

In addition to the fraud indicators described above, digital fraud detection programs can produce useful reports on non-fraud indicators, such as errors and compliance reports, in the following categories:

a. Significant procurement statistics. For example, the number of contracts awarded to certain contractors by certain approving officials, or the average cost of certain procurements, followed by "outliers" significantly outside those parameters.
b. Economy and efficiency indicators. For example, the verification of the selection of the best product for the best price or the failure to do so, as well as the failure to collect available discounts and rebates from vendors, and so on.
c. Compliance reports. For example, contracts in violation of procurement rules, such as the acceptance of bids from debarred companies or sole source contracts above the sole source limit.

## Reduction of false positives

Dealing with "false positives"—red flags of potential fraud that have an innocent explanation—is one of the primary difficulties in implementing effective digital fraud detection programs. False positives are more numerous if the fraud detection algorithms are too general, irrelevant, or not tailored to the risk environment being examined.

a. False positives can be reduced by using precise, unambiguous indicators, such as:
    - Payments without needed authorizations
    - Purchases from unapproved vendors
    - Invoice and payment amounts that exceed purchase order amounts
    - Different bids from the same IP address
b. Other strong indicators, such as bids from different bidders that are an exact percentage apart. In a recent case in which collusion was confirmed, line item bids from three different bidders were exactly 1.343 percent apart.
c. Transactions with multiple indicators, such as a high number of red flags associated with a single purchase
d. A pattern of indicators or repeat transactions, such as a high number of split purchases by the same procurement official from the same supplier

False positives can also be reduced by linking the indicators to tips or reports of potential fraud, such as whistleblower complaints. In such cases, the complaints provide a very useful focus for the fraud tests, which in turn can be used to quickly and effectively evaluate the complaints. If the allegations are true, one would expect to find the indicators of the alleged scheme and vice versa.

## Scoring of fraud and corruption risks

Scores can be assigned to each indicator or pattern of indicators according to the likelihood that a fraud is actually present and the perceived risk level. The scoring system can be calculated automatically and used to determine the priority of the case and the appropriate level of response. This is important especially if, as is often the case, there are more fraud cases than an agency can address.

The likelihood of fraud being present depends primarily on the number and nature of the indicators. The more indicators, the higher the score, and some indicators, such as a bidder listed on an excluded party list or bids from supposedly different companies submitted from the same computer, are more telling than others.

The perceived risk level refers to the operational, reputational, and financial damage that a scheme might cause if present. A possible collusive bidding case in a US$100 million procurement would, of course, present a higher risk level and priority than an inflated invoice for office supplies.

The scoring system might be devised by a committee of procurement, audit, and operational personnel as part of a risk-assessment exercise.

# X. Country Digital Fraud Detection Initiatives in Procurement

The following country government agencies have conducted ex post digital fraud detection reviews, as described below.

## Brazil

### Brazil Public Spending Observatory

The Office of the Comptroller General of the Union launched the Public Spending Observatory (Observatório da Despesa Pública) in 2008 to enable the continuous detection and punishment of misconduct and corruption. The Observatory cross-checks procurement data with other government databases. Possible misconduct is identified by "orange" or "red" flags for follow-up investigations. The system looks for 20 indicators of potential wrongdoing, including:

a. Conflicts of interest by procurement personnel
b. Procurement abuses, such as contract splitting to avoid competitive bidding
c. Unusual bid patterns
d. Bidders with the same address
e. Rotation of winning bidders
f. Contract amendments within one month of contract award

A description of the Observatory can be found on the OECD's website at: https://www.oecd.org/governance/procurement/toolbox/search/public-spending-observatory-brazil.pdf.

Brazil also has adopted open data policies to help attack corruption. See http://webfoundation.org/docs/2017/04/2017_OpenDataBrazil_EN-2.pdf.

Other references to procurement fraud detection programs at Brazil's Public Spending Observatory can be found in the OECD's Public Governance Review of Procurement in Mexico.

## Chile

The public finance nongovernmental organization (NGO), Observatorio Fiscal, has been working in collaboration with the government's central purchasing body, ChileCompra, to develop an automated tool to detect risky procurement practices.

The "red flags" tool will analyze official public procurement data for the previous five years to identify potential indicators of irregular activity in public tenders, such as exceptionally short tendering periods, low participation, or changes to tender specifications. The tool will rely on international best practice for red flag modeling and adapt it to the Chilean context.

More information on this new tool can be found at https://www.open-contracting.org/2019/06/06/red-flags-in-chile/.

## Colombia

OECD's review of public procurement in Colombia, including the SECOP e-Procurement system, provides a good overview on e-Procurement systems and challenges more generally. Entitled, "Making the Difference in Public Services Delivery: The Review of the Colombian Public Procurement System," it can be found at:

https://www.colombiacompra.gov.co/sites/cce_public/files/cce_documentos/the_review_of_the_colombian_public_procurement_system.pdf.

OECD's report, "Towards Efficient Public Procurement in Colombia," which refers to ongoing fraud monitoring programs, also addresses these concerns (OECD 2016).

For more detailed information on the development of a model for the early detection of fraud in public procurement in Colombia, see "Preventing rather than Punishing: An Early Warning Model of Malfeasance in Public Procurement," which can be found at:

https://repository.urosario.edu.co/bitstream/handle/10336/18525/dt222.pdf.

## Indonesia

The U.S. Millennium Challenge Corporation (MCC) recently worked with the Indonesian National Procurement Agency (LKPP) to develop an ex ante fraud detection program ("Governance Filters") to be installed in Indonesia's e-Catalog and e-Procurement systems. The program was developed with the assistance of an international e-Procurement company and a local IT firm.

In addition to the e-Catalog system mentioned above, the program involves the planned installation of Governance Filters in the government's database of historic procurement information. The indicators to be installed include the following, with more planned to be introduced later:

a. Recommended contract award to other than the low bidder
b. The low bidder withdraws, followed by award to the second low bidder
c. Bids from different bidders that:
    - have the same business address, telephone number, or email address
    - are from the same IP address
    - are submitted within a certain number of seconds/minutes (adjustable) of each other
    - are identical (including line item bids)
    - are an exact percentage apart (including line item bids)
d. The significant 6-9-17 bid pattern (second low bid is 6 percent higher than the low bid, third low bid is 9 percent higher, fourth low bid is 17 percent higher)
e. Total or line item bid prices equal cost estimates (or within a certain [adjustable] percentage)

f. High price bids: bids are a certain percentage (adjustable) above cost estimate
g. Inadequate resources, infrastructure, training, and IT capacity, and less than 30 percent of companies that bought bid packages submit bids

The following collusion indicators were discovered in Indonesian procurements during the development of the Governance Filters project:

a. Rotation of winning bidders in large infrastructure tenders
b. Different bidders submitting "ping-ponged" bids for identical different lots or in similar tenders, for example:

**FIGURE 10 - PING-PONGED BIDS EXAMPLE**

| BIDDERS | LOT A Bid (Specs same as Lot B) | LOT B Bid (Specs same as Lot A) |
|---|---|---|
| Company One | $100 | $200 |
| Company Two | $200 | $100 |

c. Different bidders submitting bids from the same IP address
d. The same Bid Evaluation Committee members selecting the same companies a disproportionate percentage of times

Other collusive bidding indicators discovered in Indonesia are listed in Annex A.

## Latin America initiative

In 2019, procurement practitioners from government, oversight authorities, civil society, and the media in seven countries (Argentina, Colombia, Peru, Honduras, Chile, Paraguay, and Mexico) met to explore the use of technology to improve the efficiency and integrity of procurement systems. The group identified a number of red flag risk indicators, including:

a. Short tender periods
b. Low number of bidders
c. Low percentage of contracts awarded competitively
d. High percentage of contracts with amendments
e. Large discrepancies between award value and final contract amount

For more details on this initiative, see https://www.open-contracting.org/2019/06/27/examining-procurement-red-flags-in-latin-america-with-data/.

The OECD book, "Integrity for Good Governance in Latin America and the Caribbean," provides a comprehensive overview of e-Procurement issues and fraud detection techniques. The study notes that more contract information is available because of e-Procurement, but it is not being used systematically enough to identify red flags or malpractice, such as bid rigging (OECD 2018, 80).

## Mexico

The report, "Upgrading Mexico's CompraNet to a System that Delivers for All Stakeholders," is a good source of information on e-Procurement, indicating that many e-Procurement systems need to be redesigned and expanded to cover the full procurement cycle.

Another report entitled, "Smarter Crowd Sourcing for Anti-Corruption," also provides a good overview of automated fraud detection techniques.

## Romania

PREVENT is an integrated computer system aimed at preventing conflicts of interest in real time. The project was developed for Romania's National Integrity Agency (ANI) using EU funds. The platform is designed to interact with the country's SICAP e-Procurement system.

The Romanian Agency for Public Procurement (ANAP) received assistance from a World Bank Reimbursable Advisory Services (RAS) arrangement to "create a proactive mechanism for identifying system dysfunctions" and "methodologies for data analysis, problem identification and… corrective actions." The mechanism is intended to assist ANAP in its supervisory function over SICAP.

The SICAP e-Procurement system currently is not configured to run a "proactive mechanism" and does not contain sufficient data to run the full array of red flag indicator tests for "problem identification."

The system can be modified to collect the missing data and run proactive tests. The modifications would include uploading bids through a structured electronic data format, rather than through the acceptance of PDF documents, as is currently done. The additional data requirements consist primarily of invoice and payment information and line item detail in bids and receiving reports. Collection of this additional data would permit a broader and more accurate identification of red flags in large tenders and standard purchasing transactions than is currently possible.

In the meantime, progress is being made in the extraction and analysis of currently available information from the SICAP system to generate ex post reports of possible fraud and irregularities.

## South Korea

South Korea has instituted "BRIAS," the "Bid Rigging Indicator Analysis System." According to a 2016 report by OECD,[32] BRIAS looks at bid prices (as a ratio compared to a reference price), the number of participants, and the competition method and applies a formula that generates a potential bid-rigging score. A significant score leads to the collection of more information from the procurement system, followed by a referral for an investigation if deemed warranted.

The OECD report found that the results "have been limited: only three cases initially identified by BRIAS have led to findings of guilt." This is attributed to competition from a more traditional whistleblower reporting system, but it may also be the result of the relatively limited categories of data—price, number of participants, and competition method—that the system initially collects.

Interestingly, the OECD report noted that "during the period of [BRIAS] operation, voluntary reporting by cartel participants has increased significantly, and some of this increase is attributed to the raised awareness and fear of being caught generated by the implementation of the BRIAS system."

---

[32] See "Country Case: Korea's Bid Rigging Indicator Analysis System (BRIAS)," at https://www.oecd.org/governance/procurement/toolbox/search/korea-bid-rigging-indicator-analysis-system-brias.pdf. The full report can found at OECD (2016).

## Switzerland

The Swiss Competition Commission (COMCO) has conducted significant research on the digital detection of collusive bidding and bid rigging. Although not directly linked to e-Procurement, such research has identified useful indicators that can be included in e-Procurement systems and run on a proactive, real-time basis.

For example, COMCO identified the following recurring patterns in its cartel investigations:

a. The range of bids (from highest to lowest) was lower in tenders in which collusion was found, that is, the highest and lowest bids tended to occur within a 10 percent window. In similar tenders in which collusion was not found, the typical range of bids was in a 20 percent window.
b. There was a wider gap between the lowest and second-lowest bids than between the higher bids (namely, a 3.5 percent difference compared to a roughly 1 percent difference). This was attributed to the desire to ensure that the designated "low" bidder, nominated by the cartel, would have a sufficiently lower bid price to survive a higher technical score by the next lowest outside bidder.
c. The close distribution of bids by the losing bidders also was different than the patterns detected in non-collusive bids in other cases.
d. The cases revealed a pattern of a rotation of winning bidders among the same group of repeat bidders.

The Swiss findings are discussed in more detail at https://www.slideshare.net/OECD-DAF/cartel-screening-in-the-digital-era-swiss-competition-commission-january-2018-oecd-workshop, and https://www.oecd.org/competition/workshop-on-cartel-screening-in-the-digital-era.htm.

## Ukraine

### ProZorro

ProZorro, which means "transparent" or "clear" in Ukrainian, is a public, open source e-Procurement platform launched in 2015 to counter endemic corruption in Ukrainian procurement. It was developed in a collaboration between the Ukrainian government, the business community, and civil society, with primary assistance from Transparency International and a host of volunteers.

The project was extended in 2016 to include the sale of all types of state assets, including those of failed banks, through "ProZorro.Sales." That same year, ProZorro was awarded the World Procurement Award (WPA) and the annual prize of the Open Government Awards. In 2017, a number of automated risk indicators were added to the system, which has been credited with saving more than 10 percent of the procurement budget and lowering the incidence of fraud by an estimated 25 percent.

ProZorro uses the Open Contracting Data Standard (OCDS) and is featured by the Open Contracting Partnership (OCP) (see below) as a highly successful example of the benefits of transparent procurement practices[33].

---

[33] For more information on ProZorro see:
https://prozorro.gov.ua/en
https://ti-ukraine.org/en/news/prozorro-introduces-risk-indicators-to-check-suspicious-tenders/
https://docs.google.com/document/d/1M2lR3WhlAYPg8x2HzLp3bMEPx8rCl83lucyPi7WJFrE/edit

## DoZorro

DoZorro is an online platform that includes analytic and risk management tools that allow users to monitor and report wrongdoing in public tenders. The system was launched in 2016 and is administered by Transparency International Ukraine.

In 2018, DoZorro added an AI component to identify tenders with a high risk of corruption. Twenty procurement fraud experts were asked to identify fraud risks in about 3,500 tenders. The expert responses were used to generate proposed AI algorithms that were forwarded to civil society organizations, which reviewed the findings. Algorithms that proved to be useful were saved in the system.

According to DoZorro, the AI program identified 26 percent more tenders with improper selection procedures, 37 percent more tenders with groundless disqualifications, and 298 percent more tenders involving collusion among the parties. Most of the violations occurred in the most expensive tenders[34].

# United Kingdom

The UK Competition and Markets Authority (CMA) developed a tool for use by public sector organizations to detect potential anti-competitive behavior. The system's indicators include, among others:

a. Tenders with a single bidder or low number of bidders
b. Price discrepancies: winning price is an outlier, similar bid prices, apparently arbitrary cost calculations
c. "Low endeavor" bids, e.g., bids by the same author
d. Similar text and word count in different bids. This is an innovative and useful application, as one of the primary indicators of collusive bidding is physical similarities in bids from different bidders, including similar text and word counts, which previously eluded electronic detection.

The tool has been distributed to almost 90 organizations in the United Kingdom and is being reviewed by 29 national competition agencies. More information can be found at https://www.slideshare.net/OECD-DAF/cartel-screening-in-the-digital-era-uk-competition-markets-authority-january-2018-oecd-workshop.

However, on January 20, 2020, the CMA announced, without explanation, that the screening tool had been withdrawn from use. See

---

http://uacrisis.org/59870-prozorro-risk-indicators#prettyPhoto/1/
http://uacrisis.org/53278-proekt-prozorro-prodazhi

[34] For more information on DoZorro see:
https://ti-ukraine.org/en/news/dozorro-artificial-intelligence-to-find-violations-in-prozorro-how-it-works/
https://oecd-opsi.org/innovations/dozorro/
https://digitalsocial.eu/project/3224/dozorro
https://oecd-opsi.org/innovations/digital-tools-to-monitor-and-predict-risks-in-auditing-ukraines-revolutionary-online-public-procurement-system/

https://www.gov.uk/government/publications/screening-for-cartels-tool-for-procurers.

# XI. Toward Ex Ante Fraud Detection and Prevention: e-Procurement Systems

E-Procurement systems offer the best opportunity to obtain the benefits of ex ante fraud detection, given the easy, real-time access to the large volume of relevant data that such systems collect and store.

As noted above, however, it appears that, currently, very few if any standard e-Procurement systems include proactive fraud detection algorithms, known as "Integrity Filters" or "Governance Filters," and there appear to be no such programs that monitor ex ante large-scale tender transactions, where large losses are routinely incurred.

The reasons and potential fixes for the slow implementation of ex ante programs are discussed below.

## The promises and challenges of e-Procurement systems

Current standard e-Procurement systems, even without the installation of Integrity Filters, represent a major advance in the efficiency and integrity of procurement procedures, streamlining the process, reducing its cost, and eliminating the many opportunities for human interference and mischief.

A 2016 article in *The Economist* reported that:

> … For more than a decade, [the Copenhagen Consensus] has assessed the global costs and benefits of different development schemes … The winner, yielding a fantastic $663 in benefits for every dollar spent, is digital procurement. … One study suggests that eProcurement cuts the price of contracts by about 12%. Because switching to online bids is fairly cheap, the assumed returns are huge. (*The Economist* 2016)

The installation of Governance Filters would further enhance the benefits of e-Procurement by:

a. Instantly reviewing 100 percent of all transactions, rather than limited samples as in standard audits
b. Blocking non-compliant or improper procurement transactions, such as bids from companies on ineligible lists or bids received after the bid deadline
c. Providing instant alerts of possible fraud, prioritized by importance and level of risk
d. Permitting detailed, real-time remote monitoring by oversight agencies, which is not currently feasible in paper procurement transactions
e. Creating detailed audit trails and digital evidence for auditors and investigators

A 2014 report from Transparency International report found that "although the majority of EU countries have central and/or local databases for public procurement, only half of them query their data about unusual patterns, and only a few develop or use indicators that point to possible cases of corruption. Similarly, only three countries have e-procurement platforms that contain a module designed for the detection of corruption" (TI 2014, 5). The report did not identify the three countries, and further research has not revealed them.

The reasons for the lagging implementation include:

a. E-Procurement systems are designed by procurement and IT professionals to efficiently accomplish electronic procurement transactions, with, understandably, little if any thought given to the inclusion of fraud detection measures.
b. As a result, most current e-Procurement systems do not collect the necessary data to run the full array of Governance Filter tests. For example:
    - Many e-Procurement systems accept bids offline or in PDF formats.
    - Some systems collect purchase orders and receiving documents, but not the invoices or payment records that are required to identify false invoices and vendor frauds.
    - Most systems do not collect unit prices in major procurements, which are necessary to identify certain collusion and bid-rigging cases.

The potential fixes:

a. Include fraud detection algorithms in the design stage of new e-Procurement systems and ensure that the necessary data is collected and stored in an accessible manner
b. Modify[35] current e-Procurement systems to:
    a. Collect relevant bid data in a structured, electronic format readable by the fraud detection algorithms, which could be accomplished by requiring the bidders to download and populate standard bidding templates with predefined fields. This would allow the computers to immediately cross reference the information from the different bidders to proactively identify indicators of collusion, bid rigging, and other frauds. The pre-structured bid forms should include line item bid prices when called for.
    b. Collect receiving, invoicing, and payment information in purchasing transactions, or link e-Procurement systems to an IFMIS or other expense management and payment apps. This would allow the integration of invoicing and payment records with procurement documents and permit the detection of false invoices and vendor frauds.

Procurement transactions can also be processed entirely through an IFMIS with procurement modules, which would provide easier access to receiving, invoicing, and payment information. Opening an IFMIS to outside vendors in procurement transactions may, however, create concerns about maintaining the cybersecurity of the IFMIS.

## Application of anti-fraud measures to the contract implementation stage

Much of the damaging impact of corruption occurs in the implementation stage, after a contract is awarded, particularly in construction and infrastructure projects. Contractors, subcontractors, and suppliers can submit false and inflated invoices and deliver substandard work in order to increase profits and generate funds to pay the bribes that were agreed to in the procurement stage. These can be extremely costly, even more so than the procurement abuses, and lead to the failure of an entire project.

[35] Many of the existing systems were originally designed in the 1990s and now need to be redesigned to operate more efficiently. This could provide a good opportunity to make the necessary modifications to install the Filters.

The detection and prevention of schemes in the implementation stage can be facilitated by digitalizing the construction contract's procurement, billing, receiving payment, and inspection records. This would permit the application of algorithms to detect and prevent the following schemes:

a. Inflated Bills of Quantities ("BoQs") (listing unnecessary and inflated quantities to increase contract values)
b. False and inflated payment applications, including:
    - Front loading of payments
    - Inflated percentage of completion claims
    - For work not performed
    - For materials not purchased
    - For equipment not leased
    - Improper labor rates
    - Inflated equipment rates
    - Charges for time and materials on lump sum contracts
    - Payments without work orders
    - Acceptance of inflated invoices from subcontractor and splitting the profits
c. Forged lien waivers
d. Failure to pay subcontractors and vendors
e. Payments to fictitious subcontractors and vendors
f. Substitution of substandard materials, equipment, and goods
g. Deliberate failure to meet contract specifications
h. Purchases for personal use; diversion of materials or equipment to other projects
i. Change order abuse

Blockchain technology could be used to secure the information. For example, under a typical fraudulent practice in construction projects, a subcontractor may receive a proper invoice from a legitimate supplier for $100, submit a forged copy of the invoice and increase the amount to $200, submit it for payment to the prime contractor, who further inflates the price to $400 and submits it to the project owner. With paper records this would be difficult to prevent and would require some effort to detect, probably in an audit after the transactions are completed. If the information is digitalized, however, an automated fraud management system, using blockchain for increased security, could automatically match the original invoice data and price information to later copies to prevent the fraudulent increase in prices.

Vendor verification and due diligence checks also could be automated[36].

[36] See the following resources for more information on digital detection of construction fraud:
https://www.constructiondive.com/news/recognizing-and-combating-construction-fraud/514519/
https://www.constructiondive.com/news/using-technology-to-head-off-construction-fraud/560730/
https://www.levelset.com/blog/construction-fraud/
https://www.constructionbusinessowner.com/insurance/most-common-types-construction-fraud

# XII. Digital Fraud Detection in IFMIS Systems

## Introduction to Integrated Financial Management Information Systems

According to the World Bank:

> Financial Management Information Systems (FMIS) support the automation and integration of public financial management processes including budget formulation, execution (e.g. commitment control, cash/debt management, treasury operations), accounting, and reporting. FMIS solutions can significantly improve the efficiency and equity of government operations, and offer a great potential for increasing participation, transparency and accountability. Whenever FMIS and other PFM information systems (for example, e-procurement, payroll, debt management) are linked with a central data warehouse (DW) to record and report all daily financial transactions, offering reliable consolidated platforms can be referred to as integrated FMIS (or IFMIS).[37]

According to the U4 Anti-Corruption Resource Center:

> Emerging information and communication technology (ICT) can play an important role in fighting corruption in public finance systems by promoting greater comprehensiveness and transparency of information across government institutions. As a result, the introduction of Integrated Financial Management Systems (IFMIS) has been promoted as a core component of public financial reforms in many developing countries. Yet, experience shows that IFMIS projects tend to stall in developing countries, as they face major institutional, political, technical and operational challenges.[38]

IFMIS platforms can be vulnerable to a number of fraud and corruption schemes, such as the misallocation of budget items, processing of inflated payments to shell companies or phantom vendors, and payments to offshore accounts as part of a money laundering scheme.

There are a number of robust commercial fraud detection and prevention systems, discussed below, that can be installed in or linked to commercial IFMIS and ERP systems, such as SAP (see below).[39] These systems can provide continuous monitoring and ex ante alerts of potential fraud, many related to accounts payable transactions. Similar functions may be programed in homegrown systems, but the expense and technical difficulty of doing so may raise issues.

---

[37] See World Bank, "Financial Management Information Systems (FMIS)," https://www.worldbank.org/en/topic/governance/brief/financial-management-information-systems-fmis. Since 1984, the World Bank has financed 150 projects (108 completed, plus 39 that are active and three in the pipeline) in 82 countries totaling over US$4.930 billion for the design and implementation of FMIS solutions. The total amount of funds spent or allocated for FMIS projects is roughly US$5.952 billion, including borrower co-financing and other donor funds, and nearly US$2.379 billion has been spent for FMIS-related information and communications technology (ICT) solutions. As of January 2020, the total project cost (108 completed and 39 active) was roughly US$6.4 billion, including borrower co-financing.

[38] U4 Anti-Corruption Resource Center, "The Implementation of Integrated Financial Information Management Systems," U4 Expert Answer, April 8, 2009, https://www.u4.no/publications/the-implementation-of-integrated-financial-management-systems-ifmis/.

[39] Fifty-five percent of IFMIS platforms installed by the Bank in developing countries are commercial products, such as SAP; the remainder are homegrown.

## Potential fraud schemes in an IFMIS susceptible to digital fraud detection

Standard statistical methods are being applied to the field of fraud prevention in order to detect basic anomalies and more elaborate fraud schemes, for example, false expense reporting or false invoices or outlier transactions in procurement. Such techniques can detect when two procedures could not be performed during the same event, for example, or detect if the receipts are fraudulent or contain outlier values based on temporal, financial, or identification information. Data science, per se, is a vast field, so the modular approach to the implementation of an FMIS should be considered in order to adapt the best techniques to the data modeling. Although there are companies in the market that sell software aiming at flagging and detecting, or even forecasting, certain types of fraud, like false invoices, for example, inside the systematic approach innovation is incentivized. Considering that the IFMIS is embedded in an ecosystem, a multi-sided platform that can interact with other data from different sources, the work on each case offers an opportunity to expand the capabilities and the analysis over the entire system.

Not sticking to any method or algorithm but exploring open knowledge on the topic might keep the in-house solutions equivalent to those developed by the industry, since the market reveals innovative approaches to fraud detection every day. One of the tools to search for novelty algorithms, packages, and techniques is participation at the GitHub, a task-oriented platform where developers post recent software techniques to improve and share knowledge.

## Sample commercial anti-fraud products for an IFMIS

The commercial products listed below provide examples of sophisticated ex ante fraud detection and alert systems that can serve as models for similar programs installed in homegrown IFMIS and e-Procurement systems.

### SAP HANA Fraud Management

https://help.sap.com/saphelp_fra120/helpdata/en/72/1c65968bbe4cd4b157f62c5f2a4b34/frameset.htm

SAP Fraud Management is a solution that runs on the in-memory S4 HANA database. The system is programmed to detect, investigate, and prevent fraud in day-to-day processes, including order-to-cash, procure-to-pay, plan-to-product, request-to-service, and core capabilities.

SAP describes the benefits of the Fraud Management system as including:

a. Ex ante detection of potential fraud and anomalies in very high data volumes
b. Real-time alerts and the ability to block suspicious transactions
c. The ability to minimize false positives by adjusting the parameters of red flag detection formulas (For example, when looking for statistically significant and unexplained high prices and high-volume purchases, the price and volume thresholds can be adjusted to eliminate insignificant transactions.)
d. Tools for follow-up investigations, including network analysis visualization programs
e. Fraud prevention, using rules and predictive analytics to react to changing fraud patterns

f. Integrity screening of business partners and vendors, including politically exposed person (PEP) lists, corporate registration records, and access to corporate reputation websites
g. Money laundering detection methods, including payments to offshore accounts

The fraud management system can integrate with other transactional and analytical software, such as procurement and payment programs.

A SAP list of 50 detection methods for the detection and investigation of fraud in procurement, internal audit, and anti-corruption compliance can be found in the link below and in Annex B.

https://help.sap.com/doc/saphelp_fra120/1.2.1.0/deDE/27/46eb53bf7ca647e10000000a4450e5/content.htm?no_cache=true

More comprehensive, technical information on SAP Fraud Management and its detection methods can be found in the link below and Annex B. This information could be used to inform the installation of similar functions in a homegrown IFMIS.

https://help.sap.com/viewer/b6f43004b5bd4c9c919203f9d4a90f29/1.2.6.0/enUS/721c65968bbe4cd4b157f62c5f2a4b34.html

## Oversight Systems

Similar to SAP Fraud Management, Oversight Systems is an "AI powered" ex ante spend management and risk mitigation solution that links to the IFMIS, ERP, and other business management systems.

The system claims to provide, among other features:

a. Machine automation to perform audits of 100 percent of transactions less expensively, more quickly, and more accurately than human auditors working with only a small sample of transactions
b. Continuous monitoring capabilities to identify potential fraud and anomaly indicators and link them to specific employees, vendors, and transactions
c. Real-time, proactive alerts to system operators, which specify the indicator(s) detected, the potential wrongdoing they indicate, the steps to be taken to resolve the issues, and the management reporting requirements

The system covers the following business sectors:

a. Accounts payable: The system can identify discrepancies between purchase order information and invoicing, receiving and payment information, fraudulent, inflated, and duplicate invoices, inflated payments, and other questionable transactions
b. E-Procurement (limited to standard purchasing transactions, not tenders)
c. Travel and expense reimbursement
d. Purchasing cards
e. Fleet transactions;
f. General ledger transactions

For more information, see

https://www.oversightsystems.com/file:///Users/mikekramer/Desktop/Oversight%20Systems%20Blog.html.

A 21-minute demonstration video can be found at:

https://insideanalysis.com/markets/operational-intelligence/oversight-systems/.

## APPZEN

APPZEN is an AI cognitive machine learning audit and spend management app that links to an IFMIS and other business management systems. It provides services similar to SAP Fraud Management and Oversight Systems by identifying anomalies and possible fraud in accounts payable, travel and other expenses, and contract management.

Unique to APPZEN is the ability to deploy what it claims is AI technology to read and interpret written content in documents to identify anomalies and compliance issues. For example, the system can "read" the text in expense receipts to identify disallowed items.[40]

In addition, among other applications, APPZEN can automatically:

a. Check online reputation databases and watch lists for information on relevant firms and individuals
b. Extract key terms from contracts, such as pricing discounts, termination, and renewal dates
c. Verify work activity by automatically pulling and reading text from business emails, messages, system logs, and access records[41]

## GALVANIZE - ACL ESSENTIALS

Similar to SAP Fraud Management, Oversight Systems, and APPZEN, ACL Essentials is a suite of analysis apps that continuously assess ERP processes to identify red flags and fraud risks.

There are 14 prebuilt process controls:

Accounts Payable
Accounts Receivable
Cash Disbursements
Fixed Asset Management
General Journal Analysis
Human Resources Management
Procure-To-Pay
Purchase Order Management
Salaries & Payroll
Sales Analysis

---

[40] An illustration used by APPZEN is a meal receipt that lists "Grey Goose" as an itemized expense. The app can identify this as a vodka brand and disallow it as a reimbursable expense.
[41] More information can be found at:
https://www.appzen.com
https://www.appzen.com/blog/proactive-fraud-detection-the-future-is-artificial-intelligence-part-2/
https://venturebeat.com/2018/08/13/appzens-insights-uses-ai-to-automatically-detect-expense-reporting-fraud/

Segregation of Duties: Key Activities
Stock & Inventory Management
Travel & Entertainment Expenses
Vendor Management

Each of the above modules is available by itself or can be bundled in a mix-and-match solution. Details are available at:

https://help.highbond.com/helpdocs/essentials/6/user-guide/en-us/Content/global_topics/index.htm

### ACL robotic process automation

According to ACL, its robotics can be used to fully automate the testing of internal controls for compliance, without tedious recurring manual reviews, and can automate the vendor due diligence process to reduce third-party risk.[42]

Other GALVANIZE anti-fraud products can be found in Annex B and on this website:

https://www.wegalvanize.com/news-releases-acl/breaks-ground-robotic-process-automation-grc/

## XIII. Digital Detection of Fraud and corruption in Human Resources

This section focuses on the use of digital technologies to detect and prevent fraud and corruption in the human resource management (HRM) sphere of the public sector. It does so by first outlining the HR data that is typically collected and used by governments for public sector workers. This is followed by a discussion of the various incidences of fraud that can be prevented by using HR management information systems (HRMIS), with country examples provided where applicable. An important point to note here is that whereas there have been significant advances in using digital tools to monitor and prevent fraud and corruption using procurement and IFMIS platforms, there has been limited use of such technologies in the HR sphere. However, as this section will demonstrate, HR information systems present a novel opportunity for governments to expand existing systems strategically in the fight against corruption in the public sector.

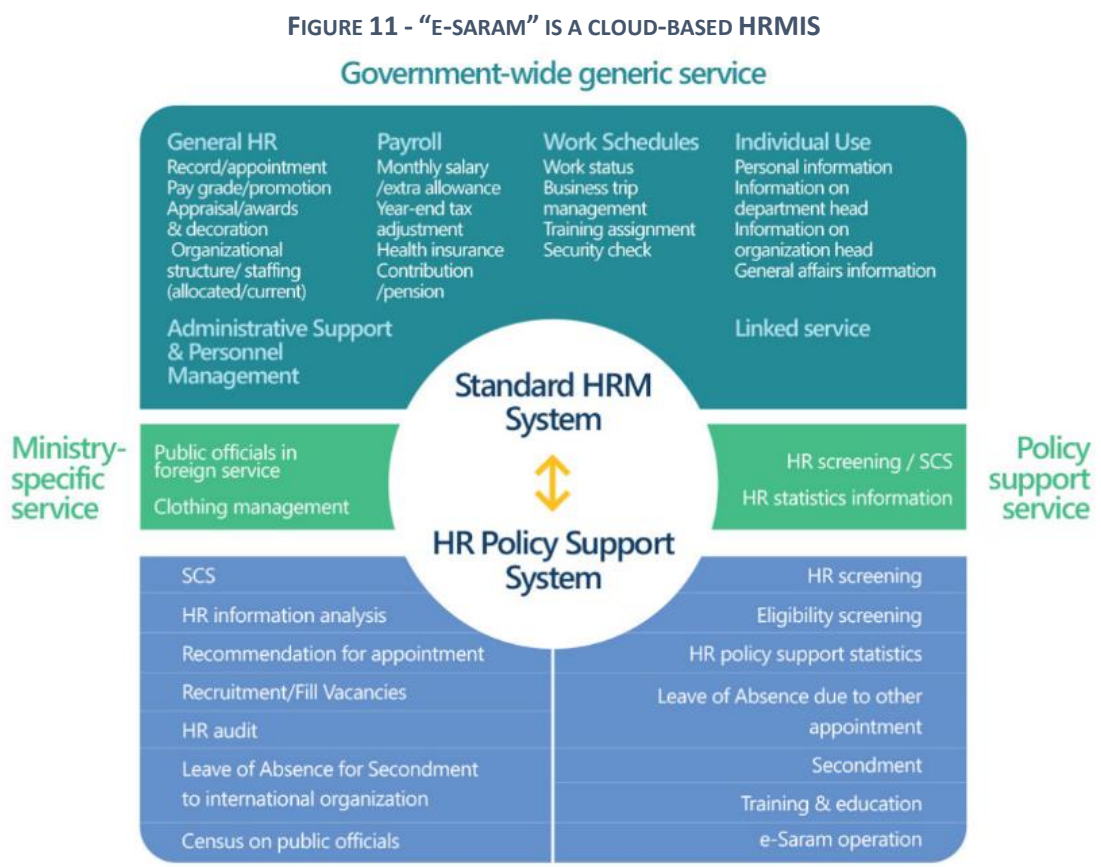
### Human resource management information systems (HRMIS)

Governments around the world often make use of HRMIS platforms to manage and support their personnel-related policies and operations. These systems may vary in their degree of sophistication and/or automation across countries. However, typically, they include key information on public sector employees such as staff biographical data, employment and compensation information, attendance

[42] An interesting example of the use of robotics comes from Brazilian project, Operação Serenata de Amor. It coded a robot capable of going through 2 million reimbursement claims made by members of Brazil's National Congress over 10 years in roughly one hour. The output was a list of several thousand suspicious reimbursements. The system freed human labor from manually auditing more than 99 percent of the data, allowing HR to focus on transactions with a higher likelihood of wrongdoing. See Y. Cordova and E. V. Goncalves, "Rosie the Robot: Social Accountability One Tweet at a Time," Governance for Development, The World Bank (blog), October 29, 2019, https://blogs.worldbank.org/governance/rosie-robot-social-accountability-one-tweet-time.

records, and performance evaluation information. Public sector agencies are able to make use of this data for a variety of personnel-related tasks, such as managing recruitment, performance evaluations, trainings, salaries, retirements, and so forth (see figure 2). An HRMIS can also be linked to other core government systems related to budgeting and accounting and can therefore serve as an essential tool in government decision making and public sector management.

**Figure 2. South Korea's Human Resource Management System**




"e-saram" is a cloud-based HRMIS that supports government-wide personnel administration and personnel policy tasks from recruitment to retirement.[43]

## Fraud and corruption in HR

The 2016 Global Fraud Survey found that the second highest number of occupational fraud cases were found in the government sector, after banking and financial services (ACFE 2016). Further, according to the 2013 Transparency International Global Corruption Barometer, 88 percent of survey respondents reported that corruption was a "serious" or "very serious" problem in their country's public sector.[44] At

[43] South Korea, Ministry of Personnel Management, http://www.mpm.go.kr/english/system/eSaram/.

[44] This information is available at https://govdata360.worldbank.org/indicators/hfbe3491a?indicator=32627&viz=bar_chart&years=2013.

the same time, most corruption investigations within public administration currently rely on traditional audit procedures or tips from whistleblowers. Digital tools and AI can help make this process more effective by uncovering patterns of systemic corruption and by identifying potential corruption risks before they become entrenched (CAPI 2017). The following sections discuss some of the key HR dimensions where fraud and corruption may occur and the ways in which digital tools can be adapted to detect and prevent them.

## Recruitment and promotion decisions

Recruitment and promotion decisions in the public sector should be based on merit and job requirements. However, around the world, government jobs are often awarded on the basis of favoritism or nepotism. In addition, candidates may sometimes provide false educational records or not disclose all relevant background information related to criminal records, civil lawsuits, or other administrative actions. Governments can employ algorithms as an add-on to an existing HRMIS to cross-reference data elements and raise red flags with regard to recruitment and promotion decisions. For example, the algorithm could raise a red flag if an unusually high number of appointments are made by the same person or if a significant number of newly created positions originate from a single individual. The algorithm could also detect commonly occurring family names or similar addresses to flag potential familial relationships that may indicate nepotism in hiring and promotion decisions (CAPI 2017). Governments may automate background checks, linking employee records to academic registries and police reports to flag any issues with regard to false diplomas or criminal history. Algorithms could also be designed to check internal government records to ensure that employees who have been awarded new positions or other promotions actually meet the minimum education, training, and years of service requirements.

Additional ways in which digital technologies can be used to decrease the occurrence of fraud and corruption in the recruitment process and promote greater overall transparency include the use of artificial intelligence in the screening process. Cognitive solutions can help organizations tap into multiple data sources and reveal new insights for better candidate profiles and to improve the hiring and recruiting process. Tools such as Evolv and TalentBin allow employers to find the best person for any given job based on their skills, interests and actions. In addition, vendors such as LinkedIn are increasingly offering big data and AI tools to sift through candidate profiles and identify the most suitable people for a position. Although these tools have most been utilized in the private sector so far, there is increasing scope for their use in the public sector as well.

## Employee identification and attendance

Chronic absenteeism and “ghost workers” (see below) are a significant challenge in public sectors across the developing world. For instance, in India, estimates suggest that roughly one-quarter of government teachers and over one-third of government doctors in primary health centers are absent without a legitimate reason on any given day (World Bank 2016, 168). This represents both a loss of money for the government as well as substandard public administration capacity and service delivery. Physical monitoring of service providers can be costly and may produce limited results if monitors themselves shirk their duties or collude with government service providers, as has been reported in several country cases.

Digital tools can fill this monitoring gap. For example, Nigeria’s digital ID system revealed 62,000 “ghost workers” in the public sector and saved the government an annual US$1 billion. In Guinea, the

government enrolled all civil service employees in a biometric identification system to identify and eliminate fictitious positions, saving the government potentially up to US$1.7 million (World Bank 2019d). Other countries have set up biometric scanning machines at all entrances to government offices and require employees to scan when they arrive and leave as a way to monitor attendance. This data is then fed into the employee-level attendance records maintained under the central HRMIS. The system is able to generate red flags when employees are chronically absent or miss regular working hours. Governments may also design and add on algorithms to their HR management systems to run iterative tests on public employee records and raise red flags. For example, the system could flag duplicate employee records or match payroll and HR records to flag inconsistencies or suspicious gaps indicating misuse of funds or staff time.

**FIGURE 12 - SIERRA LEONE CASE EXAMPLE**

According to a 2008 study by the International Records Management Trust (IRMT), Sierra Leone announced that it had reduced the number of ghost employees by 20 percent after the installation of an IFMIS that contained an HR management module. The report by IRMT revealed that most of the necessary steps to identify and remove the ghosts were done by manual document collection, reviews, and interviews before being entered into the IFMIS HR module. This is a useful illustration of the limitations of automated systems and the need to integrate them with traditional methods. The report can be found at: http://www.irmt.org/documents/building_integrity/case_studies/IRMT_Case_Study_Sierra%20Leone.pdf.

## Employee compensation

In addition to "ghost workers" who may be receiving government salaries and perks without showing up to their jobs, many employees may also be "double-dipping," that is, receiving multiple pay checks or receiving allowances and other benefits for which they are not eligible. Algorithms can be designed to cross-check HR and payroll records to identify compensation fraud. For example, the system could flag employees who use a post office box or mailbox as their home address, are issued multiple paychecks within a single pay period, or are paid bonuses during times when bonuses are not typically paid out. In addition, the system could link salary and allowance records to eligibility criteria as set out in civil service regulations and flag any employees who receive base salaries or allowances for which they are not eligible per their grade level or job classification. Similar checks may also be carried out on the logging of overtime or travel expense reports, for example, if employees are logging unusually high weekend overtime or if overtime is taken without the approval of supervisors or managers.

## Bribes and conflicts of interest

Petty corruption in the form of bribes as well as grand corruption in the form of beneficial ownership and conflicts of interest continue to pose a challenge in many public sectors around the world. As table 1 below demonstrates, a significant number of citizens living in a diverse set of countries report having paid a bribe to access such basic services as education, public health, police support, land registration, utilities, and more. Through the use of big data and AI, governments can design add-on algorithms for their HR management systems to help detect employees who may be guilty of receiving bribes or personally benefiting from government procurement and awarding of contracts. HR and payroll records could be matched against bank account transactions above a certain currency level, tax filings, or other income disclosure documents to flag suspicious levels of income or money transactions. Employee records could also be cross-referenced against vendor data to detect recurring family names or addresses to ensure that employees do not use access to government procurement information for personal or familial business gain. For example, in Romania, the government has introduced an integrated electronic procurement system that flags potential conflicts of interest before a contract is awarded. The system cross-checks e-Procurement information to check whether bidders are related or in any way connected to public officials handling the procurement and generates a risk rating for each tender. The system is linked and therefore able to query records related to public asset declarations of government officials and data on bidders (Pușcaș 2017).

**FIGURE 13 - PERCENTAGE OF PEOPLE WHO PAID A BRIBE TO ACCESS PUBLIC SERVICES, 2013**

| | |
|---|---|
| Sierra Leone | 84 |
| Kenya | 70 |
| Cambodia | 57 |
| India | 54 |
| Morocco | 49 |
| South Africa | 47 |
| Mongolia | 45 |
| Bangladesh | 39 |
| Egypt | 36 |
| Vietnam | 30 |

*Source*: Global Corruption Barometer.[45]

## Key lessons

The above sections describe common examples of HR-related fraud and corruption in the public sector and offer innovative digital approaches to addressing them. Digital tools, big data, and AI present enormous potential in the fight against fraud and corruption in the public sector, and governments can and should seize this emerging opportunity. At the same time, some key lessons should be kept in mind:

1) Country case studies show that fraud detection using rules-based algorithms or cognitive machine learning is most effective when it is applied in areas identified beforehand as being susceptible to corruption based on investigations carried out by human auditors (Aarvik 2019).

2) It is important to note that any IT system or algorithm that may be developed will need to be complemented with traditional human measures. For instance, an algorithm may flag some cases as fraud, but the discrepancy may be due to human error in record keeping. These kinds of challenges are common in public sectors around the world and should not be overlooked when dealing with algorithms and the HR data on which they are based.

[45] Transparency International, "Global Corruption Barometer," https://www.transparency.org/research/gcb.

# XIV. Other Sectors of Possible Digital Fraud Detection and Prevention

A report by the U4 Anti-Corruption Research Center, "Artificial Intelligence – a Promising Anti-Corruption Tool in Development Settings?" identified a number of interesting AI initiatives, including programs to identify the risk of corporate tax evasion, fraud, and corruption in international aid projects and by civil servants (Aarvik 2019).

Other sectors that can be addressed by anti-fraud digital technology include (In alphabetical order):

Accounts payable
Application for permits
Banking
Construction
Customs
e-Commerce
Eligibility for government benefits and disability claims
Emergency benefits claims (hurricane, flood damage, etc.)
Health care (billing codes and services)
Inspections
Insurance claims (health, property and casualty claims, etc.)
Retail frauds
Payments to individual beneficiaries in humanitarian and other aid projects
Tax and revenue collection

# XV. Summary of Challenges to the Successful Implementation of Digital Anti-Fraud Solutions

As mentioned above, there are significant challenges to the successful implementation of the digital anti-fraud programs discussed above. Primary among these are:

1. The lack of political will to implement the anti-fraud measures where they are needed the most, or to take the necessary steps to sanction misconduct when discovered
2. Lack of local digital expertise and resources to install, operate, and maintain the systems
3. Lack of availability and access to the necessary data; poor data quality; incomplete or erroneous data entry; the need to clean and harmonize data before it can be used
4. Cyber security, data security, and integrity issues. Systems can be hacked to change or delete information, including submitted bids in e-Procurement, vendor records in IFMIS, and salary information in HR systems. Hackers also can override controls and standards procedures; utilizing blockchain technology may help to prevent these abuses.
5. Risk of capture or monopolization of data by corrupt officials who may have exclusive access to the digital systems, particularly the IFMIS; the officials can use this to abuse the procedures and prevent review by outside parties
6. The existence of data privacy laws and regulations that may deny access to necessary data, especially when conducting background checks or collecting employment history data

7. “Algorithm bias”: Algorithms may reflect the biases inherent in the data sets from which they are created, resulting in rules that are unfair or unreasonable. For example, on what basis was a company or individual targeted for investigation? Was it fair or biased? How does the e-Procurement system or Governance Filter evaluate bids and assign winners? Why are bidders excluded in ex ante systems?
8. A related issue arises when the basis for the design of an algorithm cannot be determined (the “black box” problem), or when the responsibility and accountability for the design cannot be established, denying aggrieved parties the ability to challenge the algorithm
9. Inadequate IT project management skills, a much bigger problem than imagined. Successful anti-fraud IT solutions require the following combination of knowledge and skills—and the ability to clearly communicate them to the other team members:
    - The client’s specific needs and expectations
    - Anti-fraud expertise to identify the desired fraud detection and prevention requirements (knowledge of the appropriate indicators and algorithms, etc.)
    - IT expertise that can identify and implement the appropriate solutions
10. An uncertain legal and regulatory environment, for example, absent or unclear enabling legislation and regulations for e-Procurement and IFMIS systems, uncertainty regarding the admissibly of electronic evidence, etc. [46]
11. The need for training for procurement personnel, auditors, investigators, and other anti-fraud professionals on digital anti-fraud measures and follow-up steps
12. The need for investigative agencies that have the capacity, will and independence to follow up with traditional investigative methods, and sanction systems that can be applied against even upper level officials, both of which are absent or severely limited in many developing countries

For more information, see Aarvik (2019).

[46] Questions regarding the admissibility of electronic evidence from e-Procurement or IFMIS systems are frequently cited in the literature. It should be noted, however, that the digital fraud detection methods discussed in this paper identify “indicators” of possible fraud, not evidence that is intended to be offered in court. Admissible evidence will be generated by the follow up investigation using mostly traditional methods.

# Annex A: Detailed Information on Procurement Fraud Red Flags, Data Requirements, and Follow-Up Steps

The sample indicators in the sections below are prioritized and color coded as follows for application in ex ante detection systems.

RED: Real-time BLOCKS or ALERTS of apparent improper transactions, e.g., a bid submitted by a debarred company or different bids from the same IP address

BROWN: Pre-programmed REPORTS for other common procurement fraud schemes, waste, or abuse

ORANGE: Other less common reports that can be listed in a HANDBOOK or ONLINE GUIDE for auditors, investigators, or other users

BLUE: Links to online public records, including telephone and address information

Both the "primary data sources" and "other potential data sources" listed for each scheme should be readily available from any e-Procurement system. The primary data requirements refer to the information needed to identify the most significant indicators. Other potential data sources refer to the information needed to identify useful but less critical indicators.

## Collusive bidding

Secret agreements by bidders or suppliers to divide work and artificially inflate prices, often with the complicity of government officials.

Indicators subject to digital detection include:

- Different bids from the same IP address
- Bidders with the same contact information
- Unusual bid patterns, e.g., bids an exact percentage apart
- Sequential bid securities
- Same bidder's rebid in same order in later rounds
- High price bids, e.g., bids that exceed the confidential owner's estimate by > 30 percent
- Pattern of rotation of winning bidders
- Same bidders always bid, win, and lose
- Losing bidders become subcontractors
- Unusual bid patterns, e.g., "6-9-17 bid pattern"
- Bids not in conformity with prior legitimate bid patterns
- Distant bidders that are cheaper than local bidders
- Losing bidders that cannot be located in corporate registries or directories or on the internet

### Data requirements

Primary data sources

- Bidder's address, telephone, fax, email, IP address
- Winning and losing bids
- Bid securities
- Owner's cost estimates

Other potential data sources:

- Line item prices
- Subcontracts
- Previous bids

The charts below illustrate the bid patterns associated with legitimate bids and bids rigged as the result of collusion among bidders. The top chart shows an irregular but plausible distribution of bid prices from seven bidders. The bottom two charts show bids that are an exact percentage apart, an indicator of collusion.

**FIGURE 14 - SAME GRAPHIC REPORTS OF COLLUSIVE BIDDING INDICATORS**

Sample Graphic Reports of Collusive Bidding Indicators

Blue and orange highlighted bids indicate potential collusion

**Jobsite: East African Network Tollroad**

| Bidder | Bid | Ratios of Bid to Estimate | Ratios of Bid to Winner | Ratios of Bid to Prev Bid |
|---|---|---|---|---|
| Engineer Estimate | $ 132.7M | - | - | - |
| Barrytron | $ 130.9M | -1.4% | - | - |
| Tessier-Ashpool | $ 135.8M | 2.4% | 3.8% | - |
| Stay Puft Corporation | $ 136.6M | 2.9% | 4.3% | 0.5% |
| Barrytron | $ 138.5M | 4.4% | 5.8% | 1.4% |
| Galaxy Corp | $ 140.8M | 6.1% | 7.5% | 1.6% |
| 123 Warehousing | $ 144.1M | 8.6% | 10.1% | 2.4% |
| Spade and Archer | $ 157.1M | 18.3% | 20.0% | 9.0% |

**Jobsite: Rila motorway Development**

| Bidder | Bid | Ratios of Bid to Estimate | Ratios of Bid to Winner | Ratios of Bid to Prev Bid |
|---|---|---|---|---|
| Engineer Estimate | $ 109.3M | - | - | - |
| Carrys Candles | $ 102.0M | -6.7% | -22.2% | - |
| General Services Corporation | $ 131.2M | 20.0% | - | - |
| The Legitimate Businessmens Club | $ 137.7M | 26.0% | 5.0% | 5.0% |
| Flowers By Irene | $ 140.3M | 28.4% | 7.0% | 1.9% |
| Allied Biscuit | $ 143.0M | 30.8% | 9.0% | 1.9% |
| United Fried Chicken | $ 145.6M | 33.2% | 11.0% | 1.8% |
| Acme Corp | $ 148.2M | 35.6% | 13.0% | 1.8% |

**Jobsite: I-85/West Point Interchange Project (Troup County)**

| Bidder | Bid | Ratios of Bid to Estimate | Ratios of Bid to Winner | Ratios of Bid to Prev Bid |
|---|---|---|---|---|
| Engineer Estimate | $ 122.6M | - | - | - |
| LexCorp | $ 137.8M | 12.4% | - | - |
| Krustyco | $ 141.3M | 15.3% | 2.6% | - |
| General Services Corporation | $ 151.5M | 23.6% | 10.0% | 7.2% |
| Sixty Second Avenue | $ 166.7M | 36.0% | 21.0% | 10.0% |
| Smith and Co. | $ 183.3M | 49.6% | 33.1% | 10.0% |
| LuthorCorp | $ 201.7M | 64.6% | 46.4% | 10.0% |

For more information on collusive bidding and follow-up steps, see https://guide.iacrc.org/potential-scheme-collusive-bidding/.

## Bid rigging

Bid rigging is the improper manipulation of the bidding or vendor selection process to favor certain bidders to the exclusion of others.

Indicators include:

- Procurement official's contact information is same as bidder's contact information
- Shorter notice to submit bids than rules require
- Sole source awards greater than sole source limits
- Split purchases
- Multiple purchases just below procurement threshold
- Award to only one evaluated bidder
- Award to other than the low bidder
- Unusually high line item bid, followed by change order increasing quantities
- Unusually low line item bid, followed by change order removing or reducing line item
- Winning bid price the same as cost estimate

### Data requirements

Primary data sources:

- Bid evaluation committee members and bidder contact info
- Winning and losing bids
- Bid notice and due date
- Debarment list
- Procurement thresholds

Other potential data sources:

- Line item bid prices
- Contract date and price
- Change orders and amounts
- Procurement plan information
- Previous similar tender results

For more information on all eight common bid-rigging schemes and follow-up steps, see https://guide.iacrc.org/potential-scheme-bid-rigging/.

## Corruption - bribes and kickbacks

Indicators include:

- Bid-rigging indicators, above
- SPQQD indicators

SPQQD refers to the following factors regarding a procurement from a particular contractor or vendor:

- Irregularities in the SELECTION of the contractor or vendor
- The payment of unexplained high PRICES
- The purchase of excessive QUANTITIES of goods, works, or services
- The acceptance of low QUALITY goods, works, or services
- The DELIVERY and acceptance of such items that do not match the purchase order or contract requirements
- Family or personal connections between the related procurement official and a contractor or vendor
- Sudden, unexplained wealth by the related procurement official

A pattern of SPQQD abuses over time by a particular contractor or vendor and procurement official is particularly significant.

### Data requirements

See bid rigging, above.

## Shell company vendor

These are vendors that are secretly owned by procurement agency officials.

Indicators include:

- Vendor located at a non-business address or not listed on the internet
- HR/vendor matches (employee and vendor list the same cell phone number, etc.)
- Vendor not on approved vendor list
- Sole source purchases above competitive threshold
- Multiple purchases just below competitive threshold
- Split purchases
- Segregation of duties violations (same person orders, approves, and receives purchases)
- SPQQD factors present
- Vendor provides variety of disparate goods or services in contrast to existing vendor norms (per vendor codes and product codes)
- Prompt payment in contrast to the existing payment norm

### Data requirements

Primary data sources:

- Vendor master file
- HR master file
- Purchase order, receiving, invoice, payment information
- Procurement thresholds
- Segregation of Duties requirements

Other potential data sources:

- Benchmark prices
- Vendor and product code lists
- Payment date

For more information on shell company vendors and follow-up steps, see https://guide.iacrc.org/potential-schemes-hidden-interests/.

## Phantom vendor

Also known as ghost suppliers, these are fictitious vendors set up by insiders to embezzle funds.

Indicators include:

- Vendor not listed in corporate registries or directories or on the internet
- Vendor located at non-business address
- Paid vendor not on approved vendor List
- HR employee record/vendor record match
- "Fuzzy match" vendors with different bank accounts
- High number or percentage of sequential invoice numbers
- Broken sequence invoice numbers
- Purchases just below competitive thresholds
- Split purchases
- Benford's Law violations
- Small initial purchase
- Vendor provides hard-to-verify goods, works, or services (per product code)

### Data requirements

Primary data sources:

- Approved and paid vendor lists
- HR and vendor master files
- Purchase order, invoice, receiving, payment information

Other potential data sources:

- Procurement thresholds
- Benford's Law distributions
- Vendor and product code lists

For more information on phantom vendors and follow-up steps, see https://guide.iacrc.org/potential-scheme-fictitious-contractor-2/.

## Purchases for Personal Use, Resale, or Diversion

This is a very common abuse that can be quite costly if not adequately monitored and controlled.

Indicators include:

- Purchase of inappropriate personal "consumer items" per product code
- Purchased items not in inventory

- Different “ship to” address
- Split purchases
- High number of purchases of certain items susceptible to personal use (laptops, tires, gas, etc.)
- Returns without credits
- Multiple purchases just below thresholds
- Small initial purchase
- Incomplete information on purchase order or invoice
- Purchased items, volumes differ from procurement plan
- Employee has outside business (used to resell or divert products)

### Data requirements

Primary data sources:

- Vendor product codes
- Purchased item product codes
- Purchase order, invoice, and receiving records information
- Procurement thresholds

Other potential sources:

- Returns and credits
- Inventory records
- Procurement plan information

## False, inflated, and duplicate invoices

Whether done intentionally or inadvertently, this is a common problem that can be quite costly if not controlled.

Indicators include:

<u>False invoices:</u>

- Invoice information does not match purchase order, receiving, or payment information
- Sequential invoice numbers
- Broken sequence invoice numbers
- Outliers in price, quantity
- Benford’s Law violations
- Missing information on invoice

<u>Inflated invoices:</u>

- Invoice price, quantities greater than the purchase order price, etc.
- Total payments greater than total invoice amounts

<u>Duplicate invoices:</u>

Invoices with same number, dates, quantities, item description, or amounts

## Data requirements

Primary data sources:

- Purchase order, invoice, receiving, and payment information, including:
  - Dates
  - Invoice numbers
  - Item number, descriptions
  - Product codes
  - Price and quantities
  - Receiving information
  - Payment amount
- Other data sources:
  - Benford's Law distributions

For more information on false, inflated, and duplicate invoices and follow-up steps, see https://guide.iacrc.org/potential-scheme-false-inflated-and-duplicate-invoices/.

# Annex B: Information on IFMIS Fraud Detection Applications

## Overview of detection methods in SAP Fraud Management

SAP provides over 50 detection methods as standard business content for the detection and investigation of fraud scenarios in procurement and internal audit and for anti-corruption compliance. The business content is ready to use and provides a starting point for additional content. The standard scenarios and detection methods are shown in the following tables.

## Irregularities in Accounting Documents

| Used to Find ... | Documentation Link |
|---|---|
| Accounting documents that were posted on exceptional dates | Detection Method: Accounting Documents Posted on Non-Working Day |

## Irregularities in Outgoing Payments

| Used to Find ... | Documentation Link |
|---|---|
| Creditors that are located in high-risk countries | Detection Method: Payment to High-Risk Country |
| Creditors or debtors with a bank account that is located in a high-risk country | Detection Method: Bank Account in High-Risk Country |
| Payments that are made to business partners who are located in high-risk countries | Detection Method: Business Partner Address in High-Risk Country |
| Large payments that were divided up into smaller payments (also called smurfing) | Detection Method: Accounting Document Line Item Smurfing |
| Customers who are located in a high-risk country | Detection Method: Customer Located in a High-Risk Country |
| Any changes to customer master data | Detection Method: Changes to Customer Master Data |
| Customers who have bank account located in a high-risk country | Detection Method: Customer Bank Account in High-Risk Country |
| Customers whose bank location differs from their location | Detection Method: Customer and Bank Location Differ |
| Cases in which the paying customer is different from the invoiced customer | Detection Method: Paying Customer Differs from Invoiced Customer |
| Split payments of invoices (smurfing) | Detection Method: Customer Invoice Irregularities (Split Invoice) |
| Suspicious terms in customer invoice items | Detection Method: Suspicious Terms Screening for Customer Invoice |

## Irregularities Concerning New Vendors

| Used to Find ... | Documentation Link |
|---|---|
| New vendors whose turnover in the first year exceeds a specific threshold | Detection Method: Turnover of New Vendor in First Year Exceeds Threshold |

| | |
|---|---|
| New vendors that have a suspiciously high turnover growth between the first and second years | Detection Method: Growth Between 1st and 2nd Year Exceeds Threshold |
| New vendors that have a large percentage of their turnover approved by a single employee | Detection Method: Percentage of Turnover Approved by a Single Person |

## One-Time Accounts (One-Time Vendor)

| Used to Find ... | Documentation Link |
|---|---|
| Bank accounts that were used multiple times in one-time accounts | Detection Method: Multiple OTA Postings to Same Account |
| One-time bank accounts that also belong to a regular vendor | Detection Method: OTA Uses Bank Account of Regular Vendor |
| One-time accounts that already exist as regular vendors | Detection Method: Duplicate Regular Vendor and One-Time Vendor |

## Irregularities in Purchase Orders and Purchase Order Items

| Used to Find ... | Documentation Link |
|---|---|
| Purchase orders that have had an excessive number of changes | Detection Method: Multiple Changes on Purchase Orders |
| Purchase orders containing addresses that are on sanctions or politically exposed persons (PEP) lists | Detection Method: Address Screening for Politically Exposed Persons |
| Purchase order items that have a vendor located in a high-risk country | Detection Method: Purchase Order Item with Vendor from High-Risk |
| When the invoice receipt quantity is greater than the goods received quantity | Detection Method: Purchase Invoice Greater Than Goods Received |
| When the amount paid in an invoice is greater than the amount shown in the relevant purchase order item | Detection Method: Purchase Order Overpaid |

## Irregularities in Vendor Data and Transactions

| Used to Find ... | Documentation Link |
|---|---|
| Vendors whose bank data has been changed and then reverted to the original data (flip-flop bank data) | Detection Method: Vendor Bank Data Change (Flip-Flop Vendor) |
| Vendors whose alternative payee field has been changed and then reverted to the original state (flip-flop payee) | Detection Method: Alternative Payee (Flip-Flop Payee) - Cross Company Code |
| Vendors whose alternative payee field has been changed and reversed within one single company code | Detection Method: Alternative Payee (Flip-Flop Payee) - Company-Code Specific |
| Employees who have the same bank data as regular vendors | Detection Method: Employees with Same Bank Data as Vendor |
| Vendors that have no banking details recorded in the vendor master data | Detection Method: Vendor Without Bank Details |

| | |
|---|---|
| Vendors that are located in high-risk countries | Detection Method: Vendor Address in High-Risk or Embargo Country |
| Vendor invoice items with regular or one-time vendors that are located in a high-risk country | Detection Method: Vendor in Invoice Item in High-Risk Country |
| Vendors whose address is a post office box or incomplete | Detection Method: Vendor Address Suspicious |
| Vendors that have no phone number or the phone number is located in another country | Detection Method: Vendor Telephone Number Suspicious |
| Vendors that are paid prematurely, relative to the average days sales outstanding (DSO) | Detection Method: Vendor DSO Shorter than Company Average DSO |
| Vendors whose bank account is located in a high-risk country | Detection Method: Vendor Bank Account Located in High-Risk Country |
| Vendors whose bank is located in a different country than they are | Detection Method: Vendor and Bank Countries Differ |
| Vendors with similar bank accounts | Detection Method: Vendors with Similar Bank Accounts |
| Duplicate invoice reference numbers for a single vendor | Detection Method: Duplicate Invoice with Same Approver 1 |
| Duplicate invoices that were approved by the same person | Detection Method: Duplicate Invoices with Same Approver 2 |
| Duplicate invoices that have the same vendor ID or value added tax (VAT) number | Detection Method: Duplicate Invoices |
| Invoices that do not have corresponding purchase orders | Detection Method: Invoice Without Purchase Order Reference |
| Invoice items that are split into smaller payments, whose sum exceeds a certain threshold | Detection Method: Split Invoices Exceed Limit |
| Vendors that have a high percentage of invoices with rounded amounts | Detection Method: Round Invoice Amounts Above Threshold for Vendor |
| New invoices for inactive vendors | Detection Method: New Invoices to Inactive Vendors |
| Payments that were made to banks in a country other than that of the vendor in the invoice | Detection Method: Divergent Vendor and Payment Country |
| Manual payments to a vendor | Detection Method: Manual Payment to a Vendor |
| When a vendor was paid too early | Detection Method: Vendor Payments Too Early |
| Payment proposals to which manual changes have been made | Detection Method: Manual Change to Payment Proposal |
| Vendor invoice items that have suspicious terms | Detection Method: Suspicious Term Screening for Vendor Invoice Items |
| Vendor invoice items that have similar amounts | Detection Method: Vendor Invoices with Similar Amounts |
| Blocked vendors that have active duplicates | Detection Method: Find Duplicates of Blocked Vendors |
| Vendors that have C/O in their address | Detection Method: Vendor with "Care Of" in Address |
| Vendors that have similar names | Detection Method: Vendors with Similar Names |

## Irregularities in Travel Expenses

| Used to Find ... | Documentation Link |
|---|---|
| An employee who has submitted and reused receipts on more than one travel expense | Detection Method: Duplicate Travel Expense Claim Made by One Employee |
| An employee who has filed travel expenses with unusually rounded amounts above a certain threshold | Detection Method: Travel Expenses with Rounded Amounts |
| An employee who has suspicious trends in his/her trip expenses | Detection Method: Suspicious Trend in Trip Expenses |

## Other technical information on Sap Fraud Management and detection scenarios

Generic Content for SAP Fraud Management

Content for Internal Auditing and Anti-Corruption Compliance

eCATTs for Creating Detection Methods and Detection Strategies

Overview of Detection Methods in SAP Fraud Management

Detection Scenarios and Detection Methods

Detection Scenario: Irregularities in Accounting Documents

Detection Scenario: Irregularities in Outgoing Payments

Detection Scenario: Irregularities in Travel Expenses

Detection Scenario: Irregularities in Customer Transactions and

Detection Scenario: Irregularities Concerning New Vendors

Detection Scenario: Irregularities in One-Time Vendor Accounts

Detection Scenario: Irregularities in Purchase Orders and Purchase

Detection Scenario: Irregularities in Vendor Data and Transaction

Detection Method: Vendor Bank Data Change (Flip-Flop Vendor)

Detection Method: Alternative Payee (Flip-Flop Payee) # Cross Co

Detection Method: Alternative Payee (Flip-Flop Payee) # Company-

Detection Method: Duplicate Invoice with Same Approver 1

Detection Method: Duplicate Invoices with Same Approver 2

Detection Method: Round Invoice Amounts Above Threshold for Vend

Detection Method: Duplicate Invoices

Detection Method: Split Invoices Exceed Limit

Detection Method: Suspicious Term Screening for Vendor Invoice I

Detection Method: New Invoices to Inactive Vendors

Detection Method: Invoice Without Purchase Order Reference

Detection Method: Vendor Invoices with Similar Amounts

Detection Method: Divergent Vendor and Payment Country

Detection Method: Vendor in Invoice Item in High-Risk Country

Detection Method: Vendor Payments Too Early

Detection Method: Manual Payment to a Vendor

Detection Method: Vendor DSO Shorter than Company Average DSO

Detection Method: Find Duplicates of Blocked Vendors

Detection Method: Employees with Same Bank Data as Vendor

Detection Method: Vendor with "Care Of" in Address

Detection Method: Vendors with Similar Names

Detection Method: Vendor Address in High-Risk or Embargo Country

Detection Method: Vendor Address Suspicious

Detection Method: Vendor Telephone Number Suspicious

Detection Method: Vendor Without Bank Details

Detection Method: Vendor Bank Account Located in High-Risk Count

Detection Method: Vendor and Bank Countries Differ

Detection Method: Vendors with Similar Bank Accounts

Detection Method: Manual Change to Payment Proposal

# Galvanize Anti-Fraud and GRC Solutions

## FraudBond

FraudBond is an overall fraud management solution that claims to:

- Provide oversight over ERP controls
- Assess and monitor control weaknesses
- Apply advanced analytics and machine learning to identify high-risk trends and activities

- Consolidate regulations and standards to manage anti-bribery and anti-money laundering compliance programs
- Flag violations, automate follow up, and notify stakeholders
- Record, investigate, and report on fraud tips from anonymous whistleblower hotlines

https://view.highspot.com/viewer/5e2f1873811717230896f336

## HighBond

FraudBond is a product in the HighBond platform, a comprehensive enterprise GRC (governance, risk, and compliance) software platform for anti-fraud, risk management, and compliance purposes.

Other products in the HighBond suite include:

| **Product** | **Description** |
|---|---|
| AuditBond | an audit management solution that helps organizations improve efficiency across their entire audit workflow, from planning to reporting |
| ComplianceBond | a compliance management solution that helps organizations implement, automate, and demonstrate assurance over a compliance program |
| ControlsBond | an internal controls management solution that helps organizations manage and automate their internal controls program |
| RiskBond | a risk management solution that helps organizations identify, assess, respond to, and monitor enterprise risks |
| ACL Robotics | a continuous monitoring solution that helps organizations automate time-intensive and repetitive but nevertheless critical business processes |

https://www.wegalvanize.com/highbond/

# Annex C: Information on Human Resources Fraud Detection Applications

The most common and costly schemes in HR include payments to ghost employees, inflated salary and expense payments, nepotism, conflicts of interest, and the hiring of unqualified candidates due to patronage schemes and inadequate controls. These offenses can lead to grossly inflated payrolls and incompetent government employees and be a huge burden in many developing economies.

ACL Essentials, discussed above, offers apps that continuously assess critical HR and travel and expense functions in ERP systems to identify fraud risks and red flags. See Human Resources Management; Travel & Entertainment Expenses. Research for this report did not reveal any other commercial fraud detection apps dedicated to HR programs.

The schemes discussed below, however, can be effectively addressed with homegrown solutions by digitizing and cross-referencing HR data rosters, attendance records, time sheets, benefits, and so on, as illustrated below.[47]

## Definition of "ghost employees"

"Ghost employees" refer to entirely fictitious employees or registered employees who do not report for work. They can be detected by the algorithms described below.

## Data requirements to detect ghost employees

All of the data listed below may not be necessary or available in the subject employment system.

The most important data points are the payroll registers and HR master files.

a. Establishment information: budget and staffing information
b. Information from the Payroll Register:
    - Employee:
        - Name
        - ID number
        - Address
        - Telephone (include cell phone)
c. Information from the HR master file
    - Employee:
        - Name
        - ID number
        - Address
        - Telephone (include cell phone)
        - Employment application
        - Letters of appointment
        - Medical certificates

[47] The tests suggested here illustrate the most fundamental principal in fraud detection, digital or traditional: The essence of fraud detection is not the collection, but the ***intelligent cross-referencing*** of the relevant information.

    - CVs and educational credentials
    - Tax withholding information
    - Payroll deductions: health benefits information
    - Emergency contact information
    - Hiring and termination dates

d. Time and attendance sheets
e. Access badge usage, computer log-in information
f. Employee bank account and payment information
g. Employee government identification records (import records)
h. Government death records

## Methods to detect ghost employees

To the extent feasible, digitize the above records, then query the records as listed below to identify fictitious employees:

a. Cross reference payroll and HR records; look for "employees:"
    - On the payroll register who are not listed in HR files
    - On the payroll register prior to their recorded start date or after their termination date
    - With no deductions for taxes or benefits (no withholdings)
    - With no pay increases, or more than two pay increases, within a year
    - With no paid time off, no vacation, no sick leave used
    - With a high ratio of gross to net pay on employee salary and tax records (this can identify those employees with low or no withholding amounts)
    - With the same home address
    - Who have either a post office box or a mail drop for their address
    - With blank address or other contact information fields
    - With blank contact information or government ID fields
    - With more than one address change within a year

Also look for:

a. Non-salaried employees on the payroll register but not in the time-keeping system
b. Multiple paychecks issued to an employee within a single pay period
c. Bonuses paid during times when bonuses are not typically paid out or to employees who are not eligible

Match employee's records to:

a. Government identification records databases; note absences or duplicate registrations
b. Government death records

## To identify "no show" employees

Compare employee pay records to:

a. Electronic time and attendance logs
b. Access badge usage, computer log-in records
c. Biometric attendance records

## To Identify conflicts of interest

To identify employees who also own or are employed by vendors, match the employee's name, address, telephone (including cell phone), spouse, children, and emergency contact information in the HR master files to the vendor master files. Also see below background checks that can identify such conflicts.

## To identify travel and expense fraud

The IFMIS platforms and add-ons cited above have apps that can identify indicators of travel and expense fraud and block payments. See ACL Travel & Entertainment Expenses.

## To identify other HR abuses

Conduct comprehensive online and traditional background checks to identify other HR abuses, such as nepotism, false educational credentials or work history, and criminal records.

The background checks should include:

a. General internet searches
b. Social media sites
c. Public records
d. Media reports
e. Court records
f. Education verification sites

For general information on conducting background checks on firms and individuals, see https://guide.iacrc.org/due-diligence-background-checks-on-firms-and-individuals/.

A report by the Center for the Advancement of Integrity of Columbia Law School includes useful information on using technology to confront HR-related fraud by public employees (CAPI 2017, 13–16).

## Automated Tests for Payroll Audits

http://autoaudit.com/payroll-fraud-detection/

Employee algorithms

- Multiple employees using same bank account for direct deposit
- An employee using multiple bank accounts for direct deposit
- Identify two or more employees sharing any piece of information, such as phone number
- Identify employees sharing any piece of information with an accounts payable vendor
- Identify employees who have either a post office box or a mail drop for their address
- Invalid social security numbers—match with the Social Security Administration's social security number verification system
- Blank social security numbers
- Multiple employees with the same social security number
- Multiple employees with the same home address
- Employees with more than one address change within a year
- Employees on the payroll register prior to their start date or after their termination date
- Non-salaried employees on the payroll register but not in the time-keeping system

- Employees on the payroll register but not in the employee master file
- Identify deceased employees, match with death master file or social security number file
- Manual payroll checks
- Multiple paychecks issued to an employee within a single pay period
- Employees with no deductions for taxes or benefits (no withholdings)
- Ratio of gross to net pay
- Bonuses paid during times when bonuses are not typically paid out or to employees who are not eligible
- Employees with no pay increases, or more than two pay increases, within a year
- Employees with no paid time off, no vacation, no sick leave used

False salary and wage schemes

- Differences between pay rates recorded on the payroll register and those in the employee master file
- Employees with more than one pay increase in the past year
- Employees with abnormally large pay increases
- Inappropriate wage levels given employees' classifications
- Unusually high bonus payments
- Employees with more than the expected number of paychecks per year or per pay period
- Employees receiving unusually large percentage of their pay via overtime
- Bonus payments, by department or employee, that substantially exceed budgeted or prior year amounts
- Hours reported per timecard system that differ from those shown on payroll register
- Overtime hours that substantially exceed budgeted or prior year amounts
- Employees with over 40 hours per pay period
- Unsupported adjustments to gross or net pay

# References


Aarvik, Per. 2019. "Artificial Intelligence – A Promising Anti-Corruption Tool in Development Settings?" U4 Report 2019:1, U4 Anticorruption Resource Centre, Chr. Michelsen Institute, Bergen, Norway.

ACFE (Association of Certified Fraud Examiners). 2016. "Global Fraud Study: Report to the Nations on Occupational Fraud and Abuse." ACFE, Austin, TX.

Avis, Eric, Claudio Ferraz, and Frederico Finan. 2016. "Do Government Audits Reduce Corruption? Estimating the Impacts of Exposing Corrupt Politicians." National Bureau of Economic Research, Cambridge, MA.

Berret, Charles, and Cheryl Phillips. 2016. *Teaching Data and Computational Journalism*. New York: Columbia Journalism School.

CAPI (Center for the Advancement of Public Integrity). 2017. "Taking a Byte out of Corruption: A Data Analytic Framework for Cities to Fight Fraud, Cut Costs, and Promote Integrity." CAPI, Columbia Law School, New York.

CFRR (Centre for Financial Reporting Reform). 2017. "Public Sector Internal Audit: Focus on Fraud." World Bank, Washington, DC.

Chaudhry, Asif., 2020. "Over 1,500 'Ghost' and 'Dubious Employees' Found in P&SHD." *Dawn News*, January 17, 2020. https://www.dawn.com/news/1528750.

Chuah, Lay Lian, Norman V. Loayza, and Bernard Myers. 2020. "The Fight against Corruption: Taming Tigers and Swatting Flies." Research and Policy Brief 27, World Bank, Washington, DC.

Ciziceno, Marco, and Giovanni A. Travaglino. 2019. "Perceived Corruption and Individuals' Life Satisfaction: The Mediating Role of Institutional Trust." *Social Indicators Research* 141 (2): 685–701.

Dener, Cem, Joanna Alexandra Watkins, and William Leslie Dorotinsky. 2011. *Financial Management Information Systems : 25 Years of World Bank Experience on What Works and What Doesn't*. A World Bank Study. Washington, DC: World Bank.

Dilmegani, Cem, Bengi Korkmaz, and Martin Lundqvist. 2014. "Public-Sector Digitization: The Trillion-Dollar Challenge." McKinsey Digital, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/public-sector-digitization-the-trillion-dollar-challenge.

Djankov, Simeon, Asif Islam, and Federica Saliola. 2016. "How Large is Public Procurement in Developing Countries?" Realtime Economic Issues Watch, Peterson Institute for International Economics, Washington, DC.

Dubois, Pascale Helene, J. David Fielder, Robert Delonis, Frank Fariello, and Kathleen Peters. 2019. "The World Bank's Sanctions System: Using Debarment to Combat Fraud and Corruption in International

Development." In *Good Governance and Modern International Financial Institutions*, AIIB Yearbook of International Law, vol. 1, ed. P. Quayle and X. Gao, 217–38. Leiden: Brill Nijhoff.

Economist, The. 2016. "Developing Bangladesh: How to Spend It – An Ambitious Attempt to Work Out the Best Use of Scarce Resources." *The Economist*, May 5, 2016, London.

Filer, Tanya. 2019. "Thinking about GovTech: A Brief Guide for Policymakers." Bennett Institute for Public Policy, Cambridge University, Cambridge, UK.

Lee, Yunsoo, and Hindy Lauer Schachter. 2019. "Exploring the Relationship between Trust in Government and Citizen Participation." *International Journal of Public Administration* 42 (5): 405–16.

Lepri, Bruno, Jacopo Staiano, David Sangokoya, Emmanuel Letouzé, and Nuria Oliver. 2016. "The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good." In *Transparent Data Mining for Big and Small Data*, ed. T. Cerquitelli, D. Quercia, and F. Pasquale, 3–24. Cornell University: Ithaca, NY.

Lyon, David. 2017. "Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity." *International Journal of Communication* 11: 824–42.

Manzetti, Luigi, and Carole J. Wilson. 2007. "Why Do Corrupt Governments Maintain Public Support?" *Comparative Political Studies* 40 (8): 949–70.

Masson, Bernard, and Alex Margot-Duclot. 2018. "GovTech: Europe's Next Opportunity." Accenture and Public. https://www.accenture.com/_acnmedia/pdf-90/accenture-govtech-pov.pdf.

NIJ (National Institute of Justice). 2007. "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors." Special Report. U.S. Department of Justice, Washington, DC.

Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: NYU Press.

OECD (Organisation for Economic Co-operation and Development). 2016. *Towards Efficient Public Procurement in Colombia: Making the Difference*. Paris: OECD.

———. 2018. *Integrity for Good Governance in Latin America and the Caribbean: From Commitments to Action*. Paris: OECD.

———. 2019. "Enhancing Access to And Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies." Paris, OECD. https://www.oecd.org/going-digital/enhancing-access-to-and-sharing-of-data.pdf.

O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Broadway Books.

Pathways for Prosperity Commission. 2019a. “The Digital Manifesto: How Developing Countries Can Get Ahead in the Digital Age.” Blavatnik School of Government, University of Oxford, Oxford, UK.

———. 2019b. “The Digital Roadmap: How Developing Countries Can Get Ahead.” Blavatnik School of Government, University of Oxford, Oxford, UK.

Petheram, Andre, and Isak Nti Asare. 2018. “From Open Data to Artificial Intelligence: The Next Frontier in Anti-Corruption.” Oxford Insights (online). https://medium.com/oxford-insights/from-open-data-to-artificial-intelligence-the-next-frontier-in-anti-corruption-f2a9bf4f78a8.

Piexoto, Tiago, and Tom Steinberg. 2019. “Citizen Engagement: Emerging Digital Technologies Create New Risks and Value.” World Bank, Washington, DC.

Pușcaș, Bogdan. 2017. “Romanian Public Procurement System: Reducing Corruption Risks in Public Procurement.” The National Agency for Public Procurement, Bucharest. http://pubdocs.worldbank.org/en/999851495278567902/Romania-13th-PRIMO-Forum.pdf.

Romano, Leah Voigt. 2005. “VI. Electronic Evidence and the Federal Rules.” *Loyola of Los Angeles Law Review* 38: 1745–1801.

TI (Transparency International). 2014. “The Role of Technology in Reducing Corruption in Public Procurement.” Anti-Corruption Helpdesk, Transparency International, Berlin.

Veldhuizen, Roel van. 2011. “Bribery and the Fair Salary Hypothesis in the Lab.” University of Amsterdam and the Tinbergen Institute, Amsterdam.

Wdowin, Julia, and Stephanie Diepeveen. 2020. “The Value of Data: Literature Review.” Bennett Institute for Public Policy, Cambridge, UK.

WEF (World Economic Forum). 2018. “How to Prevent Discriminatory Outcomes in Machine Learning.” Global Future Council on Human Rights 2016–2018, White Paper, World Economic Forum, Geneva.

Wike, Richard, and Kathleen Holzwart. 2008. “Where Trust is High, Crime and Corruption are Low.” Pew Research Center, Washington, DC.

World Bank. 2016. *World Development Report 2016: Digital Dividends.* Washington, DC: World Bank.

———. 2019a. “Anticorruption Initiatives: Reaffirming Commitment to a Development Priority.” World Bank, Washington, DC.

———. 2019b. *Data-Driven Development*. 2018 Information and Communications for Development. Washington, DC: World Bank.

———. 2019c. “GovTech: Putting People First.” World Bank Draft Program Document. [←what does this mean? Is it a forthcoming publication? If so, it would be listed as “forthcoming.”]

———. 2019d. “Resource Guide to International Organizations. Using Technology to Promote Integrity.” World Bank Draft Proposal. [←again, what does this mean? Was it published?]

Zhu, Jiangnan. 2012. “Do Severe Penalties Deter Corruption? A Game-Theoretic Analysis of the Chinese Case.” *China Review* 12 (2): 1–32.