

Embracing Digitalisation: How to use ICT to strengthen Anti-Corruption



Published by

Embracing Digitalisation: How to use ICT to strengthen Anti-Corruption

March 2018

Authors:

Niklas Kossow | Hertie School of Governance

Victoria Dykes | Technologiestiftung Berlin

The publication “Embracing Digitalisation: How to use ICT to strengthen Anti-Corruption” was commissioned by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, Anti-Corruption and Integrity Programme, on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ).

The contents of this publication do not represent the official position of neither BMZ nor GIZ.

Table of contents

Executive Summary	5
1. Introduction	7
2. Understanding what we are up against... ..	8
3. The mechanisms behind ICT against corruption	9
4. Overview of existing ICT anti-corruption tools	12
4.1. E-Government services and digital public services	13
4.2. Crowdsourcing platforms	15
4.3. Whistleblowing platforms	17
4.4. Transparency platforms	20
4.5. News reporting and information dissemination platforms	23
4.6. DLT and blockchain technology	24
5. Recommendations.....	27
5.1. General recommendations on ICT in anti-corruption	27
5.2. Recommendations for specific ICT anti-corruption tools	30
Appendices.....	32
Appendix I: References	32
Appendix II: List of projects	35

Abbreviations

APCC	Assistance in Preventing and Combating Corruption in Indonesia
BMZ	German Federal Ministry for Economic Cooperation and Development
DFID	UK Department for International Development
DLT	Distributed Ledger Technology
EACC	Kenyan Ethics and Anti-Corruption Commission
FOI	Freedom of Information
GDC	German Development Cooperation
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
ICT	Information and Communication Technology
KfW	German Development Bank
KPK	Indonesian Anti-Corruption Commission
PI	Privacy International
TI	Transparency International
UNDP	United Nations Development Programme

Executive Summary

Digitalisation has transformed the public and private sectors in innumerable ways, affecting both the speed and scale at which tasks like communication or data analysis can be carried out. This is just as true for the field of anti-corruption, where Information and Communication Technology (ICT) has opened new doors for the prevention, detection, and prosecution of corruption. The aim of this study is to provide the German development cooperation (GDC) with options and recommendations on how to leverage ICT for anti-corruption; it builds on contributions to the digital agenda of the German Federal Government, as well as on the anti-corruption strategy of the German Federal Ministry for Economic Cooperation and Development (BMZ), and the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.

For this report, corruption is defined as *the abuse of entrusted authority for illicit gain*. From a theoretical perspective, the nature of corruption can be understood as both a principal-agent and a collective action problem. Both of these approaches can be addressed by ICT in various ways: through the digitalisation of public services (which removes opportunities for public officials to misuse their discretionary powers), upward transparency (whereby the state receives citizen feedback to understand how lower-level bureaucrats are performing), downward transparency (whereby government activities are made more transparent to citizens), and the mobilisation of citizens. Alongside standard ICT innovations, distributed ledger technology (DLT) also offers new potential to fight corruption, but this development is still in its infancy.

With regards to actual implementations of ICT tools for anti-corruption, six main categories emerge:

- **E-government and the digital public services;**
- **Crowdsourcing platforms;**
- **Whistleblowing platforms;**
- **Transparency platforms;**
- **News reporting and dissemination platforms;**
- **DLT & blockchain technology.**

The report analyses each category of tools, using reviews of existing literature as well as interviews with key experts and leaders of ICT anti-corruption projects to offer insights on use cases, implantation considerations, and advantages and disadvantages of a given tool. For example, crowdsourcing platforms benefit significantly from the existence of a follow-up mechanism that allows citizen complaints to be acted upon, and transparency platforms centred on freedom of information requests are likely to succeed only if citizens feel empowered to make requests of their own without fear of being seen as confrontational or facing retribution.

Based on this analysis, the report offers several recommendations to German Development Cooperation on how to successfully use ICT to support the control of corruption. ICT should be integrated into a broader anti-corruption framework, rather than being seen as an end in and of itself.

Key recommendations include:

- **A realistic risk assessment** of what drawbacks the use of a certain tool could entail, particularly if its implementation is not fully thought out (e.g., the risks associated with a whistleblowing platform that does not provide adequate protection for reporters)
- Built-in **accountability** mechanisms that ensure citizens see responses to indications of corruption
- Strengthening **civil society actors** who can both utilise and further support ICT-based initiatives against corruption
- Securing **government buy-in** to ensure long-term success of tools
- Provision of the requisite **legal framework** to ensure maximum efficacy of tools (for example, with respect to freedom of information portals)
- Adequate **publicity** for tools to ensure the public is aware of them to either make use of them or to demand the government maintain tools sufficiently (for example, government maintenance of open data portals)
- Ensuring projects are **sustainable**, particularly when they begin as third-party initiatives whose ownership is then handed off to the government or to other bodies

Further recommendations specific to each type of tool are expanded upon in the report.

ICT alone cannot lead the fight against corruption, but the tools associated with it can be a crucial and powerful addition to a broader anti-corruption portfolio – provided they are implemented within a supporting framework and in a fitting context.

1. Introduction

The Digital Revolution is impacting the lives of people everywhere. While at first it mainly affected industrialised countries, the last ten years have seen digitalisation speed up around the world. Globally, 48% of the population uses the internet, and more and more people in developing countries own mobile phones, many of which are smartphones (International Telecommunication Union, 2017). Digitalisation processes have the potential to not only transform people's daily lives, but also to revolutionise societal relations and the delivery of public services. As such they offer opportunities but also challenges for development cooperation. The German Federal Ministry for Economic Cooperation and Development (BMZ) has recognised these developments and reflected them in their contribution to the digital agenda of the German Federal Government, which outlines strategies to harness the digital revolution for sustainable development (Federal Ministry for Economic Cooperation and Development, 2017). The aim of this study is to provide the German development cooperation (GDC) with options and recommendations on how to leverage Information and Communication Technology (ICT)¹ for the prevention, detection, and prosecution of corruption. It is written on behalf of the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH. It provides recommendations on how ICT tools can support the four principles of BMZ's Anti-Corruption Strategy: transparency, participation, accountability, and integrity (Federal Ministry for Economic Cooperation and Development, 2012).

In the field of anti-corruption and good governance support, ICT has become increasingly important. Over the past 20 years, a wide array of projects on different levels of governance have attempted to use ICT tools for this purpose. These tools have affected the work of all actors recognised as key in the fight against corruption: state institutions, civil society organisations, civic movements and the media, as well as the private sector. Most of them work across different stakeholders and aim to bring these disparate groups together. While there are manifold approaches for harnessing the capability of ICT to stymie corruption, the success of these tools varies widely. Moreover, each tool comes with its own unique set of drawbacks and pitfalls that may make it more or less appropriate for a given context. Yet, these tools all share a similar theoretical understanding of the underlying nature of corruption; they also rely on a small number of mechanisms which are understood to drive their success.

This study provides an overview of what these success factors are, what aspects of corruption and which principles of anti-corruption they can address, and what the limitations of ICT tools in this context are. To do so, the report will first shed light on the theory and mechanisms behind ICT tools against corruption. Based on this review of theory, the report will classify the variety of tools that were used over the past fifteen years. It will present a summary of these tools and an analysis of their potential, the risks involved in using them, and the factors that contribute to or hinder their success. Based on this analysis the report will present recommendations aimed to inform GDC on how to use ICT tools in its anti-corruption work.

¹ This report focusses on the use of recent internet-based innovations and leaves aside, for instance, SMS-based reporting mechanisms.

2. Understanding what we are up against ...

Over the past ten years, a number of studies commissioned by a variety of actors in the field of international development cooperation have analysed the use of ICT tools in anti-corruption. This includes studies by the U4 Anti-Corruption Resource Centre (2013; 2014; 2016), the Asian Development Bank (Serrat & Ear-Dupuy, 2014), or the UNODC (2016), as well as several academic papers (e.g. Bertot *et al.* (2010) or Starke *et al.* (2016)). Most studies are fairly similar with regards to the types of tools they analyse; however, they differ in the way that they typologise and define those tools. Moreover, few of these studies look at the underlying assumptions of what drives corruption. While taking previous research into account, this study offers a more systematic assessment of ICT-based anti-corruption initiatives. Based on this analysis it makes targeted recommendations to GDC on how to leverage ICT tools in its anti-corruption work.

As a first step, however, it is crucial to establish an understanding of corruption and its drivers in order to properly understand under what conditions the use of ICT tools can enhance the effects of anti-corruption work. Most theories about the nature of corruption look at it as an expression of what we understand as a principal-agent problem (Rose-Ackerman, 1978; Klitgaard, 1988; Bardhan, 1997; Ugur & Dasgupta, 2011). This conceptualisation looks at citizens as the principal and government officials, political leaders, and bureaucrats alike as agents acting on their behalf. As agents have political discretion and often a monopoly over the distribution of resources, there is potential for corruption, which we define as “the abuse of entrusted authority for illicit gain” (NORAD, 2009, pp. 40-41). This principle is applied to both grand and political corruption, as well as the interaction of bureaucrats with citizens or the private sector. Consequently, strategies to fight corruption should focus on decreasing power discretion of individual government officials and on giving both their superiors and citizens means to monitor their work.

In studying such strategies, however, scholars have increasingly started looking at corruption as a type of collective action problem (Mungiu-Pippidi, 2011; Persson, Rothstein, & Teorell, 2013). This perspective stresses the social dimension of corruption, as government officials, businesses and citizens take their expectations about the behaviour of others into account. For example, if they expect their peers to accept bribes, they know they would lose out if they refuse bribes. At the same time officials and citizens know their honest behaviour is unlikely to change the system and make up for the costs associated with widespread corruption.

Marquette and Peiffer (2015) highlight that neither of these two theories of corruption work in an exclusive manner; both describe important aspects of corruption and help to understand its nature. They also stress that corruption can sometimes provide a strategy for dealing with fundamental societal problems that those who engage in corrupt activities try to overcome, such as low wages in the civil service or poor public service delivery.

These different theories provide important lessons for anti-corruption programming. Corruption that shows characteristics of a principal-agent problem can be addressed through better oversight, for instance. Collective action problems need a more complex approach that focuses on anti-corruption norms and on bringing citizens together against corruption. Different anti-corruption tools reflect

these perceptions of how corruption works and how it can be contained. They can, for instance, foster collective action against corruption by providing information or mobilising citizens, but also support transparency and accountability. These different perspectives thus can help diagnose the underlying societal problems behind corruption and help design context-driven solutions. This is especially valid for ICT tools against corruption, which often need to be adapted to local contexts and use a variety of mechanisms which support the basic principles of anti-corruption: transparency, participation, accountability, and integrity.

3. The mechanisms behind ICT against corruption

The digitalisation of anti-corruption strategies has already been a topic for the last 15 years. Sturges (2004) already describes a variety of projects funded by the UK Department for International Development (DFID) which use ICT to support transparency in the delivery of public services. Later studies by Bertot *et al.* (2010) or the U4 Anti-Corruption Resource Centre (2013; 2014; 2016) focussed on the issue by citing transparency as the principal mechanism behind successful ICT anti-corruption tools. Further studies, such as Serrat & Ear-Dupuy (2014), Starke *et al.* (2016), UNODC (2016) and Kossow & Kukutschka (2017) also looked at the digitalisation of public service delivery as a means of reducing corruption opportunities, as well as at the role of ICT tools in supporting the work of civil society actors through mobilisation and promotion of public participation.

Building on this work, this report will thus outline four mechanisms in more detail before taking stock of a variety of ICT tools used around the world in efforts to contain corruption: digitalisation of public services, upward transparency, downward transparency, and mobilisation. Additionally, it will also look at the emergence of blockchain technology as a potential lever in anti-corruption work. Besides looking at these mechanisms, the report also considers the potential risks involved in the adaptation of these tools: Greater transparency can lead to government officials simply hiding corrupt activities better, rather than decreasing corruption. Open data has potential conflicts with individuals' rights to privacy. Digital public services can be difficult to use for those who are not familiar with ICT, in the worst case excluding these people from using them. Whistleblowing platforms can endanger users if security measures are not properly implemented. Similarly, blockchain technology poses a challenge to data security and legal regulation. These risks should be kept in mind when considering the merits of ICT anti-corruption tools and will thus also inform the analysis of these tools provided here.

The general **digitalisation of public services** has been advanced in many countries around the world. It is primarily driven by the intent to increase efficiency in public service delivery. E-government tools can decrease waiting times, make some public services available around-the-clock and, in many cases, enable remote services and, crucially, reduce costs (Ndou, 2004). They are also put forward as an anti-corruption instrument as they reduce direct contact points between citizens and public officials. Citizens can file motions, submit petitions or apply for public services online, using personal computers or e-government terminals in government buildings. This reduces opportunities for corruption and favouritism by public officials. Several quantitative (Shim & Eom, 2008; Andersen, 2009; Elbahnasawy, 2014; Gurin, 2014) and qualitative case studies (United Nations, 2005; Kim, Kim, & Lee, 2009) have suggested that e-government is indeed effective in reducing corruption. While the positive

effects of e-government as an anti-corruption tool are thus well-established, the underlying mechanism is not just the reduction of opportunities. E-government also makes it easier to obtain information on the performance of public officials and analyse data on public service delivery.

In this way, ICT tools are also expected to increase **upward transparency** (Heald, 2006). This is seen as a mechanism to increase the state's ability to get citizen feedback and learn about the work of lower-level bureaucrats. Upward transparency thus helps senior state employees check on those in the lower ranks to ensure graft does not take place. It also helps the state hear from citizens and ask for their feedback on the performance of public services. The types of ICT tools that leverage upward transparency are online reporting platforms, crowdsourcing tools, e-government tools (both automated service and online service delivery) and other initiatives to gather citizen feedback, for example through the use of social media. Additionally, these tools also include safe platforms for whistleblowers. All of these tools provide ways of getting information from citizens to the government and information on lower-ranked bureaucrats to their superiors. They support not only transparency and accountability but also participation, three of the principles outlined in the anti-corruption strategy of the BMZ.

In contrast, **downward transparency** aims at opening up the government and providing information on its activities to the public. Citizens can thus use this data and hold state actors to account. Tools aiming at downward transparency make use of freedom of information laws and, for instance, help citizens request data from the government. Officials proactively make government data available through transparency portals, which give access to key government documents online, and through open data portals, which provide diverse government data in open formats², making bulk-analysis of data possible. As citizen initiatives, civil society organisations and journalists can use information provided through such tools to hold governments and bureaucrats to account. As corruption becomes harder to hide, public officials have incentives to act more honestly (Davies & Fumega, 2014).

Furthermore, ICT tools can be used for **mobilisation** against corruption. Especially in countries with more restricted media environments, citizen initiatives and civil society organisations use different tools to provide citizens with information about government corruption and mobilise citizens to take action against corruption. Social media-based initiatives and news websites can share information that often otherwise does not reach citizens. They can support the capacity of a society for collective action by helping coordinate the work of different anti-corruption initiatives and bringing together different people through enhanced communication and greater ease of sharing information. NGOs can use ICT tools to reach out to citizens and thus help in citizenry united against corruption (Kossow & Kuktuschka, 2017). In sharing information and mobilising citizens, such initiatives support participation and integrity.

² Data is considered as open data, if it is provided in a way that can be freely used, re-used and redistributed by anyone. For this purpose it has to be provided in a machine readable, non-proprietary format (Open Knowledge International, 2017).

In the past two to three years, anti-corruption activists and policymakers are increasingly looking at **blockchain technology** as a means of supporting anti-corruption work. Blockchain is a technology that promises higher transactional security by storing information in a digital ledger in the form of “blocks”, where each block contains data about a transaction. Copies of a blockchain are stored on a large number of servers around the world in a decentralized, peer-to-peer network. Through this design the copies represent a verifiable record which cannot be changed without altering subsequent blocks, thus limiting opportunities for fraud to go undetected. This robust record-keeping as well as blockchain’s decentralized nature and lack of a central authority overseeing its implementation (limiting opportunities to distort the process to serve the interests of a central authority) mean it can provide a secure and trustworthy way of keeping records. This can be particularly helpful in low-trust environments, which are often also characterised by high levels of corruption (Nakamoto, 2008; Kim & Kang, 2017). Another much-discussed application of blockchain technology is “smart contracts”, which are effectively contracts that automatically execute when the pre-determined conditions agreed to by both parties are satisfied (Luu, Chu, Olickel, Saxena, & Hobor, 2016). While the use of blockchain technology in anti-corruption is still in its cradle, potential uses include increasing security in public procurement or land registries, and securing financial transactions against fraud.

While all the tools mentioned above are, in one way or another, used in the context of anti-corruption work, none of them is guaranteed to be successful. Tools that aim to leverage downward or upward transparency, for instance, might provide useful data that can be used to fight corruption, but they do not necessarily result in more accountability and an actual decrease in corruption. The relationship between transparency and accountability is not linear and is indeed rather complex (Fox, 2007; Bauhr & Grimes, 2014). Accordingly, ICT tools can only ever be one part of a comprehensive anti-corruption strategy. The following analysis will consequently not only look at how these different tools were implemented, but also in which contexts they were successful and in which they failed to support the struggle against corruption.

4. Overview of existing ICT anti-corruption tools

Corruption can take many different forms, ranging from low-level officials asking for small bribes to highly prominent elected representatives misusing federal funds for their own personal gain. But, as the U4 Anti-Corruption Research Centre notes, anti-corruption means more than simply seeking criminal consequences for those who engage in corrupt activities. A comprehensive approach focuses on “preventing [corruption], [...] building transparent, accountable systems of governance and strengthening the capacity of civil society and the media as well as improving public integrity, strengthening the personal ethics of public and private officials, and perhaps even challenging social norms that encourage corruption” (U4 Anti-Corruption Resource Centre, 2017). Unsurprisingly, there is no single tool that can do all of these things. Instead, there are a myriad of ICT tools that can address various parts of this approach, with different types of tools being better suited to addressing different challenges.



In an attempt to capture this diversity, this report divides tools into six broad categories:

- E-Government services and digital public services
- Crowdsourcing platforms
- Whistleblowing platforms
- Transparency platforms
- News reporting
- DLT & blockchain technology

In the theoretical section above, it was noted that effective anti-corruption policies should focus on decreasing the power discretion of individual government officials and grant superiors and citizens the means to monitor these officials' work. Each of the six tool groupings identified allows for either decreased personal discretion, greater monitoring potential, or both. There is of course overlap between the categories: there are e-government innovations that could also be considered transparency platforms and blockchain-based tools can provide a form of digital public services. The categories should thus not be seen as rigid or mutually exclusive. Yet, broadly speaking, the ICT tools subsumed under these categories reflect certain characteristics in the way they address corruption.

This section looks at each ICT tool type individually, presenting a non-exhaustive list of use cases (representing both initiatives from the German development cooperation as well as initiatives from outside this sphere) and offering an assessment of the primary features and the strengths and weaknesses of such an approach. These assessments are bolstered by interviews with experts involved in the design and/or deployment of such tools.



4.1. E-Government services and digital public services

Key Anti-Corruption Applications:

- Automatisation of public services
- Greater transparency in government operations

Key Challenges:

- Ensuring the services provided are the ones people actually want, need and that they are able to access them
- Integrating new systems with existing infrastructure
- Convincing government employees to use the new system
- Ensuring that systems are kept up-to-date

Mechanism type(s):

- Digitalisation of public services
- Downward transparency

E-government is a broad term that is generally understood to refer to “the use of ICTs to more effectively and efficiently deliver government services to citizens and businesses.” (UNDESA, 2017). Digital public services exist under this umbrella of terms. Though efficiency and effectiveness are two of the main cornerstones of e-government, it also has the added advantage of making government operations more accessible and intelligible to citizens, opening up new opportunities for accountability and citizen oversight. Moreover, the efficiency gains of e-government are often secured through the automatisation of certain services; this removal of human discretion can also make processes fairer and less prone to corruption.

One of the first major e-government initiatives to succeed was the **OPEN system** implemented in Seoul, South Korea in 1999 (Kim *et al.*, 2009). The system was at least partly a direct response to the prevalence of corruption in the local government, particularly bribery. OPEN introduced a significant degree of transparency into public services, allowing citizens to track the progress of bureaucratic procedures they had initiated online without the need to first request a status update from bureaucrats. Moreover, the new system made it possible to see who had made what decision at what stage, essentially allowing citizens to audit the process and spot potential irregularities. Finally, the personal interactions between citizens and bureaucrats were limited by the system, reducing opportunities for bribery.

In Indonesia, the **JAGA app** (released on 1st December, 2016) aims generally to increase the quality of public services like health care and education. The app was developed by Indonesia’s Corruption Eradication Commission (KPK) in cooperation with the GIZ program **Assistance in Preventing and Combating Corruption in Indonesia (APCC)**. The total cost for both the mobile application and the web service was around 40,000 euros. A major way JAGA combats corruption is by gathering data from various government ministries about the services they provide (including information like the number of doctors employed or beds available at a given hospital) and empowering citizens to check

whether the government-provided data matches reality; the app points citizens to where they can report discrepancies they find. The app can also be used to access information about licensing services. Finally, the app also integrates government budget data and further information about public services. The app aims to combat corruption by giving citizens easy access to information on public services provided by the government. This is intended to help citizens identify gaps and disagreements between what the government presents to be the case and the actual reality of public service delivery. One of the biggest challenges currently being faced by the JAGA app is ensuring it is actually providing information that is of interest to its users – people won't use the app if it doesn't provide value for them. The app has been downloaded more than 10,000 times and is actively used by around 2,000 people. Since launching the initial versions of JAGA, it became clear to the developers that for the app to be most useful to citizens, it needs to be more tailored to specific regions' unique needs and interests. As such, the team is currently focusing on establishing regular conversations with users in more specified localities; they have, for example, released a version of JAGA that is specific to the province of Riau.

Kenya's **Integrated Public Complaints Referral Mechanism** (also known by its Swahili name *Sema! Piga Ripoti*, meaning *Speak Out! Submit your complaint*) is a joint effort between five government agencies and one NGO to develop a more efficient process for handling citizen complaints regarding hate speech, human rights violations, maladministration, discrimination, and corruption. It has been in use since 2013. The mechanism is used by several bodies responsible for handling citizen complaints: the Ethics and Anti-Corruption Commission, the National Cohesion and Integration Commission, the Kenya National Commission on Human Rights, the National Anti-Corruption Campaign Steering Committee, the Commission on Administrative Justice (Office of the Ombudsman), and Transparency International Kenya. All of these bodies have similar but distinct mandates, but citizens who lack a specialized knowledge of these mandates may not always choose the correct recipient for their specific complaint. In other instances, even when a citizen knows the appropriate body to submit a complaint to, this body may be located prohibitively far from the complainant or otherwise difficult for them to reach (online portals do generally exist, but they are not widely used). The referral mechanism is an internal tool that enables participating organizations to re-route complaints submitted to them to the body with the appropriate mandate. Participants in the system know who the other bodies are and what the scope of their oversight is. This creates a more efficient process for citizens, who do not have to resubmit their complaints to the proper body or travel long distances or incur other hardships required to report to the correct institution. The system has increased the ease with which citizens can report corruption incidents and has resulted in complainants receiving feedback on these reports in a more timely fashion. But one problem affecting use of the system, as explained by GIZ Kenya staff involved in the tool's implementation, is that many of these organisations already have their own internal, organisation-specific complaint handling systems and procedures. The joint mechanism is thus seen by some as extra work on top of their normal workflows, which reduces usage of the integrated system. This is a problem GIZ Kenya's staff are hoping to combat by increasing publicity for the mechanism so citizens put more pressure on agencies to actually use it, as well as by mainstreaming uptake of the system by including use of it in job descriptions for employees of these bodies.



4.2 Crowdsourcing platforms

Key Anti-Corruption Applications:

- Provide a way for citizens to report corruption publicly, thus tend to be used to address petty corruption
- Increase visibility of corruption and potentially highlight trends

Key Challenges:

- Getting enough people to use the platform for it to be useful
- Providing a link between reporting the problem and actually having the problem acted upon

Mechanism type(s):

- Upward transparency
- Mobilisation

In the context of anti-corruption, crowdsourcing platforms invite citizens to provide input on incidences of corruption, often in the form of sharing personal experiences. These sites can help identify specific trends as to what type of corruption is happening most frequently or where corruption is most likely to happen (both in terms of what branches of the government and where corruption is physically happening). They are heavily dependent on participation and people knowing about the site: if no one knows it exists or actually uses it, then the site has no content and no value to offer for fighting corruption.

One of the most famous examples of this type of tool is the website [IPaidABribe](#), where users can report on their bribe experiences, including times they paid a bribe, times they declined to pay a bribe, as well as honest officials they interacted with. According to a coordinator at the Janaagraha Centre for Citizenship and Democracy who helps run the website, the initial idea behind IPaidABribe was that in a society like India where everyone knows corruption occurs and talks about it with other people, no one was actually recording information about the “corruption market” – i.e., the market price of a bribe, who has to pay what and when, etc. The website originated in India, but versions of it have sprung up across the world with support from the original developers. The site is funded partly through foundations and partly through donations from both users and Indian companies. A similar project, **Bribespot**, was active between 2012 and 2016 in several countries around the world. The **Bribespot** website and app were available in six different languages, including Russian, Khmer, and Thai, and their use was promoted through NGOs in a variety of countries. While it initially got a substantial amount of traction in Thailand, Bribespot never saw the user numbers that IPaidABribe has had in India.

Several features of IPaidABribe help explain its success in comparison to other bribe-reporting platforms. The project was originally envisioned for anonymous reporting only, but later the option for reporters to provide their name was added in order to allow for the ability to follow up on reports and for the possibility of prosecutions. Importantly, IPaidABribe features the possibility of government

officials actually following up on reports. Individuals known as “Janayuktas” serve as liaisons between users of the site and the government and have the ability to follow up on reports submitted to the website – either by initiating prosecution of corrupt officials, or by analyzing anonymous reports in order to identify potential reforms to public service delivery. Both of these features are likely crucial in securing the success of IPaidABribe (it is worth noting that the above-mentioned project Bribespot did not have either of these two features). However, the Janayukta functionality is largely limited to the states of Karnataka and Bangalore, where the site is most active. According to a coordinator at the Janagraha Centre, the site intends to continue to grow and secure more coverage of India. IPaidABribe also features the option to report an honest official, to laud those civil servants who do their job without asking for a bribe or resorting to favouritism. The app thus informs citizens about corruption and discourages bribe payments (from citizens) and the acceptance of bribes (by public officials). In doing so it addresses corruption as a collective action problem.³

Crowdsourcing platforms also feature several risks. First, they can easily be used for unfounded denunciations, especially when they offer the possibility of anonymous reporting. Furthermore, non-anonymous reporting could lead to repercussions for the reporters. The institution of the Janayuktas is also meant to mitigate these risks. As they receive all reports, they can fact check and question them in order to filter out false reports. As they receive the names of reporters who chose not to stay anonymous, Janayuktas can also safeguard their identity to protect them from repercussions.

³ Another good example of a crowdsourcing platform that is not explicitly anti-corruption in nature but which has the potential to be used as such is mySociety's [FixMyStreet](#). It allows for citizens to report problems like potholes or broken street lamps. The reports are sent on to government authorities and are also viewable in a map, so everyone can see what reports are being made where. For FixMyStreet, it is again crucial that the website has a link to government officials so there is actually the chance of problems being acted upon and resolved.



4.3 Whistleblowing platforms

Key Anti-Corruption Applications:

- Provide a way for citizens to serve as corruption whistleblowers, including anonymously
Tends to be more useful to fight grand corruption

Key Challenges:

- Weighing value of anonymous vs. non-anonymous reports
- Risk of receiving more reports than can be acted upon

Mechanism type(s):

- Upward transparency

Whistleblowing platforms provide a way for citizens to report wrongdoing on the part of public officials, or in some cases on corrupt business people⁴. Crowdsourcing platforms fight corruption through collecting a large number of reports and publicising personal, informal accounts of corruption for all citizens to read, thus offering a perspective of how widespread or endemic corruption in a specific area is. In contrast, whistleblowing platforms fight corruption through collecting detailed reports of wrongdoing with the intent of building possible legal cases against corrupt actors. They aim at a lower number but higher quality of reports. Because protecting the identity of reporters is so important, whistleblowing platforms usually deploy some sort of encryption or anonymization process to protect whistleblowers' identities and encourage reporting without fear of retaliation. Organisations interested in setting up their own whistleblowing platforms do not necessarily need to come up with a home-grown solution. Two major providers of whistleblowing systems are [GloLeaks](#)⁵ (open source) and [BKMS](#)⁶ (proprietary).

An important consideration with whistleblowing platforms is that while anonymous reporting needs to be the primary option, there should nevertheless be some way to establish follow-up communications. This can be done by assigning whistleblowers a unique identification number or ID that allows them to access their case in the system, for example. Doing so is important to allow officials to follow-up on reports where there is insufficient information for prosecution, as well as to allow the whistleblower themselves to provide feedback on how the case is being handled, according to the president of the

⁴ Target groups depend on the implementation and the context of these platforms. Some companies implement whistleblowing platforms as part of their internal compliance or reporting mechanisms.

⁵ [GloLeaks](#) is an open-source and free software developed by the Hermes Center for Transparency and Digital Human Rights, based in Milan, Italy. Initiated as a project in 2012, GloLeaks has been adopted to several different settings, both in the public and private sectors. Since 2014, the software has been applied in several anti-corruption projects. As an NGO, the Hermes Center helps clients to adopt the software to their needs, while the software itself remains open-source and free to use.

⁶ The [BKMS Compliance System](#) is a proprietary whistleblowing system offered to both private sector and public sector entities. BKMS has a wide range of clients that have implemented the system and is adapted to each use and is mainly used as an internal compliance and whistleblowing system for organisations. The system encrypts and protects information provided by a whistleblower and forwards information to an internal examiner. The information and assessments added by the examiner are also protected.

Hermes Center for Transparency and Digital Human Rights, the organisation running GlobaLeaks. A governance advisor from GIZ Kenya who helped implement Kenya's anonymous whistleblowing platform (described in greater detail below) noted that some government officials in Kenya were reluctant to support a platform that allowed people to remain anonymous, as this would make it much more difficult to generate actual witnesses for potential criminal trials.

In this context, it is important that officials have the possibility of engaging in continuous interactions with whistleblowers in the hopes that sufficient trust will be built up for a voluntary identity reveal. At the same time, these platforms generate very real risks for potential whistleblowers, particularly if these individuals do choose to eventually forgo their anonymity. If providers of whistleblowing platforms decide to encourage reporters to identify themselves, these platforms need to be prepared and equipped to protect reporters' identities, both for the sake of the whistleblower and for the sake of the platform's integrity. Protection should be provided by the design of the platform: GlobaLeaks puts great emphasis on enforcing its anonymity through the technological design of its platform, which makes it impossible to trace IP addresses of potential whistleblowers. The platform also leaves data ownership to the local organisation that is implementing a system using GlobaLeaks, with no data transfer taking place between the local organisation and the Hermes Center. According to the president of the Hermes Center, these are vital steps to protect potential whistleblowers.

The risks involved in the implementation of these platforms also depend on the legal protection of whistleblowers. Though of course the presence of a whistleblower protection law would also help encourage use of whistleblowing platforms, few countries have comprehensive whistleblowing legislation, and in others legislation does not protect anonymous whistleblowers, should they be exposed later. Protection thus needs to be either adapted to legal requirements or be well-implemented to safeguard whistleblowers from repercussions.

Another possible challenge with whistleblowing platforms is handling the volume of submissions. Advertisement of a whistleblowing platform is important to bring the service to people's consciousness (and keep it there). But if too many people make use of it, there is the risk of receiving many reports that are benign or that do not provide enough information to merit follow-up actions. Platform administrators being unable to respond to all or even most submissions risks undermining trust in the system. For example, according to GlobaLeaks, when Transparency International Greece's Advocacy and Legal Advice Center launched its own whistleblowing platform, they received nearly 10,000 submissions within one month – a number far greater than what they could act upon, especially as many reports lacked necessary details. One way to mitigate this problem is by having longer or more complicated submission forms. More labor-intensive and thorough questionnaires can decrease the volume but increase the quality of submissions. This of course limits the usability of the whistleblowing platform, but it is important to strike a balance between quality reports and ease of system use. Alternative, non-digital ways of reporting (for example via telephone or in a physical office) can supplement digital whistleblowing tools, although these reporting channels make protecting anonymity significantly more challenging.

The [Kenyan whistleblowing platform](#), built using BKMS software, has been in place since 2005. It was first introduced with support from GIZ Kenya and is now under the authority of the Kenyan Ethics and Anti-Corruption Commission (EACC). At the time the system was introduced, reluctance to report as well as retaliation against corruption whistleblowers were both significant problems in Kenya, according to a governance advisor at GIZ Kenya. Moreover, there were limited ways in which individuals could file reports, and the reports submitted were often lacking in quality. The online platform provides anonymity to whistleblowers, and the information it asks from reporters helps generate higher-quality submissions that are more feasible for officials to follow up on. Similarly, the digital system allows for easier case management of corruption reports, allowing officials to categorize and sort reports and maintain a constant (but still anonymous) interaction with the whistleblower through the use of unique IDs. The Indonesian Anti-Corruption Commission (KPK) also has a secure, anonymous whistleblowing platform based on the BKMS software and with similar functions to the Kenyan platform; it has been in place since 2010. After its first year of activity, representatives from the GIZ program Assistance in Preventing and Combating Corruption in Indonesia (APCC) and the KPK evaluated the system and made necessary changes; for example, they re-configured the submission form to both make it more intelligible to would-be reporters and to ensure the information being gathered is that which is most useful to the KPK for understanding and following up on the report.

In recent years, the Kenyan platform has averaged annual reports in the thousands. However, these numbers have fallen off in the last three years. One major reason is the insufficient publicity for the portal – “The system depends on continually reminding the public of its existence,” the GIZ Kenya governance advisor notes. Previously, dozens of government ministries had links to the whistleblowing platform on their websites; today, after changes in leadership and priorities, this number has fallen significantly. Publicity is also recognized as a key success factor in Indonesia, where the KPK regularly engages in campaigns to raise awareness of their whistleblowing platform through distribution of promotional materials by a specific unit dedicated to disseminating information about the platform. Their system consistently has around 2,000 submissions per year. Even though the KPK is not able to follow up on all reports, general statistics about what types of complaints are most commonly reported can also be useful, since they can point to specific structural problems.



4.4 Transparency platforms

Key Anti-Corruption Applications:

- Provide information on government operations that could expose corrupt behaviour
- Existence of such platforms can act as a “chilling effect” on corruption

Key Challenges:

- For freedom of information (FOI) portals, need a sufficient legal basis for such requests
- Governments need to be willing to publish data
- Portals that rely on the public FOI requests need an active audience able to use data in an effective way
- Use of government-provided data to expose wrongdoing could lead to that data being removed

Mechanism type(s):

- Downward transparency

Transparency platforms are those that focus on disseminating and otherwise making public information about government operations and activities available for the general population. Common examples of these platforms are freedom of information portals and open data portals, as well as other types of tools that build on this type of information. Open data and transparency portals are often run by governments since they are generally providing direct access to government-generated data; freedom of information portals tend to be initiated by civil society actors and help citizens request information from the government.

Freedom of information portals are websites or apps that make it easier for citizens to file freedom of information requests and which publish the results of those requests publicly for other citizens to benefit from. These portals are not inherently anti-corruption initiatives in and of themselves, but they can often expose corruption or lead to a reduction in corrupt behaviour. For example, the head of development at mySociety⁷ highlighted one recent example of freedom of information portals in action: a group of citizens effectively used the UK-based [WhatDoTheyKnow](#) portal to conduct a citizen audit of their local authorities’ spending. In another case, mySociety’s products were used to publish information about the spending of community funds in Kenya; the disclosure of this information led to members of one village forcing their member of parliament to not seek re-election due to revelations about his handling of these funds. Through the [Alaveteli](#) framework, mySociety provides a way of deploying a freedom of information portal anywhere in the world – currently, projects in at least 25 different

⁷ mySociety is a UK-based NGO that has a robust set of technology solutions for enhancing democratic participation that have been replicated in a variety of country settings. Their tools are open source and have a well-documented history of success and are used in a variety of contexts.

countries are making use of their software for this purpose. Such portals have been used to increase scrutiny of public spending and discretionary expenses of public officials as well as to expose individual corruption cases⁸.

Beyond exposing potential wrongdoing, these portals also have the potential to have a chilling effect: if government officials know there is the very real possibility that information about their activities will become public, they may be less likely to engage in illegal or otherwise questionable behaviour. The key to these portals being successful, however, is active public participation. Without interest in the portal, there will be no requests submitted and no information publicized. In this way, such portals address the dual nature of corruption as a collective action and a principal-agent problem. They help to provide oversight over government agents, but also foster collective action by citizens.

The head of development for mySociety noted that freedom of information requests can be seen as “confrontational.” Citizens must thus first feel that it is genuinely safe and accepted for them to make such a request for these projects to take off. An easy way to establish this perception is to make newly established sites have a few initial successful requests already on display. Ideally, these initial requests would show the variety of forms FOI requests can take, specifically that they don’t always have to be “confrontational” in nature – for example, according to the mySociety representative, one of the most-visited pages on the Ukrainian platform is a request and government response about when a free museum day in Kyiv was happening, as this information had not been publicised elsewhere. Moreover, there needs to be a sufficient legal basis for freedom of information requests for the portal to succeed. Activists in Spain attempted to create their own instance of Alaveteli, but ultimately failed due to the complicated network of national laws dictating how such requests work.

Like the freedom of information movement, the open data movement⁹ has gained significant popularity in recent years as an important measure for transparency in government¹⁰. Open data portals themselves do not necessarily have anti-corruption effects. Yet, they increase government transparency, which, in the right circumstances, can help fight corruption. An example of this is the EU Horizon 2020 [DIGIWHIST](#) project, which aims to increase transparency in public procurement and identify potentially corrupt contracting. The project relies on publicly available procurement data; it cleans, refines, and analyses the data to make it accessible and intelligible to citizens. One of its main outputs is the OpenTender portal (launched in January 2018) which allows visitors to explore procurement data for 35 different countries, including the option to filter for contracts matching a set of pre-determined indicators for high corruption risk.

⁸ mySociety periodically documents such cases on their [blog](#), for example.

⁹ Those interested in learning more about open data in general are recommended to start with the [Open Data Handbook](#); for those interested in open data specifically in the context of anti-corruption, the Open Data Charter has [a guide](#).

¹⁰ See for example the [G20's Anti-Corruption Open Data Principles](#) or the [Open Government Partnership](#).

The intended audiences for these types of portals are civil society organisations, journalists and others in a position to investigate, visualise and publicise the data further and produce specific conclusions from it.¹¹ Though OpenTender has only recently been launched (January 2018) and thus has not yet produced concrete anti-corruption effects, the Ukrainian e-procurement platform ProZorro serves as an example of how increased transparency in public procurement can lead to more efficient public spending and thus, arguably, less corrupt contracting.¹²

Such projects are only as good as the quality of data they have to work with however – in the case of DIGIWHIST, for example, its project lead reported that the quality of publicly available procurement data ended up being much poorer than expected, forcing the project to scale back its initial expectations. Moreover, it should not be taken for granted that a preponderance of open data automatically equates to a more informed citizenry and a more accountable government; for this to be the case, data needs to be released in structured, analysable formats and, ideally, presented in ways that make it intelligible and accessible to the general public. Because of this, the DIGIWHIST project also cooperates with investigative journalists and civil society organisations to make its platforms most useful for them.

Projects based on open data also bear a number of risks. One of the most common ones is that the source data will change in some way – the data might change formats, change locations, or simply be deleted altogether – making it difficult to build a stable transparency portal out of it. More problematic is the risk that in the face of increased scrutiny due to publicly available data, governments may stop publishing the data altogether. This was the DIGIWHIST project lead's experience when looking at contract implementation data in Hungary, for example – once he started publishing findings from this data that reflected poorly on the Hungarian government, they simply removed the data. Further, freedom of information and open data portals depend, of course, on civil society actors to use the respective portals and to analyse the data that they provide. Accordingly, an active civil society sphere is needed for these portals to be effective remedies for corruption. Civil society capacity building in the field of data analysis can also support this.

¹¹ This possibility has been well-documented in various publications by the [Open Data Charter](#), [the UNDP](#), and a variety of organizations active in the field of data journalism.

¹² ProZorro is an integrated e-procurement system that provides procurement data through an open and free portal. Started in 2016 by a civil society initiative, the majority of Ukrainian tenders are today awarded through ProZorro, and its data is used to create greater transparency in Ukrainian public procurement. Documented savings through the project can be assessed via [the monitoring section](#) of its website.

4.5 News reporting and information dissemination platforms

Key Anti-Corruption Applications:

- Provide news and information about corruption-related occurrences in a given country/area
- Increase general public awareness of corruption and how to combat it

Key Challenges:

- A relatively passive approach to fighting corruption
- Portals may not make it clear what people should do with this information

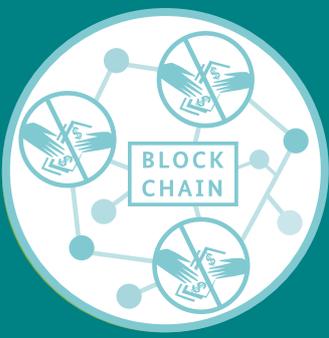
Mechanism type(s):

- Mobilisation

More passive in nature than the other types of tools listed here, these are platforms that exist to disseminate information about corruption within a given location. This can include publicizing convictions of public officials for corruption-related offenses or writing articles about newly-enacted anti-corruption legislation. Thus, the main intent of such platforms is less to galvanize citizens into action (though of course that may be a byproduct) and more to simply keep citizens informed of anti-corruption efforts happening in their area.

For example, the Hungarian website [K-Monitor](#) was started in 2007 with the general aim of creating a map of corruption cases in Hungary. From there, it has grown into a hub for information on corruption in Hungary, featuring a database of articles covering corruption- and transparency-related topics as well as original research and civic tech initiatives. Indonesia's [Anti-Corruption Clearing House](#) is one of several initiatives of the KPK, Indonesia's Corruption Eradication Commission. The website focuses less on providing up-to-date news on corruption and instead provides information on anti-corruption laws, educational materials (including games for children), original research publications, and information on criminal investigations into corruption; the general goal is to empower the public to work to prevent corruption in Indonesia. A similar project is [Nikorupciji.org](#), a website published by the Ukrainian Institute for Mass Information and sponsored by the US-based NGO Freedom House. The website is an outlet for bloggers to publish articles about corruption in Ukraine and to comment on anti-corruption reforms.

All of these platforms provide a simple way to keep citizens informed about the issue of corruption, in environments where corruption-related developments do not necessarily make frontpage news. By providing information on the problem, the platforms can foster collective action and show to citizens that corruption affects everyone on a given society. While their reach is limited, targeted news websites represent an easy-to-implement and cost-effective solution to inform citizens.



4.6 DLT and blockchain technology

Key Anti-Corruption Applications:

- Allow for a high level of transparency and accountability in transactions
- Severely reduce opportunities for fraud and deception

Key Challenges:

- A relatively new technology largely untested in the field of anti-corruption
- Integrating new technology into old systems

Mechanism type(s):

- Downward transparency
- Digitalisation of public services

As mentioned in the first section of this report, blockchain is a technology in which information is stored in “blocks” in a digital ledger; each block contains encrypted data about a transaction, and blocks cannot be changed without all subsequent blocks in the chain also being changed. At their core, the biggest contribution blockchain-based tools are able to make toward the fight against corruption is a new system for ensuring accountability. Transactions and documents stored on the blockchain cannot be changed without also changing subsequent blocks in the chain. This ensures there is a complete, public record of alterations.

One area where blockchain technology can be meaningfully deployed is that of budget transparency. The German Development Bank (KfW) is currently piloting a blockchain solution for increasing transparency in budget allocations and spending in Africa. The application, called [TruBudget](#), plans to provide a platform where international donors can see what spending decisions have been made by a given government ministry, using the immutability of the blockchain as a way to build trust that money is actually being spent according to what was announced and agreed upon. Though this initiative could be used in a variety of budgetary contexts, the currently envisioned workflow focuses on international donors supporting development projects. A sector economist and a head of division at the KfW involved in implementing TruBudget explained that the app grants rights to specific parties and generates a log of who did what. For example, a government ministry can define the budget and the specific executing body can define the workflow, but there can also be built-in checks where donors have the right to approve certain steps before they can be enacted. All the while, blockchain technology enables there to be an audit-proof record of who completed each step and what the status of the project is. Currently, TruBudget has a functional prototype, and the KfW is in talks with a few African countries to launch a test phase. Significantly, this project is based on open source solutions, meaning there is both the possibility and the hope that other countries will adapt this application to other uses and contexts.

However, the novelty of blockchain technology also presents difficulties in implementing it successfully. As the KfW economists noted, blockchain obviously represents a departure from traditional IT practices. Governments the world over tend to be locked into IT strategies dominated big-name, proprietary systems, and those in charge of overseeing IT projects may be reluctant to try out technology solutions outside of this framework. Such solutions can also be a challenge if they are implemented without necessary training.

Another budding field of application for blockchain is that of land registries. Bitfury, a private company specializing in the development of blockchain software solutions, is currently implementing a [blockchain-based land registry system](#) in Georgia. The system, as explained by a senior project manager at Bitfury, involves storing land ownership certificates on the blockchain. Having certificates on the blockchain allows for greater trust in land-based transactions and reduces opportunities for fraudulent transactions whereby someone falsely claims to have acquired property of a piece of land. Such transactions are prevented, as the data stored in the blockchain is immutable and all changes to data are recorded. This of course depends on original data being accurate in the first place.

This system is also able to take advantage of the smart contracts application of blockchain, whereby a contract is automatically executed once the pre-determined conditions of the contract are met on both sides. In the case of Georgia, the project aims to make it possible to conclude sales of land through the blockchain, with the transition of land ownership and the exchange of money happening at the same instant, limiting opportunities for fraud.

Bitfury's project began in January of 2017 and remains ongoing. Currently, all newly issued land certificates are being simultaneously logged on the blockchain as well as through paper copies; in general, the new system is not yet widely used by the populace. Features like conducting transactions on the blockchain are not yet enabled. According to Bitfury, the current plan is to have both the old and new systems running parallel for some time as significant bureaucratic and legal changes have to occur to allow for a full digital transition.

Ultimately, the relative novelty of this technology means there is not a large number of use cases in an anti-corruption context, and the efficacy and end results of these use cases are generally unclear. Blockchain is an area that should continue to be observed and studied for its anti-corruption potential. For instance, the technology could help in the digitalisation of contracts and help secure monetary transactions and increase transparency of government payouts. The blockchain can store data that makes it possible to follow up on individual transactions; this could help to fight embezzlement and fraud, as well as corrupt payments. In doing so, it does not help to create collective action, but rather provides additional transparency and accountability.

5. Recommendations

ICT anti-corruption tools can be successful in creating awareness, mobilising citizens and reforming public services. Yet, their potential should not be exaggerated. In line with key principles of anti-corruption, ICT tools can play a great role in supporting transparency, participation, and integrity. However, to be truly effective, they need a functioning accountability framework that includes an independent judicial system, press freedom and an active civil society. This can also include a more transparent and decentralised governance system, which can, for instance, be supported by blockchain technology. Hardly any of the ICT tools that were subject to this study were part of a wider anti-corruption strategy; several of them were initially not even meant as an anti-corruption tool. ICT tools have a long way to go to become standard elements of national anti-corruption strategies.

Based on the analysis above, the following recommendations for GDC can thus be made with regards to the use of ICT in anti-corruption. The recommendations are divided twofold: (1) general approaches toward the use of ICT in anti-corruption, including contextual factors for success of such tools, and (2) specific recommendations for the different tools as categorised above.

5.1 General recommendations on ICT in anti-corruption

Integrate ICT in a broader anti-corruption framework: ICT tools are easy to implement. For the most part, they do not require advanced technical knowledge and they have the potential to reach a lot of people. They also give development cooperation projects a modern appeal and are thus attractive projects to support. Taken in isolation, they can do little to meaningfully fight corruption. But when taken as a part of a broader anti-corruption policy, they have real potential to advance anti-corruption goals, as they can address specific needs, like more efficient public services or more transparency in certain government sectors. ICT anti-corruption tools should thus be developed with a local focus and keep specific corruption problems in mind. The tools analysed in the context of this report provide some examples for potential solutions that address specific types of corruption. Crowdsourcing tools, for example, can only be effective against petty corruption. Open data can be effective in the context of addressing corruption in the field of public procurement or other data-rich government activities.

A majority of ICT anti-corruption tools aim to mobilise citizens against corruption and create awareness about the problem through various means. ICT tools are well-placed to do this, as they have the potential to reach large segments of the population quickly and efficiently. Their effectiveness, however, is highly dependent on user-friendly design and on taking citizens' perspective into account. It also hinges on general ICT access, which remains an issue in rural and less-developed areas. In many cases, rather than directly affecting the likelihood of citizens or public officials to engage in corrupt actions, ICT anti-corruption supports mechanisms which might have this effect. Some tools might lead to greater transparency or citizen engagement but not directly reduce corruption themselves. Some tools might also lead to other ends in themselves, such as more effective public service delivery or effective administration and only indirectly support anti-corruption.

Realistic risk assessment: As pointed out above, ICT tools are generally easy to implement. In the same sense, they carry few direct risks for their users. But, some specific risks appear in connection with certain tools. Blockchain technology, for instance, needs a certain amount of technical knowledge to be used effectively in public administration. Even more so, whistleblowing platforms are only secure for their users if implementing local partners have the necessary technical knowledge to make sure identities of the users are protected. As such platforms promise safety and anonymity to potential whistleblowers, a sloppy and ill-thought-out technical implementation of a whistleblowing platform could compromise user identities. Potential retaliation against those who report corruption through online platforms is a risk that has to be taken seriously and counter-acted in the implementation of whistleblowing and crowdsourcing tools. Moreover, privacy rights and data protection have to be kept in mind whenever data is published on transparency portals.

Efficient accountability mechanisms as a prerequisite: ICT tools against corruption can increase transparency, mobilise citizens, and help create more effective public administrating. Yet, transparency can be particularly frustrating if there are no institutions to enforce accountability. If citizens report corrupt activities, but no institution is following up on the report, they are likely to only turn away from the political system. They may become alienated and frustrated rather than engaged, and a tool that was intended to be anti-corruption could instead create cynicism and turn citizens against the political system. This risk has to be taken into account when implementing tools that support greater transparency and citizen mobilisation. This statement was supported by several people who were interviewed for this report, as well as previous academic research (e.g. Bauhr and Grimes, 2014). A functioning and independent judiciary, as well as press freedom, are thus in many cases necessary for the success of ICT tools against corruption. This is particularly applicable to tools that promise greater transparency and are aimed at mobilising citizens; those that focus on promoting a more effective public administration are less dependent on these factors.

Support civil society: Civil society organisations are crucial actors in the fight against corruption and are often the ones that make the most use of the benefits provided by ICT anti-corruption tools. Civil society capacity building should thus be part of any project looking to implement such tools. This includes not only direct support of such organisations, but also providing them with training of how to properly use ICT tools. This can mitigate potential risks, such as the ones outlined above. In the context of data provided through transparency platforms or crowdsourcing initiatives, training on data analysis and visualisation can help civil society organisations to leverage such data in their work against corruption. The implementation of ICT against corruption thus should always look at the potential users and benefactors of these tools and provide capacity building as needed to support their success.

Assure government buy-in: The BMZ's Strategy Paper on anti-corruption rightfully notes that anti-corruption measures are particularly helpful in contexts where political will exists to implement them. This holds to be particularly true for ICT anti-corruption tools. Crowdsourcing platforms are only effective, and will only be sustainable, if citizen reports have an effect. To achieve this, they either have to be used to prosecute public officials or to initiate public service reforms, steps which can only be taken if the government supports the aims of such a project. IPaidABribe, for instance, involves so-called Janayuktas, former and current government employees, as vigilant officers that make sure

that reports submitted via the platform are followed-up by the respective government institutions. This institution helps create trust on the side of citizens that their reports actually have a purpose, as well as on the side of the government as a way of ensuring the reports transferred to them are legitimate.

Similarly, transparency platforms depend on governments providing accurate data and being willing to be subject to citizens' scrutiny. ICT tools against corruption, while often implemented by civil society partners, should ideally involve the government in the implementation of such tools. Several successful projects using ICT against corruption, such as the Ukrainian public procurement portal ProZorro, started as civil society-driven initiatives that have since been transferred to the authority of the government. Government buy-in and the integration of ICT tools in a wider anti-corruption strategy are both essential preconditions for successful anti-corruption projects.

The process of securing buy-in from bureaucrats can be challenging. Anti-corruption tools often involve disseminating information on government activities directly to citizens, which can cause officials to feel uncomfortable or like they're not in control of their own data, particularly when they aren't the ones who have designed the tool. Implementers of anti-corruption ICT tools should keep this in mind and be prepared to convince officials that increased transparency does not have to be seen as a threat to the government's control.

Legal framework needs to be considered: Similar to government buy-in, some tools require a specific legal framework in order to be effective. This includes guarantees for a free press or freedom of opinion, as publications about corruption can otherwise be used against those who publish them, especially as they often criticise the government. Transparency platforms need legal frameworks to back-up data publication and, for instance, the right to freedom of information. Whistleblowing platforms have to take into account (the lack of) legislation to protect whistleblowers. In some legal contexts, anonymous whistleblowers are not protected by legislation. In others, protection only applies to whistleblowing within an organisation. Project designers have to take such frameworks into consideration.

Effective strategy for publicising ICT anti-corruption tools: Successful tools need attention; they can only have an impact if many citizens know about the existence and the functioning of these platforms: An e-government innovation is meaningless if citizens don't know it exists or understand what it is to be used for, and a crowdsourcing platform has no *raison d'être* without a populace to contribute content. Developers of ICT tools should not take it for granted that the mere existence of a digital solution means people will flock to it. Successful projects thus need to be continuously advertised so that they enter and remain in the public consciousness. For this reason, an effective strategy for publicising ICT anti-corruption tools needs to be part of any potential project. This can include government support, social media campaigns, or even music or TV stars promoting the tool.

5.2 Recommendations for specific ICT anti-corruption tools

Several of the tools outlined above are not or were not conceptualised as exclusively anti-corruption tools. As such, they often require some amount of adaptation to fit this purpose.



1. E-government and digital public services

E-government tools have to equally take into account usability both for citizens and for public officials working with these tools. Often, they are created having citizens in mind. This is good, as they need to be accepted by citizens in order to be successfully used. Crucially, however, public officials are the ones who implement e-government tools and have to work with them on a daily basis. Instead of seeing it as a positive step toward a more just or efficient government, officials are likely to see it as simply a hindrance and they will likely avoid using the tool if possible. For this reason, it is critical to focus on usability from a civil service perspective in addition to a citizen perspective. Furthermore, the creation of parallel systems should be avoided at all costs, as this leads to confusion as to what the tool is actually useful for as well as decreases the likelihood civil servants will actually use the tool diligently. Tools should thus be designed to complement or replace existing workflows rather than work alongside and in addition to them. Further, these digitised public services have to be squared with a system that must nevertheless remain accessible to those who lack digital skills (e.g., senior citizens) and/or internet access. This provides a significant challenge to designers and developers of e-government solutions.



2. Crowdsourcing platforms

As already highlighted above, crowdsourcing platforms need to secure cooperation with different government institutions and secure their buy-in for the use of this tool. In order to secure the possibility of following-up on reports, they should also give the option for those reporting to be tracked via some form of unique ID that allows for follow-ups and, if necessary, for the reporter to waive their anonymity and provide their name.

This allows the implementing partner of such a project to follow-up on reports and, potentially, initiate prosecution against corrupt officials. IPaidABribe furthermore also encourages citizens to report honest officials, creating an incentive to act honestly – an option that should be considered by those designing localised crowdsourcing platforms.



3. Whistleblowing platforms

The success of whistleblowing platforms directed against corruption depends greatly on the local context, and in particular, on the institutions used for accountability and the existing legal framework. Furthermore, they have a difficult balance to strike between safety for the whistleblower, usability, and the quality of the information submitted. These platforms do not strive for a large number of submissions, as going through all of them would be too labour-intensive for local partners. Rather, they aim for high-quality, detailed submissions so that documents can be used to prosecute corrupt acts. Accordingly, submission systems should require a longer questionnaire than would be advisable from a mere usability perspective. This ideally both increases the quality of submissions and decreases the number of hasty or even erroneous submissions. The implementations of these systems also need a sufficient amount of local technical knowledge, especially as projects should ideally be hosted on a local and decentralised server infrastructure.



4. Transparency platforms

As already pointed out earlier, transparency platforms used in an anti-corruption context need accountability mechanisms in order to do more than just frustrate citizens. Critically, they need government cooperation, which also assures that the data displayed on these platforms is accurate and that the government is willing to respond to freedom of information requests. Platforms also have to take the legal framework into account and, for instance, ensure respect for the right to privacy for public officials to the extent that this is established in local laws. Certain government data is particularly applicable to the fight against corruption: public procurement data and government contracts can be scanned for abnormalities, conflict of interest registers can be independently analysed, and beneficial ownership registers can help to reveal conflict of interests by public officials. Data publication should ideally take open data principles¹³ into account to enable journalists and civil society leaders to analyse provided data easily. This includes the possibility of linking different datasets, which would make it possible to analyse the beneficial ownership of companies involved in public procurement, for example.

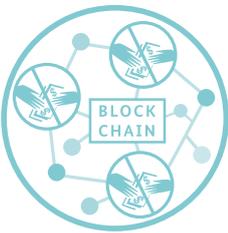
¹³ See, for instance, principles outlined by the Open Data Charter at <https://opendatacharter.net/>



5. News reporting and dissemination platforms

As these platforms can be as simple as a blog or a basic website, they are very easy to set up. Most news reporting websites now also use social media in order to increase traffic. Their challenge is to be active in what are often very challenging media environments.

As they report news about corruption and anti-corruption reforms, these news projects have to make sure to also report positive news. Without this, they risk creating fatalism and cynicism amongst their readers. Anti-corruption needs to also include a positive message about the possibility for change and reform.



6. DLT & blockchain technology

As there are no prominent successful use cases of blockchain technology in anti-corruption, its implementation in this context has to be supported with great care. Blockchain certainly has the possibility to create trust in institutions and make public service delivery more effective. The smart contracts the technology enables can be used to avoid manipulation and fraud. Particularly relevant for GDC's work is that this technology can be used to track spending of donor money and bring greater transparency and accountability to this process, which could help advance the goals of the BMZ-supported International Aid Transparency Initiative. But the novelty of the technology presents challenges. Public servants relying on blockchain technology need to understand the underlying technology in order to be able to trust it. The concept of a smart contract has to be understood by all contract partners. Setting up a system where contracts are effectively enforced also requires local technical expertise. The choice of potential project partners has to reflect this factor.

Appendices

Appendix I: References

- Andersen, T. B.** (2009). E-Government as an anti-corruption strategy. *Information Economics and Policy*, 21(3), 201-210.
- Bardhan, P.** (1997). Corruption and Development: A Review of Issues. *Journal of Economic Literature*, 35(3), 1320-1346.
- Bauhr, M., & Grimes, M.** (2014). Indignation or resignation: the implications of transparency for societal accountability. *Governance*, 27(2), 291-320.
- Bertot, J. C., Jaeger, P. T., & Grimes, J. M.** (2010). Bertot, John C., Paul T. Jaeger, and Justin M. Grimes. "Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government information quarterly*, 27(3), 264-271.
- Davies, T., & Fumega, S.** (2014). Mixed incentives: Adopting ICT innovations for Transparency, Accountability, and Anti-Corruption. Bergen: U4 Anti-Corruption Research Centre.
- Elbahnasawy, N. G.** (2014). E-government, internet adoption, and corruption: an empirical investigation. *World Development*, 57, 114-126.
- Federal Ministry for Economic Cooperation and Development.** (2012). Anti-Corruption and Integrity in German Development Policy: A Strategy. Bonn: BMZ. Retrieved January 15, 2018, from http://www.bmz.de/en/publications/archiv/type_of_publication/strategies/Strategiepapier323_04_2012.pdf
- Federal Ministry for Economic Cooperation and Development.** (2016). Toolkit – Digitalisation in Development Cooperation and International Cooperation in Education, Culture and Media. Bonn, Berlin: BMZ. Retrieved September 10, 2017, from <https://www.giz.de/fachexpertise/downloads/bmz2016-en-toolkit-digitalisation.pdf>
- Federal Ministry for Economic Cooperation and Development.** (2017). Harnessing the Digital Revolution for Sustainable Development: The Digital Agenda of the BMZ. Bonn, Berlin: BMZ. Retrieved September 10, 2017, from https://www.bmz.de/en/publications/type_of_publication/information_flyer/information_brochures/Materialie276_digitale_agenda.pdf
- Fox, J.** (2007). The uncertain relationship between transparency and accountability. *Development in practice*, 17(4-5), 663-671.
- GIZ.** (2017). Anti-Corruption and Integrity. Retrieved November 10, 2017, from Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH: <https://www.giz.de/expertise/html/5394.html>
- Gurin, J.** (2014). Open governments, open data: A new lever for transparency, citizen engagement, and economic growth. *SAIS Review of International Affairs*, 34(1), 71-82.

- Heald, D.** (2006). Varieties of transparency. *Proceedings of the British Academy*, 135, 25-43.
- International Telecommunication Union.** (2017). *ICT Facts and Figures 2017*. Geneva: International Telecommunication Union. Retrieved September 28, 2017, from <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf>
- Kim, K., & Kang, T.** (2017). Does Technology Against Corruption Always Lead to Benefit? The Potential Risks and Challenges of the Blockchain Technology. 2017 OECD Global Anti-Corruption and Integrity Forum. Paris: OECD.
- Kim, S., Kim, H. J., & Lee, H.** (2009). An institutional analysis of an e-government system for anti-corruption: The case of OPEN. *Government Information Quarterly*, 26(1), 42-50.
- Klitgaard, R.** (1988). *Controlling Corruption*. Berkeley: University of California Press.
- Kossow, N., & Kukutschka, R. M.** (2017). Civil society and online connectivity: controlling corruption on the net? *Crime, Law, and Social Change*, 1-18.
- Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A.** (2016). Making smart contracts smarter. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, (pp. 254-269).
- Marquette, H., & Peiffer, C.** (2015, January). *Corruption and Collective Action*. Developmental Leadership Program Research Paper, 32. Retrieved September 10, 2017, from University of Birmingham: <http://publications.dlprog.org/CorruptionandCollectiveAction.pdf>
- Mungiu-Pippidi, A.** (2011). *Contextual Choices in Fighting Corruption: Lessons Learned*. Oslo: NORAD. Retrieved July 17, 2017, from <https://www.norad.no/en/toolspublications/publications/2011/contextual-choices-in-fighting-corruption-lessons-learned/>
- Nakamoto, S.** (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved September 11, 2017, from <https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/bitcoin.pdf>
- Ndou, V.** (2004). E-government for developing countries: opportunities and challenges. *The electronic journal of information systems in developing countries*, 18.
- NORAD.** (2009). *Anti-Corruption Approaches: a Literature Review*. Oslo: Norwegian Agency for Development Cooperation. Retrieved January 13, 2018, from <https://www.norad.no/en/toolspublications/publications/2009/anti-corruption-approaches-a-literature-review/>
- Open Knowledge International.** (2017). *Open Data Handbook*. Retrieved September 10, 2017, from <http://opendatahandbook.org/>
- Persson, A., Rothstein, B., & Teorell, J.** (2013). Why anticorruption reforms fail: systemic corruption as a collective action. *Governance*, 26(3), 449-471.
- Rose-Ackerman, S.** (1978). *Corruption: A Study in Political Economy*. New York: Academic Press.
- Serrat, O., & Ear-Dupuy, H.** (2014). *Fighting Corruption with ICT: Strengthening Civil Society's Role*. Manila: Asian Development Bank.

- Shim, D. C., & Eom, T. H.** (2008). E-government and anti-corruption: Empirical analysis of international data. *International Journal of Public Administration*, 31(3), 298-316.
- Starke, C., Naab, T. K., & Scherer, H.** (2016). Free to Expose Corruption: The Impact of Media Freedom, Internet Access and Governmental Online Service Delivery on Corruption. *International Journal of Communication*, 4702-4722.
- Sturges, P.** (2004). Corruption, Transparency and a Role for ICT? *International Journal of Information Ethics*, 2(11), 1-9.
- U4 Anti-Corruption Research Centre.** (2013). Technological innovations to identify and reduce corruption. U4 Expert Answer 376.
- U4 Anti-Corruption Research Centre.** (2016). Literature review: The use of ICTs in the fight against corruption. Bergen: U4 Anti-Corruption Research Centre.
- Ugur, M., & Dasgupta, N.** (2011). Corruption and economic growth: A meta-analysis of the evidence on low-income countries and beyond. London: EPPI-Centre, Social Science Research Unit, Institute of Education, University of London.
- United Nations.** (2005). Compendium of Innovative E-Government Practices. New York, NY: United Nations. Retrieved September 8, 2017, from <http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN022196.pdf>
- United Nations Office on Drugs and Crime.** (2016). The use of information and communications technologies for the implementation of the United Nations Convention against Corruption. 7th intersessional meeting of the open-ended intergovernmental Working Group on Prevention. Vienna: UNODC. Retrieved September 2017, 10, from https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/workinggroup4/2016-August-22-24/Presentations/UNODC_-_Mr._Constantine_PALICARSKY.pdf

Appendix II: List of projects

The projects listed below were researched as part of the desk research that informed this report. While this is a comprehensive list of ICT anti-corruption tools, it is, by far, not an exhaustive list of all such tools that were developed in the past. Several projects were found that were only short lived or could not be classified as ICT anti-corruption tools, even though they might have some potential for this field.

Project Name	Country	Category	Website
Exonum (Bitfury)	Georgia	Blockchain	http://bitfury.com/
TruBudget	Africa	Blockchain	https://www.kfw.de/KfW-Group/Newsroom/Latest-News/Press-Releases/Pressemitteilungen-Details_426112.html
TRIMS	Nigeria	Crowdsourcing	http://www.streamhouse.org/service/trade-route-incident-management-system-trims/
IPaidABribe	India	Crowdsourcing	http://www.ipaidabribe.com/
BribeSpot	Thailand	Crowdsourcing	http://techpresident.com/news/wegov/24290/bribespot-thailand-effective-anti-corruption-tool-or-mere-outlet-disgruntled-victims
Prijavi Korupcija	Macedonia	Crowdsourcing	https://transparency-watch.org/reports
Bribeline	Worldwide	Crowdsourcing	
Piata de Spaga	Romania	Crowdsourcing	https://www.piatadespaga.ro/
FixMyStreet	UK	Crowdsourcing	https://www.fixmystreet.com/
Edosa Fakelaki	Greece	Crowdsourcing	http://www.edosafakelaki.org/
Fizettem	Hungary	Crowdsourcing	http://www.fizettem.hu/
Yosoborno	Colombia	Crowdsourcing	http://yosoborno.com/
Toidihoilo	Vietnam	Crowdsourcing	http://www.toidihoilo.com/
Ushahidi	Kenya	Crowdsourcing	https://www.usshahidi.com/
Not In My Country	Uganda	Crowdsourcing	http://anticorruptionintl.org/campaigns/
Odisha State Grievances Redress Portal	India	E-Gov	http://cmgcodisha.gov.in/
Jaga App	Indonesia	E-Gov	http://www.thejakartapost.com/news/2016/12/01/kpk-launches-mobile-app-promoting-public-service-transparency.html
Government of Estonia	Estonia	E-Gov	https://e-estonia.com/
Various eProcurement Platforms	Worldwide	E-Gov	
OPEN	Korea	E-Gov	https://seoulsolution.kr/en/content/e-government-seoul-opens-new-chapter-transparency-efficiency-and-public-participation
Kerala E-District	India	E-Gov	https://edistrict.kerala.gov.in/
Bhoomi Project	India	E-Gov	https://landrecords.karnataka.gov.in/service0/
IPCRM	Kenya	E-Gov	http://www.eacc.go.ke/WHATSNEW.ASP?ID=632&-day=3/4/2015

Project Name	Country	Category	Website
ACID	Nigeria	News Reporting	
K-Monitor	Hungary	News Reporting	http://www.k-monitor.hu/
Sithi	Cambodia	News Reporting	
ACCH	Indonesia	News Reporting	https://acch.kpk.go.id/id/
Ni Korupciji	Ukraine	News Reporting	http://nikorupciji.org/
DIGIWHIST	EU	Transparency	http://digiwhist.eu/
Frag den Staat	Germany	Transparency	https://fragdenstaat.de/
Open Corporates	Worldwide	Transparency	https://opencorporates.com/
OpenBudgets	Worldwide	Transparency	http://openbudgets.eu/
Verejne Firmy	Slovakia	Transparency	http://firmy.transparency.sk/index.php
Dinero y Politica	Argentina	Transparency	http://dineroypolitica.org/
Alaveteli	Worldwide	Transparency	http://alaveteli.org/
OpenSpending	Worldwide	Transparency	https://openspending.org
WhatDoTheyKnow	UK	Transparency	https://www.whatdotheyknow.com/
InfoMex	Mexico	Transparency	https://www.infomex.org.mx/gobiernofederal/home.action
Peruvian Transparency Portal	Peru	Transparency	http://www.transparencia.gob.pe/
Brazilian Transparency Portal	Brazil	Transparency	http://www.transparencia.gov.br/
US OD Portal	US	Transparency	https://www.data.gov/
Kenya OD Portal	Kenya	Transparency	http://www.opendata.go.ke/
MCP	Indonesia	Transparency	
Anonymoous Whistle-blowing Platform	Kenya	Whistleblowing	https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=111KACC33&language=eng
GlobalLeaks	Worldwide	Whistleblowing	https://www.globaleaks.org/
KPK Whistleblower's System	Indonesia	Whistleblowing	https://kws.kpk.go.id/

As a federally owned enterprise, GIZ supports the German Government in achieving its objectives in the field of international cooperation for sustainable development.

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH
Registered offices
Bonn and Eschborn
Division Global Policy, Governance
Section Governance, Human Rights

Anti-Corruption and Integrity Programme
Friedrich-Ebert-Allee 36
53113 Bonn, Germany
T +49 228 44 60-0
F +49 228 44 60-17 66

Dag-Hammarskjöld-Weg 1-5
65760 Eschborn, Germany
T +49 61 96 79-0
F +49 61 96 79-11 15
E anticorruptionprogramme@giz.de
I www.giz.de

Responsible:
Nicole Botha | Anti-Corruption and Integrity Programme

Authors:
Niklas Kossow | Hertie School of Governance
Victoria Dykes | Technologiestiftung Berlin

Contact:
René El Saman | Anti-Corruption and Integrity Programme
Särije Nadji Rafat | Anti-Corruption and Integrity Programme

Design und Layout:
Barbara Reuter | Oberursel | barbarareuter-grafik@web.de

URL links:
This publication contains links to external websites. Responsibility for the content of the listed external sites always lies with their respective publishers. When the links to these sites were first posted, GIZ checked the third-party content to establish whether it could give rise to civil or criminal liability. However, the constant review of the links to external sites cannot reasonably be expected without concrete indication of a violation of rights. If GIZ itself becomes aware or is notified by a third party that an external site it has provided a link to gives rise to civil or criminal liability, it will remove the link to this site immediately. GIZ expressly dissociates itself from such content.

On behalf of
German Federal Ministry for Economic Cooperation and Development (BMZ)
Division 301: Sectoral and thematic policies; governance, democracy; rule of law
Bonn

GIZ is responsible for the content of this publication.

Eschborn/Bonn March 2018



Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn, Germany

Friedrich-Ebert-Allee 36 + 40
53113 Bonn, Germany
T +49 228 44 60-0
F +49 228 44 60-17 66

Dag-Hammarskjöld-Weg 1 - 5
65760 Eschborn, Germany
T +49 61 96 79-0
F +49 61 96 79-11 15

E info@giz.de
I www.giz.de

On behalf of



Federal Ministry
for Economic Cooperation
and Development