STEPPING UP THE GAME:

Digital technologies for the promotion of the fight against corruption – a business perspective

CONTENTS

EXECUTIVE SUMMARY

Business at OECD has been actively calling on the OECD to consider the role digital technologies in the fight against corruption. This call was ultimately reflected in the preamble of the revised OECD Anti-Bribery Recommendation adopted in 2021, which recognizes 'the potential role of innovative technologies in advancing public and private sector efforts to combat foreign bribery'.

Against this backdrop, and in light of a growing emphasis on the use of digital technologies in both the public and private sectors, the *Business at OECD* Anti-Corruption and Digital Economy Policy Committees launched a novel project in March of 2022, with the aim to assess the role that digital technologies can play in anti-corruption efforts, focusing on private sector applications and pathways to implementation. These efforts galvanized in the development of this paper on «Stepping up the game: Digital technologies to promote the fight against corruption - a business perspective».

The first part of the paper provides an extensive literature review explaining and highlighting different technologies and their application in anti-corruption efforts both in the public and private sectors. It also highlights potential limitations and challenges related to these technological approaches. To provide unique insights and add to existing literature, the second part of this paper draws on a collection of use cases provided by our global business community, showcasing how companies are already actively using digital technologies to improve their risk management and compliance programs. Building on these insights, the paper further identifies success factors and barriers to implementing digital anti-corruption solutions in practice. Our analysis thereby focuses on the internal adoption process, efforts to ensure management and staff buy-in, the complementary role of governments, and approaches to fostering acceptance and trust.

Key success factors identified include, amongst others, adequate support and financial commitments by the part of the top management, structured and target-oriented approaches to the introduction of a given digital solution, sound training, clear communications with both employees and stakeholders on the (ideally quantifiable) benefits of the application, transparency on how eventual risks and data privacy are managed, a user-focused design, flexibility to improve and adapt according to feedback from end users as well as collaboration across supply chains, with other companies, and/or with the public sector in the form of public-private partnerships. Key obstacles include the availability and harmonization of data, diverging expectations and legal requirements on individual digital solutions, reluctance to embrace change, and lack of management support and buy-in for investments in new innovative compliance approaches.

Business at OECD, therefore, recommends that the OECD help raise awareness for the role of technology in the fight against corruption, promote digitalization of public sector processes (including through the use of public-private partnerships) and support the uptake of digital solutions in the private sector by helping to establish an enabling digital environment for companies.

PART I: THE FIGHT AGAINST CORRUPTION IN THE DIGITAL

Introduction

From the wide adoption of the internet to the introduction of digital finance and smartphones, connected devices, and the Internet of Things (IoT), digitalization has changed how we engage, interact, and do business. Even more so, digitalization has been removing boundaries and borders, unleashing what has been depicted as a 'digital revolution' giving way to a 'digital age'. And yet, the latest developments in blockchain technology, artificial intelligence, and big data analytics are promising to have many more such transformative impacts on our economies and societies going forward.

Against this backdrop, businesses and governments have increasingly been adopting digital solutions, with the experiences of the Covid-19 pandemic only adding further momentum to across the board digitalization. For the fight against corruption, the emergence of digital tech may entail a range of new opportunities. Digital tools offer governments and businesses new and potentially more effective solutions to prevent, monitor and investigate bribery and other forms of corruption. Yet, at the same time, digital approaches may also open new pathways and loopholes for corrupt behavior.

The business case against corruption

Corruption, in all its forms, can have disastrous effects on people, undermining the rule of law, eroding trust in institutions, leading to inefficient allocations of goods and services, and impeding free choice and equal opportunities. Importantly, corruption often has a disproportionate impact on the most vulnerable, who are struggling with increased costs and reduced access to basic services. At the same time, corruption may also create an environment that is permissive of human rights abuses. Fighting corruption is therefore a priority for safeguarding cohesion and fairness in any society.

Yet, besides obvious ethical obligations and human rights considerations, efforts to fight and eliminate corruption are clearly in the best interest of business. From the perspective of a single company, preventing corruption is a critical component of risk management aiming to prevent scandals, legal proceedings, financial penalties, or fines that could create not only financial damage but also injure a company's reputation or lead to debarment from government contracts.

At the market level, efforts to fight corruption are a prerequisite to ensuring fair competition and a level playing field for all. From a macro-economy point of view, corruption - or a high perception thereof - undermines an enabling business environment and disincentivizes people to take stakes and invest, which ultimately hampers growth and innovation.

Furthermore, as our economies and businesses are experiencing increasing supply chain disruptions, it becomes all the more important to mitigate risk factors. This includes addressing corruption, which may put the stability of global trade under further pressure.

In short, civil society, governments, and businesses all have a significant interest in fighting corruption. Importantly, though, to effectively curb corruption, all of these actors - civil society, governments, and businesses - must harmonize their collective efforts. To that end, in addition to tackling the so-called 'supply side' of bribery, attention must also be paid to anti-corruption measures in the public sector addressing the 'demand' side of bribery, meaning the public officials receiving or soliciting bribes.

Corruption in public offices not only generates inefficiencies but also undermines trust, equal opportunity, and fair competition, and hinders the promotion of a broader culture of integrity. Efforts to establish clear rules and render public processes more transparent, efficient, and less prone to corruption – including through the use of digital technology - are therefore complementary to private sector efforts.

As the official representation of the private sector at the OECD, *Business at OECD* (BIAC) advises the organization and its member governments on the design of impactful policies by bringing to the table on-the-ground insights and experiences. To that end, we are actively engaging with our global membership on key issues, including in the areas of digital and anti-corruption, with the aim to support the development of OECD analysis and recommendations, while at the same time, pointing to emerging challenges and opportunities on the ground.

The OECD and its Working Group on Bribery can be considered one of the leading organizations in the international fight against corruption. Building on its Anti-Bribery Convention, as well as instruments addressing bribery in the context of State-Owned Enterprise (SOEs), development aid, and export credits, amongst others, the organization provides an international framework for anti-corruption efforts. On top of this, the OECD conducts research and analysis, and hosts its annual Global Anti-Corruption and Integrity Forum, discussing challenges and innovative solutions connected to the broader notion of integrity.

The OECD also provides insightful analyses of the impact of digital technologies on global economies through the work of its Committee on Digital Economy Policy (CDEP) and related Working Parties. The organization has been committed to developing important common principles and frameworks based on shared values, such as the OECD Artificial Intelligence (AI) Principles and the Recommendation on Digital Security of Critical Activities. This work proves critical as the application of digital technologies is continuously expanding, including in corporate governance practices, to enhance productivity, transparency, and efficiency of business activities.

In this context, *Business at OECD* has been calling for a stronger consideration of 'the potential role of innovative technologies in advancing public and private sector efforts to combat foreign bribery', which was eventually reflected in the preamble of the 2021 OECD Anti-Bribery Recommendation. *Business at OECD* is eager to support the development of further work on this issue and is keen to provide tangible insights on the use of tech for anti-corruption from the private sector. These efforts are also in line with focus area 3 of the *Business at OECD* Anti-Corruption Committee's strategic priorities framework ("Digital solutions") and point 7 of the Committee's 18th SDG Manifesto («Tech for trust»).

Helping companies leverage the potential of digital tech in the fight against corruption

Covid-19 lockdowns forced companies and governments alike to accelerate the transition to the digital space, reinforcing a trend towards increasing digitalization, which had already started before and which profoundly transformed sectors and operations across the board, including the anti-corruption field. Many businesses have already for some time been deploying digital technologies to improve their risk management and compliance programs, while governments have been exploring e-government solutions to manage the deployment and allocation of public services and benefits.

At the same time, the attention on the nexus between the digital and anti-corruption agendas is continuously growing, which is confirmed by several international fora, such as the B20 and the G20, as well as global business initiatives taking up the issue in their respective topics in their agendas.

Yet, existing work often focuses on descriptive analysis of applications and their benefits, considering deployment in the public sector, whereas concrete examples and experiences with the deployment of technology for anti-corruption in the private sector remain scarce.

The objective of this paper is therefore to initiate a debate around the 'how' - How can companies take advantage of digital technology? How do they approach the issues? And how can policies support them in this endeavor? The OECD can play an important role in this regard, championing multidisciplinary thanks to its expertise in a wide range of interconnected socioeconomic issues, including digital technologies and anti-corruption.

In short, this paper aims to:

- Assess the role played by digital tech in the fight against corruption.
- Present an overview of existing literature.
- Showcase private sector use cases.
- Draw learnings from existing applications of digital technologies for anti-corruption.
- Explore pathways for public-private collaboration.
- Identify success factors, as well as challenges, to the implementation of digital solutions.
- Present recommendations on how the OECD can help promote the use of digital solutions to fight corruption in both the public and the private sectors.

General remarks:

This policy paper is intended to be a 'living document', which will be updated in line with new emerging trends and developments in the field. The focus of this policy paper is on the potential of technology for the fight against corruption. We thereby acknowledge the need to ensure ethical and responsible use of such technology to prevent potential challenges and risks (see 2.3.) We further recognize that there may be limitations to the role that technology can play in the fight against corruption (see 2.3.). There remains an urgent need to foster awareness and investments in prevention as well as education. That said, technology should be considered as one avenue within a broader anti-corruption toolbox. In other words, while technology can help identify and prevent bribery and corruption, it is important that actual instances of corruption are addressed and investigated, both on the demand and supply side of the transaction concerned. Finally, Business at OECD does not intend to issue specific recommendations for any selected technologies or the providers thereof.

1.1 LINKS BETWEEN ANTI-CORRUPTION EFFORTS AND DIGITAL TECHNOLOGY

The use of new technologies against corruption is on the rise

The role of new technologies in fighting corruption is receiving more and more recognition. While the literature on the issue is growing (see Annex), the potential of technology for anti-corruption purposes is also receiving increased recognition in the international policy debate. The 2020 B20 Saudi Arabia Integrity and Compliance Task Force, for example, advocated for leveraging emerging technologies to manage risks relating to corruption and fraud, whereas the G20 Anti-Corruption Working Group (2021) included in its action plan a commitment to: "Identifying the opportunities and risks of new technologies: sharing experiences and best practices relating to opportunities and risks of new technologies in relation to corruption".

What is corruption?[1]

Corruption does not have a universal definition but is defined by different laws applicable to respective jurisdictions. Commonly recognized actions include "active or passive misuse of the powers of public officials or managers (appointed or elected) for private, financial or other benefits[2]". Corruption can be classified as "grand", "petty" and "political" and it can take many forms including bribery, extortion, nepotism, embezzlement, and fraud. Corruption is also a precursor of money laundering.

Grand, petty, and political corruption:

Corruption does not have a universal definition but is defined by different laws applicable to respective jurisdictions. Commonly recognized actions include "active or passive misuse of the powers of public officials or managers (appointed or elected) for private, financial or other benefits[2]". Corruption can be classified as "grand", "petty" and "political" and it can take many forms including bribery, extortion, nepotism, embezzlement, and fraud. Corruption is also a precursor of money laundering.

Grand corruption consists of high-level government acts that distort policies or the central functioning of the State, enabling leaders to benefit at the expense of the public good.

Political corruption is a manipulation of policies, institutions, and rules of procedure in the allocation of resources and financing by political decision-makers, who abuse their position to sustain their power, status, and wealth.

Petty corruption refers to the everyday abuse of entrusted power by low- and mid-level public officials in their interactions with ordinary citizens, who are often trying to access basic goods or services in places like hospitals, schools, police departments, and other agencies.

Some expanded characterizations of corruption[3]:

Bribery refers to the offering, promising, giving, accepting, or soliciting of an advantage as an inducement for an action that is illegal or a breach of a legal obligation. Inducements can take the form of gifts, loans, fees, rewards, or other advantages (taxes, services, donations, favors, etc.). There is a 'supply' side to bribery (the act of offering, promising, or giving a bribe) and a 'demand' side to bribery (which relates to accepting, receiving, or demanding bribes).

Extortion denotes the act of a public official threatening to use (or abuse) State power to induce the payment of a bribe.

Conflicts of interest arise when there is a situation of conflict between the private interests and the official responsibilities of a person in a position of trust.[4]

Illegal Gratuities refer to the offering of something of value to a public official because of their actions, creating a climate where public officials consider potential gratuities when making decisions or taking actions.

Nepotism and Cronyism describe instances where jobs or benefits are illegally channeled to family and friends for the benefit of the decision-makers' own interests.

Embezzlement refers to the appropriation of funds and the diversion of their use.

[1] *Business at OECD* (BIAC) and IOE (2020), Connecting the anti-corruption and human rights agendas: Guide for business and employers' organizations
[2] OECD Glossary of Statistical Terms, Corruption
[3] ACFE Fraud Tree
[4] Merriam Webster online dictionary

What is digital tech?

Digitalization is the use of digital technologies and data, as well as interconnections, that result in new activities or changes to existing activities.[5]

Digitization is the conversion of analog data and processes into a machine-readable format.

Digital technologies are electronic tools, systems, devices, and resources that generate, store, or process data. Well-known examples of their application include social media, online games, and mobile phones. Digital technologies have considerably speeded up data transmissions, transforming the way people communicate and work.[7]

Digitization transformation refers to the economic and societal effects of digitization and digitalization.[8]

Cloud computing is a service model that provides flexible, on-demand access to a range of computing resources. Clients access such resources (e.g., software applications, storage capacity, networking, and computing power) online.[9]

The Internet of Things (IoT) refers to an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world. The IoT includes automation from smart home devices and appliances, wearables, and health monitors, to advanced applications like connected and autonomous vehicles.[10]

Artificial intelligence (AI) is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are based on the collection of data. With the help of these data, AI produces a model of the environment, and with the help of algorithms, AI interprets this environment. Thanks to increased storage capacity and the possibility to analyze large quantities of data (big data), AI increasingly uses machine learning (defined below). AI has pervasive, far-reaching, and global implications that are transforming societies, economic sectors, and the world of work, and that are likely to increasingly do so in the future.[11]

Machine Learning (ML) is a set of techniques that allow machines to learn in an automated manner through patterns and inferences, rather than through explicit instructions from a human. This has led to a considerable increase in the potential of AI in making predictions and decisions.[12]

Big data commonly refers to data characterized by high volume, velocity, and variety. It benefits from the IoT, among other technologies, as a source of data and from cloud computing as a source of processing power. While large quantities of data can have value in themselves, most of their value depends on the capacity to extract information from this data. Big data analytics techniques and software tools are used, for example, for machine learning.[13]

[5] OECD. (2019c). Going Digital: Shaping Policies, Improving Lives. https://doi.org/10.1787/9789264312012-en; OECD. (2020). Digitalisation and Responsible Business Conduct: Stocktaking of policies and initiatives. Digitalisation and Responsible Business Conduct (oecd.org)
[6] OECD. (2019c). Going Digital: Shaping Policies, Improving Lives. https://doi.org/10.1787/9789264312012-en
[7] OECD. (2020). Digitalisation and Responsible Business Conduct: Stocktaking of policies and initiatives. Digitalisation and Responsible Business Conduct (oecd.org)
[8] OECD. (2020). Digitalisation and Responsible Business Conduct: Stocktaking of policies and initiatives. Digitalisation and Responsible Business Conduct (oecd.org)
[9] OECD. (2019c). Going Digital: Shaping Policies, Improving Lives. https://doi.org/10.1787/9789264312012-en
[10] OECD. (2016b). The Internet of Things – Seizing the Benefits and Addressing the Challenges. Microsoft Word - InternetOfThings_FINAL.docx (oecd-ilibrary.org) ; OECD. (2019c). Going Digital: Shaping Policies, Improving Lives. https://doi.org/10.1787/9789264312012-en
[11] OECD (2019b). Artificial Intelligence and Responsible Business Conduct. RBC-and-artificial-intelligence.pdf (oecd.org); OECD (2019e). Scoping the OECD AI Principles deliberations of the Expert Group on Artificial Intelligence at the OECD. OECD Digital Economy Papers No. 291. [Title] (oecd-ilibrary.org); OECD. (2020). Digitalisation and Responsible Business Conduct: Stocktaking of policies and initiatives. Digitalisation and Responsible Business Conduct (oecd.org)
[12] OECD. (2020). Digitalisation and Responsible Business Conduct: Stocktaking of policies and initiatives. Digitalisation and Responsible Business Conduct (oecd.org)
[12] OECD. (2019c). Going Digital: Shaping Policies, Improving Lives. https://doi.org/10.1787/9789264312012-en

Blockchain is a technology based on a digital ledger or a spreadsheet that is maintained and stored across a network of computers. The network regularly updates the database in every place it exists so that all copies are always identical. This means that data records are visible and verifiable to everyone in the network ("nodes") and that there is no need for intermediaries to serve as authenticators. New events and transactions are automatically stored in "blocks" which are then chained to one another chronologically, creating a digital record, the so-called "blockchain". Attempts to change the information stored in the block will break the "chain" and alert all nodes in the network. One of blockchain's most widespread applications so far has been for cryptocurrencies. Yet, blockchain is also starting to affect many other sectors, including agriculture, manufacturing, retail, healthcare, energy, transport, and the public sector.

1.2 HOW IS DIGITAL TECH BEING DEPLOYED TO ADVANCE THE FIGHT AGAINST CORRUPTION?

Public sector - Addressing the demand side of bribery

As the digitalization wave is sweeping across all aspects of our daily lives, governments have started to explore ways in which digital tech can support their operations and goals. Partially reinforced by the experiences of the Covid-19 pandemic, during which shifting to interactions in the digital space proved to be a pathway ensuring continuity, governments launched an increasing number of e-government initiatives. Meanwhile, many governments are also considering the 'low-hanging fruits' of open data or are adopting more sophisticated technological solutions such as AI and blockchain for the fight against corruption and bribery.

The following section provides an overview of some of the most important digital tools and technologies and their concrete applications for public sector efforts against corruption.

E-GOVERNMENT

The first step in adopting e-government solutions is to transform analog, paper-based legacy systems into digital, open, and simple systems. In other words, governments first need to digitize data in order to digitalize bureaucratic procedures. This enables governments to increase transparency and accountability, reduce red tape, and curtail direct business-to-government (B2G) interactions between individuals and government officials, which in turn reduces both «demand» and «supply» side opportunities for bribery. Another benefit of governments going digital is the generation of new digital data by authorities, which can provide an important basis for the deployment of data-driven technologies. Such technologies, in turn, can also play an important role in combating corruption, which will be outlined in the next section. Specific examples of e-government tools include platforms that enable direct access to government departments, allowing citizens to obtain information and advice (e-communication with the government) or platforms allowing users to access government services (e-tax filings, e-invoicing, and e-platform for public procurement processes and licensing) . Governments have also used e-government solutions to enable citizens to track the progress of bureaucratic procedures or check the accuracy of data provided by various ministries, with the possibility to report discrepancies.

[14] OECD. (2019c). Going Digital: Shaping Policies, Improving Lives. https://doi.org/10.1787/9789264312012-en

OPEN DATA

Open data can play an important role in the prevention of corruption, enabling the development of platforms that make information about government operations available to the public, thus allowing for more transparency, while also facilitating the tracking of potentially corrupt activities. Open data can find different applications in the public sector. In the context of **public procurement**, which is especially prone to corruption due to its nature of involving large transactions and complex interactions between public officials and companies, open data platforms that are publishing information about tenders can not only reduce B2G exchanges, but they can also enable tracking of potentially corrupt activities. In addition, publicly available information about procurement activities facilitates companies' access to tenders and thereby increases competition. Another pertinent example is the establishment of ultimate **beneficial ownership registers**. Identifying and verifying beneficial owners of companies increases transparency and supports corporate due diligence and risk prevention efforts, provided that challenges related to data privacy and protection are taken duly into account. Finally, open data-based **transparency platforms**, disseminating and providing information about government activities to the public, can also support the identification of instances of corruption and can thus help deter corrupt actions by increasing transparency and inviting greater public scrutiny. In addition, digitally stored and available data may also facilitate **the exchange of data between relevant authorities**, for instance in cases of transnational bribery or asset recovery, as is also recommended in the 2021 OECD Anti-Bribery Recommendation, pointing out the role of technology in mutual legal assistance.

WHISTLEBLOWING PLATFORMS/HIGH-LEVEL REPORTING MECHANISMS

Whistleblowing platforms, specifically high-level reporting mechanisms, provide a way for citizens to report on corruption and wrongdoings on the part of public officials and contribute directly to the fight against «demand» side corruption. Digital solutions can play an important role in making whistleblowing channels more accessible, lowering the psychological barrier associated with reporting, and assuring the protection of those "blowing the whistle». As with more traditional reporting channels, finding a balance between protecting anonymity and ensuring continued cooperation with the whistle-blower to obtain all information is critical. The challenges, therefore, lie in the technologically appropriate design of such platforms.

DIGITAL IDENTITIES

A digital identity encompasses the digitized credentials of a person or entity that enable users to authenticate themselves and others. Digital identities support the fight against corruption by facilitating the verification of individuals (third-party due diligence) in transactions or service delivery and thus enable more effective transaction monitoring and risk management. The European Union, for example, is working on the introduction of a European digital identity for EU citizens, residents, and companies, to be applicable offline and online, as well as in the public and private sectors. In Estonia, the e-ID has already been firmly anchored in people's everyday lives for several years and is used, to pay bills, vote online, sign contracts, shop and access their health data, and much more.

BLOCKCHAIN

Blockchain is often considered to play a vital role in the fight against corruption, offering immu-tability and traceability of data given that changing the information on one part of a blockchain requires changes to the other 'blocks' in the chain. This allows potentially harmful alterations to be identified quickly. Moreover, blockchain spares out the need for intermediaries, while the decentralization of stored information also reduces the risk of hacking or tampering, which can be problematic with centralized government databases. Blockchain can further take the role of a 'base technology', which can find applications in public procurement, but which can also serve as a framework for managing processes such as e-voting, transactions, or the redistribution of public funds.

ARTIFICIAL INTELLIGENCE (AI)

AI technologies are self-learning algorithms that infer patterns and relationships from large amounts of data to accomplish a specific, pre-determined goal. Their ability to rapidly make predictions and reveal hidden patterns and relationships in extensive datasets makes them a valuable tool for corruption risk detection. AI-supported predictive analysis can for example be applied in the prevention of tax evasion. Generally, AI can play an important role in making existing processes more efficient and accurate as well as in analyzing and sorting unstructured information. It is also an essential tool to help authorities improve their data collection and management capabilities leading to an overall improvement in data quality. Another application of AI lies in surveillance technology, or **SupTech**, allowing the public sector to improve its monitoring, analysis, and enforcement capabilities and with that, its abilities to combat corruption and fraud more effectively.

Private Sector - Addressing the supply side of bribery

More and more companies are seeking to improve compliance and monitoring functions with the support of digital tools. Digital tools and technologies such as AI, blockchain, or open data, which have been discussed in the previous section in the context of public sector efforts against corruption, are equally important tools for private sector efforts to increasing transparency, efficiency, and accountability.

In addition, businesses are increasingly seeking opportunities to collaborate and engage in public-private partnerships to expand the support for digital tech solutions, improve culture, and ensure inclusive and effective design. Such public-private collaboration on digital tools can strengthen not only transparency but also trust. To reach a critical mass of support for this 'double anti-corruption effect', however, digital tools must deliver on key aspects such as inclusiveness, economic facilitation, and resilience.

This section provides a brief overview of how different digital technologies can support the fight against corruption in the private sector. Additional approaches and more concrete examples of applications, as well as experiences encountered in the implementation process, are showcased in the annexed collection of use cases.

DATA GENERATION AND ANALYSIS

An important first step in any digitalization strategy is the conversion of information and documents into a digital format – also known as digitization. Digitization may in fact entail several benefits: it is not only the first step towards the application of digital technologies, but it contributes to greater transparency and uniformity, and allows compliance professionals to generate time and cost savings by shifting the focus away from manual processes to more value-adding work, such as identifying new strategies and approaches to strengthen integrity across departments and processes.

E-TRAINING AND DIGITAL COMMUNICATIONS CHANNELS

Digital training platforms can play a key role in enhancing compliance trainings and programs, improving the effectiveness of individual learning, and fostering employee awareness of compliance and anti-corruption efforts. Digital channels can facilitate **awareness raising** and help convey a 'tone from the top', whilst also reminding staff of existing rules and compliance policies and procedures. Employees can also consult existing ethics and compliance guidance in a more straightforward and transparent way via digital channels, such as intranet pages and applications. A potentially more sophisticated application of digital technology for communications purposes is the introduction and use of **«chatbots**[15]**»** based on **artificial intelligence technology.**

[15] Chatbots are also known under names as smart bots, interactive agents, digital assistants, or artificial entities (An Overview of Chatbot Technology | SpringerLink).

These chatbots are trained to respond to questions and dynamically engage in conversations with humans , having been 'fed' with relevant digitized information materials, rulebooks, and internal guidance. Chatbots do not only make compliance information and data more accessible but may also entail cost and time savings for internal compliance programs.

DIGITAL REPORTING CHANNELS

Establishing and promoting whistleblower channels within companies plays a critical role in increasing transparency, promoting shared accountability, and strengthening the internal control system. **Digital whistleblowing platforms,** in turn, provide a simple, easily accessible way for employees to report corruption and wrongdoing within their company. As in the case of digital whistleblowing platforms in the public sector, appropriate design is key to ensure sound whistleblower protection and also enable follow-up with whistleblowers to verify the matter and obtain all necessary information.

DATA-DRIVEN RISK ASSESSMENTS

Technological innovations, particularly improvements in **data analytics** based on AI, big data, and machine learning, can play an important role in improving security and risk management. Data-driven approaches in this area can for instance improve the monitoring of transactions, help identify and flag irregularities, or enable predictive analyses of corruption risk.

TECHNOLOGY-SUPPORTED SUPPLY CHAIN MONITORING

Digital technology, especially blockchain, is often considered an especially promising tool for improving supply chain management. Monitoring supply chains and their associated transactions is becoming all the more challenging as supply chains are becoming increasingly global and complex. Blockchain technology can increase transparency and information availability and mitigate compliance risks within the supply chain by allowing all supply chain participants to have simultaneous access to relevant, real-time data about individual products and sections of the chain. In other words, discrepancies, problems, and irregularities that may be indicative of corruption actions can be uncovered more easily.

FOSTERING COOPERATION BETWEEN PUBLIC AND PRIVATE SECTORS

Public-private cooperation is generally considered to be an effective tool in fighting corruption, but it may be especially important for the design of inclusive and practical digital anti-corruption solutions. The private sector can, for example, help governments digitize their processes, such as e-filing of taxes and e-licensing, by developing breakthrough technologies, improving data collection and analysis, and developing and promoting user-friendly interfaces. While this promotes the effectiveness of the public sector, it is equally beneficial for the private sector: A World Bank report, for instance, confirmed that filling out tax returns electronically significantly reduces private companies' tax compliance costs[16]. Similarly, beneficial ownership registers that have been developed through public-private consultation and cooperation can support corporate third-party due diligence checks and verification of counterparties. In addition, such registers may help companies prevent duplication of efforts and increase the efficiency of their risk management programs. Last but not least, public-private approaches may generally help raise awareness of available digital tools targeted at companies and citizens, thus contributing to their uptake among companies and society more broadly.

[16] World Bank Group. (2016). Digital Dividends

… and the role of civil society

A final aspect to consider, beyond public and private sector applications, is the critical role that technology may play in empowering civil society in the fight against corruption. Digitized information and digital communications tools, for example, can support buy-in for the fight against corruption, educating people about corruption and its negative impact on fairness and cohesion. In addition, open data platforms and transparency platforms allow civil society organizations to better monitor corruption-prone environments, while tools such as digital whistleblowing platforms enable civil society to flag observed or suspected breaches.

1.3. WHAT ARE THE CHALLENGES AND LIMITATIONS RELATED TO DIGITAL TECH SOLUTIONS?

Despite the key role played by digital technologies in supporting the fight against corruption in the public and private sectors, the successful application of different technical solutions hinges on ethical and responsible use thereof, as well as the fulfillment of necessary technical and framework preconditions that enable countries and corporations to make use of digital tools.

To that end, there remain a number of practical factors which may hamper uptake, as well as a range of potential risks that may be associated with novel digital technologies that are poorly governed. In addition, it must be kept in mind that the process of integrating digital technologies into anti-corruption strategies, albeit promising, may also have practical limitations calling for complementary efforts from governments and companies to effectively eradicate corruption.

CHALLENGES AND RISKS

Many digital technologies depend critically on the **availability of complete and quality data**. The quality of open data platforms and blockchains is highly dependent on the information stored and/or integrated in these tools. AI, which is trained on big data, also requires sufficiently large and verified datasets. Incomplete or inaccurate data, on the other hand, can lead to inefficient outcomes, such as biases or the failure of AI to identify new patterns and developments. A key challenge is thus to support governments as well as companies in collecting and managing qualitatively encompassing and correct data.

Increased connectivity, digitization of activities, and expansion of data-intensive government and economic activities are also entailing a number of **security and privacy risks** to account for. It is therefore a priority that governments and companies develop principles that promote digital security to protect activities, people, and society without inhibiting benefits and opportunities of digital innovation.

A related, yet even more fundamental challenge that digital technologies face is **explainability**. Due to their recent emergence and complex nature, technologies such as blockchain and AI are often misunderstood and are quickly associated with potential flaws. This underlines the importance of awareness raising and emphasizes the critical role of transparency and education around the use of digital technologies.

Relatedly, in the absence of clear definitions for emerging digital technologies and a lagging understanding of their workings, **regulation or overregulation** that is quickly introduced may further hinder predictability, legal security, and promotion of innovation.

Another key fundamental challenge is the availability of appropriate **digital infrastructure** to support the implementation of digital solutions. This may range from broad-based access to high-speed

internet connections to the necessary hardware and the availability of smart applications and compatible user devices. In the case of blockchain, large computing capacities are required which may reduce its scalability due to high demands on available infrastructure.

Even if the necessary infrastructure is available, it is equally important to ensure that sound **governance** frameworks for the use of novel digital technologies are in place. This comprises both 'hard' investments in digital security and 'soft' efforts to ensure that digital tech is being applied in an ethical and responsible manner to meet privacy concerns and foster trust.

In addition, **digital skills** are required to put available technology to good use, both on the part of end users and on the part of those overseeing the implementation of those technologies. A lack of education and training emphasizing digital skills can thus create an important barrier to leveraging the potential of digital technologies.

Following the successful adoption of a given technological solution within a given company, businesses may still face challenges related to **the speed of adoption and interoperability** with approaches used by business partners or suppliers. Such lack of alignment may prevent companies from making full use of the potential of digital technologies. On the public sector side, public-private collaboration and **"partnering for the goal"** can play a key role in expanding support for certain digital tech solutions, improving culture, and ensuring inclusive and effective design.

In addition, it must also be borne in mind that digital technologies often require **substantial up-front investments.** To that end, the introduction and adoption especially of more sophisticated technologies may hinge on the availability of an adequate budget. This can represent a significant obstacle to implementation, especially for smaller and medium-sized enterprises facing tighter resource constraints, or companies facing internal cost-cutting pressures.

Finally, while digital technology solutions may play a key role in advancing the fight against corruption, they may also open **new pathways and loopholes for corrupt behavior.** A key concern in the context of blockchain, for instance, is the technology's potential role in facilitating money laundering. Attempts to introduce regulation and establish oversight over blockchain transactions are emerging but remain scattered. Moreover, while cryptocurrencies enable secure publicly visible transactions, the parties involved in those transactions remain anonymous.

LIMITATIONS

In addition to the practical challenges that may arise when adopting digital technologies, it is important to note that while digital technologies can play a key role in improving oversight and supporting corruption prevention, they should not be considered as an end in themselves.

In particular, continued efforts are needed **to address the root causes of corruption**, which often relate to an environment of poor governance and rule of law as well as high prevailing poverty. Governments should address such deficiencies and consider the development (and implementation) of National Action Plans against corruption. Beyond this, governments can foster education and awareness raising in schools and society more broadly. Businesses, too, can invest in awareness raising, fostering a culture of ethics, establishing a strong "tone from the top", and strengthening their corporate compliance programs.

In addition to prevention, it is further critically important **to ensure follow-up and enforcement** in the case of identified cases of corruption. This concerns both the "supply side" as well as the "demand side" of the bribery equation.

Finally, as outlined above, companies may be facing challenges in the adoption of digital approaches given limited human and financial resources, capacities, and overall lower digital literacy and awareness.

PART II. PROMOTING DIGITAL SOLUTIONS

Championing corporate digital anti-corruption solutions

In order to obtain a better picture of how companies are already deploying digital technologies in the fight against corruption, members of the Business at OECD (BIAC) global network were invited to submit use cases showcasing their digital solutions and share their experiences in implementing these technologies in practice.

The collection of use cases was supported by a number of guiding questions, including:

- What specific issue related to anti-corruption is your company/organization aiming to address with digital technology and what technology are you deploying in this regard (the solution)?
- What steps did you take to implement the technology and what hurdles did you encounter in the process? What factor supported implementation?
- What do you think is necessary for management and staff buy-in at the corporate level?
- From your point of view, how can governments support the uptake of digital solutions in companies? Should government and private sector collaborate, and if yes, in what manner?
- How are you managing acceptance across stakeholders to ensure successful adoption of and trust in the technology?

Received use cases originated from a variety of different sectors, ranging from health and life sciences, retail, and consumer goods to telecommunications, information technology, and construction. They included pertinent examples outlining the role of technology in developing mobile verification devices, rationalizing compliance processes and learning, improving risk management and due diligence, including third-party screening and management of stakeholder engagement, developing centralized risk management centers, enhancing reporting tools, for instance on gifts and hospitality, and leveraging information platforms and chatbots that render compliance related information more accessible.

Other use cases illustrated how the adoption of technological solutions can be facilitated by public-private partnerships and multi-stakeholder initiatives, such as the Digital Tools for Rule of Law and Recovery (DT4RR) project. This project promotes digitization in key regulatory areas including Licensing and Permitting and has led to tangible progress in addressing bottlenecks in the Costa Rican construction sector through the implementation of a digital platform that comprehensively verifies permits required for construction processes.

Overview of the use cases

In order to obtain a better picture of how companies are already deploying digital technologies in the fight against corruption, members of the Business at OECD (BIAC) global network were invited to submit use cases showcasing their digital solutions and share their experiences in implementing these technologies in practice.

The collection of use cases was supported by a number of guiding questions, including:

	Application(s) of technology to combat corruption	Digital Technology
Altana	Commerce platform to process public and non-public shipment records and supply chain data points	Technology-supported supply chain monitoring
Amazon	PPPs for improving the transparency of local compliance requirements for MNEs and combating illicit commodity trafficking in global supply chains	Fostering cooperation between public and private sectors, Digital reporting channels
Autostrade per l'Italia	Continuous monitoring system	Artificial Intelligence, Data-driven risk assessments
BRF	Compliance-Chatbots	Digital communication channels
Integrity Distributed	Improvement of algorithms through machine learning, ledger technology, and AI to detect supply side corruption in accounts payable and third-party management systems used by multi-nationals	Data-driven risk assessments
Merck	Third-party risk management; stakeholder engagement and reporting tools	Data-driven risk assessments
Novartis	Pocket-sized, mobile, and application-enabled spectrometric drug sensor to detect falsified medicines	Data generation and analysis
Rolls Royce	Centralized, standardized, and technology-based due diligence, Third-party risk management	Technology-supported supply chain monitoring
Sanofi	Real-time, proactive ethics and compliance with artificial intelligence	Artificial Intelligence
SNAM	Supplier's Compliance Monitoring	Technology-supported supply chain monitoring
Telefonica	Third-party screening; advanced gifts and hospitality reporting tool	Data generation and analysis, Technology supported supply chain monitoring
Unilever	Centralized, smart risk management center	Data-driven risk assessments
Walmart	Multi-stakeholder cooperation for the digitalization of licensing & permitting processes (the Digital Tools for Rule of Law and Recovery (DT4RR) initiative - Costa Rica)	Fostering cooperation between public and private sectors, E-government

The collection of use cases can be found in the Annex. The use cases, as well as bilateral exchanges with members of the *Business at OECD* (BIAC) Anti-Corruption and Digital Economy Policy Committees, served as the basis for the identification of success factors and obstacles in the deployment of technology for anti-corruption purposes presented in the following section.

Interested companies are encouraged to share their experiences and submit their use cases should they wish to support and contribute to this project going forward.

Fostering the uptake of digital technologies in the private sector

Despite the potential for digital technologies to advance the fight against corruption, the uptake of digital solutions remains far from the norm in the private sector. A 2019 survey from the Association of Certified Fraud Examiners, for example, found that only 13 percent of companies were using machine learning or artificial intelligence to fight fraud[17]. While this may also be attributed to smaller companies being less likely to adopt sophisticated digital solutions, lagging awareness of how digital technologies can be implemented may also play a role in explaining these observations.

Building on insights from our collection of use cases, this section of the paper aims to identify success factors as well as obstacles in the implementation of digital anti-corruption solutions. It thereby considers both internal company-level factors and potential complementary actions needed by governments to leverage the full potential of digital solutions.

The internal adoption process

Factors that may support implementation internally may include:

A clear **solutions-oriented reasoning** for implementing new technology, starting with an assessment of bottlenecks/ challenges related to existing processes and grounded in a sound understanding of how a given technological solution can help resolve these issues as well as an assessment of what functional requirements must be met to ensure effectiveness (e.g. by conducting a feasibility study).

In this respect, it is important to ensure that the technological solution does not create additional bureaucracy, that it is smartly designed, and that it becomes embedded in existing processes where possible

Fulfilled hard requirements, such as the availability of necessary hardware and skills necessary to develop and implement technological solutions. Efforts to promote upskilling may be necessary to enable employees to manage and master the application of technical solutions.

A solid **implementation strategy** and a **sound governance structure** supporting the introduction of new technology. This can include setting up dedicated working groups, including experts from different departments, consulting with external experts, and setting clear priorities and objectives.

A building block approach with gradually increasing depth over time can help to progressively develop and streamline a given technological solution while maintaining sustainable investment levels.

An **enabling environment**, both internally and externally. On the company level, the existence of well-developed compliance and internal control systems as well as clearly defined accountabilities within the organization can prove to be strong supporting factors.

[17] https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report

Early stakeholder engagement and **co-ordinated efforts** both internally - **across different divisions** – and externally - **across supply chains and networks** to harmonize data collection and data sharing have been identified as exceptionally important. Such engagement can also help foster broad-based implementation of a given digital solution across different entities.

Whereas obstacles may relate to:

The availability of **quality data and harmonization** of data collection and aggregation. Data is moreover often **confidential and non-public**, which may lead to challenges related to privacy concerns, protection of business sensitive information, etc.

Challenges in **balancing preferences and needs** of users and business stakeholders with **compliance requirements.**

Reluctance to embrace change.

The need to continuously review, adapt and update processes and procedures. This may often be resource-intensive and can be complicated by a dynamic environment with changing risk scenarios.

Management and staff buy-in

Strategies may include:

The right **'tone from the top'**, starting with a strong commitment to strengthen compliance functions and improve anti-corruption efforts. Sustained support and direction from senior management are also key. Relatedly, engaging senior executives and management early in the process of adopting a given technological solution may support broad-based buy-in.

Communicating why a given technological solution is being adopted. This includes promoting the narrative of a strategic investment (not a list of «compliance checks») emphasizing **how enhanced anti-corruption and compliance tools can reduce the risk** of monetary (e.g., legal proceedings), operational (e.g., debarment), and reputational costs arising from wrongdoing. It is equally important to **underline other ways in which the solution may benefit the company** and its processes (time and cost savings, simplification, accessibility, oversight, etc.).

Ensuring transparency. Trust in the technological solution requires full information on its workings and disclosure of how potential risks are being managed.

Engaging with stakeholders at all stages of implementation and tailoring solutions to end users. In this regard, ensuring accessibility, user-friendliness, and efficiency (e.g., speed and accuracy with which information can be accessed or processed) is key.

Providing complementary **training programs,** potentially supplemented by incentives to participate.

While challenges may arise in the context of:

Ensuring management support for additional and potentially costly investments that go beyond existing compliance, risk, and anti-corruption efforts. In other words, convincing management to invest in complex technology for compliance purposes may be more challenging than convincing management to invest in technology for revenue-generating operations (compliance functions being considered as 'cost centers'), especially when seemingly well-functioning risk and compliance frameworks are already in place.

The complementary role of governments

Public sector efforts can support private sector efforts by:

Raising awareness of the harms of corruption and promoting corporate compliance efforts (e.g., providing incentives, and showcasing best practices).

Leading by example, promoting digitalization, and allocating dedicated funds for developing digital infrastructure.

Adopting transparency platforms and digital portals allowing the private sector to monitor activities and access information.

Establishing public databases supplementing information assets of companies and increasing the capacity for data-driven analysis. Publicly driven efforts to promote Ultimate Beneficial Ownership in particular may also play an important role in sporting companies' due diligence and compliance efforts.

Enacting **policy and/or legal reforms** to support digitalization and fostering an **ecosystem** in which the use of digital technologies at the company level is promoted (for instance through the provision of incentives).

Supporting **interoperability** between different technical approaches and fostering the **integration** of company and government solutions.

Providing **guidance** on compliance frameworks, **offering free software or training**, and **streamlining reporting requirements.**

Consultation with the private sector, including for the evaluation of existing and/or planned digital public sector solutions, and exploring the possibility of launching **private-public cooperation.**

Governments can also help promote strategic partnerships with companies and other public sector actors. When working hand-in-hand, the public and the private sectors can further increase the odds of success of digital solutions rendering them more accessible and user-friendly and/or increasing interoperability. Public-private cooperation can also play a critical role in efforts to **foster awareness** of the benefits of digital solutions and **promote education and training** supporting technology uptake. In other words, businesses and governments can work jointly towards creating a broader ecosystem encouraging companies to adopt digital solutions.

Acceptance and trust

Success factors may include:

Embedding the digital solution **within existing business processes** and systems where possible.

Ensuring **full disclosure of relevant information** on the deployment of technical solutions.

Quantifying the impact of a given solution on the achievement of a given company's goals, such as its anti-corruption strategy, in KPIs. Many digital applications, by nature, entail greater measurability, which helps demonstrate the effectiveness of compliance efforts.

Communicating about the workings of the technology and how potential risks are being addressed (including how sensitive data is being protected).

Illustrating the unique value added of a given digital solution and demonstrating how the deployment of the given solution is opening new opportunities that go beyond the potential of standard tools (e.g., time savings, cost savings, simplification, accessibility, oversight, etc.).

Seeking **continuous improvement** of technical solutions and incorporating user feedback for instance by conducting check-ins with end users in order to understand problems and bottlenecks. One approach is to establish a **dedicated oversight mechanism** that reviews KPIs, monitors progress, and flags challenges.

Key policy recommendations for the OECD

OVERARCHING

Develop communications materials on the role of modern digital technologies with a view to **demystifying and educating** about different types of technologies and their applications.

Streamline digital aspects into the organization's work on anti-bribery and develop **further analysis** on the potential of digital technologies in the fight against corruption, while also accounting for potential integrity challenges and exploring pathways to prevent misuse.

FOSTERING THE UPTAKE OF DIGITAL TECHNOLOGY IN THE PUBLIC SECTOR

Promote the **use of digital technology** to support transparency and efficiency **in public sector processes**, thereby also raising awareness of the critical role of consultation, collaboration, and public-private partnerships.

FOSTERING THE UPTAKE OF DIGITAL TECHNOLOGY IN THE PRIVATE SECTOR

Support countries in establishing and ensuring **enabling environments** for private sector efforts to leverage digital tech, including appropriate regulatory frameworks and complementary investments in necessary skills and infrastructure.

Foster **harmonization and cross-border cooperation** on digital aspects as well as on anti-corruption requirements.

USE CASES

Illuminating the global trade and supply chain network - Altana Technologies

The global trading system is the principal global nexus for illicit activities. Any illicit actor - whether engaged in corruption, human rights abuse, or sanctions evasion - must eventually interact with the licit system of international trade in order to move or keep their ill-gotten gains. Global trade and supply chain activity is very difficult to police because the information environment is fractured and opaque, and because supply chains are highly complex and interconnected. Regulators, enforcement agencies, and compliant businesses lack the visibility necessary for systemic enforcement across the global trade and supply chain network.

Altana Technologies is illuminating the global trade and supply chain network. Altana's Trusted Commerce Platform, the Altana Atlas, processes billions of public and non-public shipment records and supply chain data points to create a dynamic network model of the global supply chain, covering the flows of goods through 400 million companies around the world. In order to create a shared source of truth on the global supply chain, it was necessary to somehow unlock, and learn from, sensitive, non-public data. Much of the world's supply chain and B2B data is non-public due to sovereignty, intellectual property, and privacy concerns. Labeled data on known illicit activity is similarly difficult to access for machine learning purposes. The Altana Atlas solves this problem by bringing its platform to siloed data, and not the other way around. Governments, logistics providers, and enterprises each connect to an isolated, dedicated copy of Altana Atlas. The Altana Atlas shares learnings about the supply chain network, and non-compliance across the network, without sharing or pooling each dataset. A unique federated learning architecture makes this possible. The result is a federated, "hub and spoke" learning network across the world's supply chain information, while protecting the confidentiality of the data from each participant.

This visibility and federated machine learning architecture helps solve key problems related to corruption, illicit trade, and human rights abuses, including forced labor.

Fortune 500 corporations, global logistics providers, financial institutions, and government investigators alike are using the Altana Atlas to detect trade-based money laundering and revenue evasion with the assistance of artificial intelligence, detect sanctioned parties doing business through affiliate and trading partner relationships, and map the flows of goods produced with forced labor into the web of the global supply chain.

The world's most important governments, logistics providers, and enterprises are connecting to the Altana Atlas platform to build trusted global business networks. For these organizations, they must feel confident that they are tapping into a unique network of visibility and global compliance intelligence while simultaneously protecting their sensitive data. We are able to show them unprecedented, transaction-level visibility into their direct - and indirect - business relationships globally, and provide them with analytics and pre-trained AI systems that have learned across a global network of proprietary, non-public data, including labeled outcomes on non-compliance.

Public-private collaboration is essential for combating forced labor, corruption, trade-based money laundering, or any type of illicit activity in the global commercial network. The data necessary to root out corruption and illicit activity in global business is held, and siloed, across businesses and governments, who cannot and will not share all of the relevant data directly. Through federated learning, and public-private partnerships that build on the legal and intellectual frameworks of financial KYC/AML compliance, "Trusted Trader" programs for trade facilitation, and defense contracting frameworks, it is possible for public-private partnerships to generate carrot-and-stick incentive structures for businesses to participate in these frameworks. It is therefore technically, commercially, and legally possible to transform the efficacy and reach of systemic anti-corruption and compliance programs throughout the global trade and supply chain network by scaling public-private partnerships premised on federated learning across siloed data.

The critical role of public-private partnerships - Amazon

What specific issue related to anti-corruption is your company/organization aiming to address with digital technology and what technology are you deploying in this regard (the solution)?

Amazon is committed to tackling corruption in commercial operations and global supply chains. We are particularly focused on digital tools that (1) help improve transparency of local compliance requirements (e.g., permits, licenses) for multinational companies operating in foreign markets, and (2) combatting illicit commodity trafficking in global supply chains.

From your point of view, how can governments support the uptake of digital solutions in companies? Should government and private sector collaborate, and if yes, in what manner?

Public-private partnerships (PPPs) can help companies more effectively leverage technology to improve transparency and combat potential government misconduct. This could include efforts to establish and empower a consortium of companies to more effectively fight corruption through improved data analytics and AI solutions. For example, the development and maintenance of a database of non-confidential compliance information, based on pooled public and private sector data, would help multinational companies more effectively identify instances of foreign bribery in commercial operations by enabling rates, schedules, and fees required for industrial facilities to be published publicly.

On critical minerals, public-private partnerships can accelerate the adoption of new technologies that help map high-risk supply chains and promote ethical procurement of critical commodities, particularly as countries transition to greener economies. This might include applying distributed ledger technology to monitor and formalize the mineral chain of custody and supporting open and crowdsourcing data access initiatives that are mutually beneficial for local actors and large companies. PPPs can also support capacity building programs to guide small-scale miners towards improved extractive and business management programs, facilitating their participation in formalized mineral supply chains and, in turn, making it more feasible for them to meet OECD responsible sourcing guidelines.

Tech for a smart Continuous Monitoring Model - Autostrade per l'Italia

What specific issue related to anti-corruption is your company/organization aiming to address with digital technology and what technology are you deploying in this regard (the solution)?

The use case provides an overview of Autostrade per l'Italia's Continuous Monitoring Model including 1) Predictive Compliance solutions, 2) Continuous Risk Management program and 3) Fraud Free Zone Model.

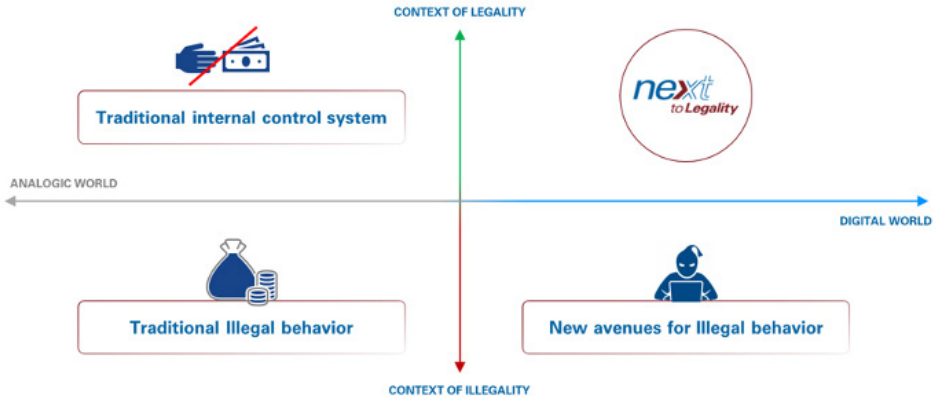
Premise: Autostrade per l'Italia's Strategic Plan triggering our compliance capacity upgrade. We could describe Autostrade per l'Italia's new 4-year Strategic Plan with two numbers:

€21.5 billion, a highway infrastructure investment and maintenance program that generates an induced effect on the economy of €65 Billion overall, and;

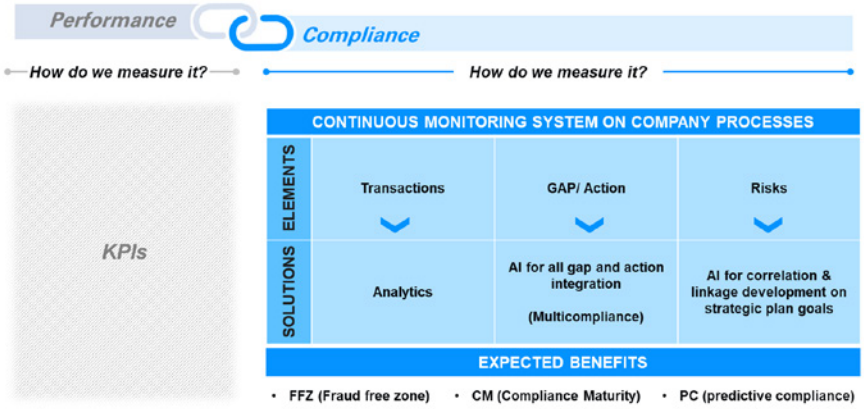
+2900, the professionals we are committed to hire in order to become an integrated operator in the field of sustainable mobility.

Through an anti-corruption lens, these two numbers imply the urgent need to strengthen our internal control system. In order to provide an effective and timely response, a specific program called 'Next to Legality' has been defined within the Strategic Plan. One of the key elements of the program is the structuring of efficient and monitored processes also through the adoption of innovative technology. The foundations of this program are the effective implementation of guidelines, tools, frameworks and the gold standards of monitoring of the OECD, Business at OECD (BIAC), B20 and G20.

The digital solutions we implemented are focused on defining a continuous monitoring system that closely links to the company's strategic objectives. Through the daily analysis of 100% of available data and the execution of "smart" controls, the solutions generate real time results capable of discriminating between threat and opportunity and, most importantly, effectively support management in the decision-making process.



By implementing transparent processes and systems, integrating performance & compliance and by using AI and Analytics, Autostrade per l'Italia has developed a process-based continuous monitoring model on company transactions, gaps, actions and risks.



What steps did you take to implement the technology and what hurdles did you encounter in the process? What factor supported implementation?

Key success factors

As the deployment of technology is a challenge that requires resources, time and cultural change, using a building block approach is a key factor supporting implementation. In our experience, the ability to provide quick results, with gradually increasing depth over time, helped to progressively streamline the solution throughout the entire organization while maintaining sustainable investment levels. In particular, this allowed us to extend the solutions to our subsidiaries, which are Small and Medium Enterprises. Furthermore, other key success factors to ensure solution effectiveness are:

Internal Control System (ICS):

A strong and mature ICS with clearly assigned responsibilities, applicable procedures, applicable and accountable processes and procedures, a healthy culture and an effective three-line monitoring system.;

Organization:

Clear accountability within the organization, given by:

- The positioning of the compliance structure at the c-level
- The definition of information flows between 1, 2 and 3rd level control owners

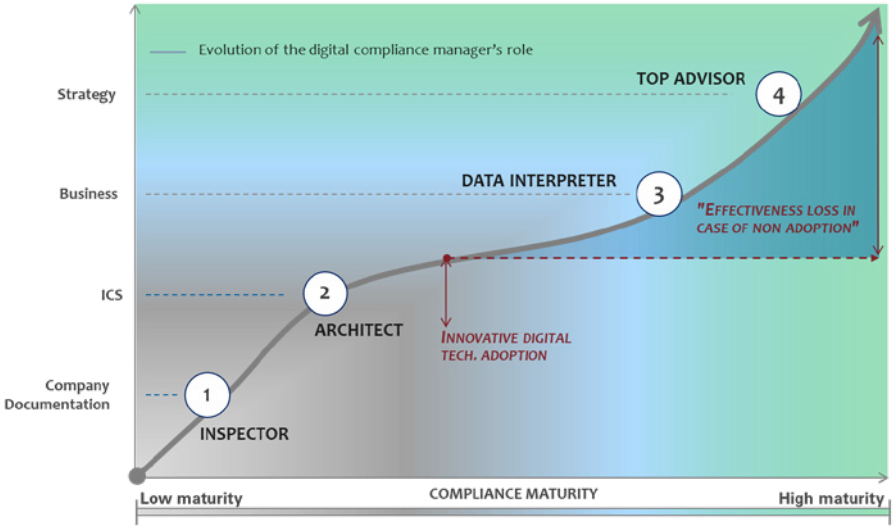
Data:

Data availability (current and historical) and consistency, enabling the definition of:

- KPIs - Linked to Strategic Plan objectives;
- KRIs - Risk Indicators correlated with each other based on potential triggers;
- KFIs - Fraud Indicators.

The human factor

Continuous monitoring does not mean to work as a substitute for the human factor, in fact upskilling is fundamental. Below is a representation of the evolution of the typical digital compliance manager, from Inspector to Top Advisor. The graph shows that the introduction of Artificial Intelligence enables a necessary skill upgrade, while a stationary situation highlights that the company will not need more than ICS architects, but the benefits of the "Top Advisor" scenario will not be accessible.



Operational Steps to implement the solutions:

In order to deploy the solution, the following steps were taken:

1.
Assessment of relevant company processes, and preliminary identification and evaluation of risks and fraud scenarios;

2.
Prioritization of mitigation intervention areas in terms of cost/benefit ratio, regulatory requirements, etc.;

3.
Definition of the functional requirements of the platform (direct integration with business systems, daily audits, perimeter of all process transactions, etc.) and construction of the data architecture (Data Model);

4.
Design of indicators ("smart controls") related to processes and identified risks and fraud scenarios. Such smart controls are verification algorithms, of varying levels of complexity, that are able to cross-reference and compare data coming from different business systems and external sources;

5.

Development of the platform using the following technologies:
- RPA = for sending automatic data flow to dashboard and VIES verification.
- Process Mining = process activity definition and monitoring.
- Data Analytics = for massive analysis on the enterprise dataset/external data sources at hand.
- Machine Learning for = predictive analytics on transaction development with alarm bells.

6.

Implementation of the Smart Controls within the platform;

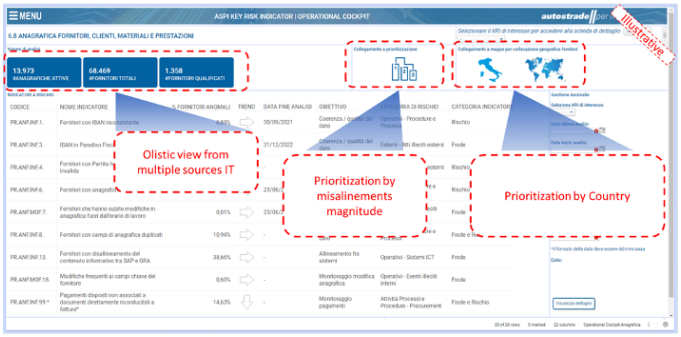
7.

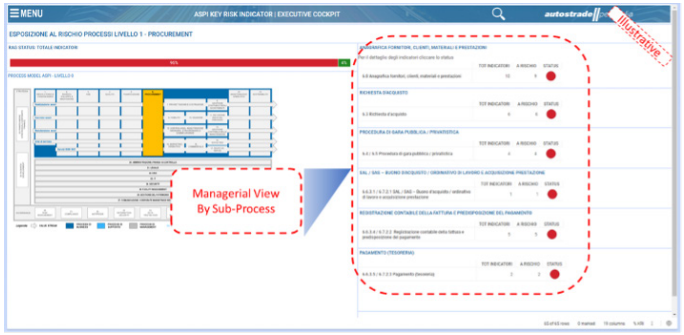
Definition of a correlation model. Afterwards, through a self-learning mechanism, the platform was able to provide suggestions to fine-tune risk correlations and evaluations based on existing data and scenario simulations;

8.

Continuous Maintenance of the platform.

Following are some illustrations of the implemented dashboard:



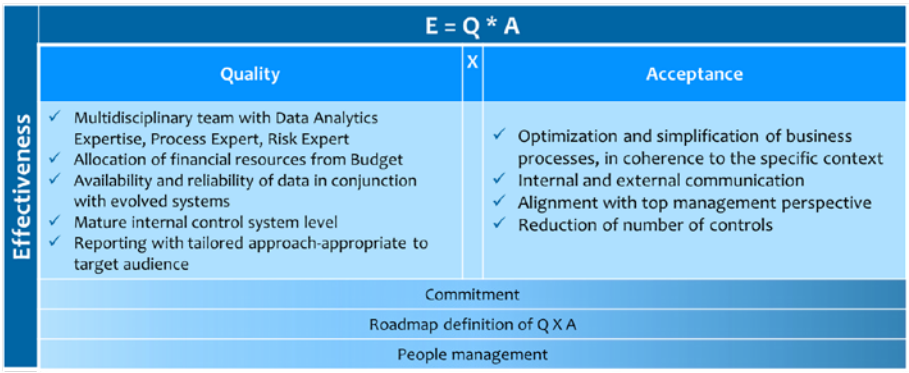


Main hurdles of the project

Among the main obstacles encountered during the implementation journey:
Data availability and data quality:
- Data related to some processes were not contained in digital documents.
- Data related to some processes were contained in different company IT systems.
- Initial results coming from the tool needed to be skimmed thoroughly by the Compliance team members. Anyhow, this represents a limitation that persisted only during early stages of deployment, thanks to the underlying machine learning technology.
- Cultural barriers: some of the stakeholders (e.g., traditional control owners) were resistant to change.

What do you think is necessary for management and staff buy-in at the corporate level? & How are you managing acceptance across stakeholders to ensure successful adoption of and trust in the technology?

The successful adoption of Digital Compliance solutions depends on a number of ingredients that can be represented in following equation:



- Diffusion of a culture marked by telling the solutions not just as a list of «compliance checks» but as a strategic tool
- New way of working based on transparency and integrity
- Onboarding top management and other key stakeholders from the first POC demonstrations to ensure engagement of all Process Owners involved in the preparatory functional analyses for the correct definition of solution requirements
- Use KPIs to measure and communicate results to strengthen key stakeholder engagement
- Homogenization and simplification of language, enabled by an integrated Risk & Compliance approach
- Coaching of process owners who will use the dashboard

From your point of view, how can governments support the uptake of digital solutions in companies? Should government and private sector collaborate, and if yes, in what manner?

From our point of view, fruitful collaboration between public bodies and private companies could be substantiated through the provision of useful public databases to supplement the information assets of the Companies, increasing capacity for analysis.

For example, our digital solution accesses the EU VIES Database to perform a consistency check of EU VAT numbers to prevent fraudulent entries of fictitious suppliers, avoiding errors in invoicing processes, and ensuring tax compliance. This check is only possible for Community VAT numbers, while it cannot be performed on purely National ones. Access to the Revenue Agency's counterpart database would allow a more in-depth analysis of our Company's national supplier base.

Furthermore, Public-private partnerships could be instrumental in order to generate a favorable ecosystem for companies implementing and adopting innovative digital solutions for compliance. In particular, Governments could:

1.
Incentivize companies by reducing the tax burden for all forms of investment dedicated to R&D and digital solutions.

2.
Consider digital solutions in compliance context as a plus in public tenders.

3.
Stimulate the business ecosystem through communication, training and knowledge sharing.

4.
Allocation of dedicated funds for developing digital solutions.

5.
Define rewarding mechanisms for companies, and in particular SMEs that have/are investing in digital solutions for compliance.

Chatbots to foster internal compliance awareness – BRF

What specific issue related to anti-corruption is your company/organization aiming to address with digital technology and what technology are you deploying in this regard (the solution)?

BRF is the #1 global poultry exporter with more than 100 thousand employees. A critical challenge within is to answer all employees' questions and requirements related to Integrity and Compliance Policies and Procedures. BRF developed a Chatbot as an agile platform to answer all these employees´ demands.

Approximately, 65% of BRF employees have already had contact with the Chatbot. On average, 42 thousand messages are sent to the Chatbot per day and the most usual searches are to check the pay stub, timecard and planning of vacations.

What steps did you take to implement the technology and what hurdles did you encounter in the process? What factor supported implementation?

The alignment with Human Resources (HR) Chatbot platform was a successful factor for the implementation, considering that all employees were already used to the Chatbot platform. The Compliance team "trained" the Chatbot to answer all different forms of information requirements. A continuous improvement process was implemented to improve the accuracy of the standard answers.

Today, there are 22 items regarding the themes of the Compliance, including the Acceptance term to the Transparency Manual, that all employees of BRF must agree to, access to the Transparency Channel and access to the self-declaration forms.

What do you think is necessary for management and staff buy-in at the corporate level?

Availability 24x7 of the system, useability, assertive and quick responses, and a flexible platform based on WhatsApp that can interact with employees through text and voice using AI. The Chatbot is prepared to answer more than a thousand different questions in Portuguese and English, in addition to being available in six countries (Brazil, Oman, Qatar, Saudi Arabia, United Arab Emirates and Kuwait) at the palm of employees' hands.

From your point of view, how can governments support the uptake of digital solutions in companies? Should government and private sector collaborate, and if yes, in what manner?

Governments should foster and recognize private initiatives related to investments in technologies to fight against corruption.

The development of transparent portals from the government also allows the private sector to monitor and consult public databases.

The collaboration of governments with the private sector is key for the successful development of technological solutions to fight against corruption. Solutions related to education, public procurement, governmental expenditures, and lobbying are possible filed of collaboration.

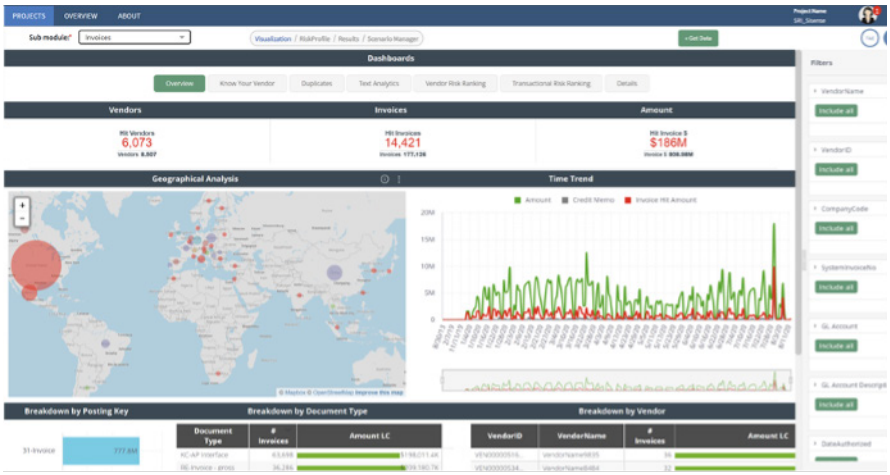
How are you managing acceptance across stakeholders to ensure successful adoption of and trust in the technology?

The change management process is very important in the adoption of new technologies, the acceptance of different stakeholders depends also on the support of top managers, the available resources for the projects, an effective communication of the benefits from the new systems and continuous support to implement the improvements in the processes.

Algorithms to detect supply side corruption - Integrity Distributed

What specific issue related to anti-corruption is your company/organization aiming to address with digital technology and what technology are you deploying in this regard (the solution)?

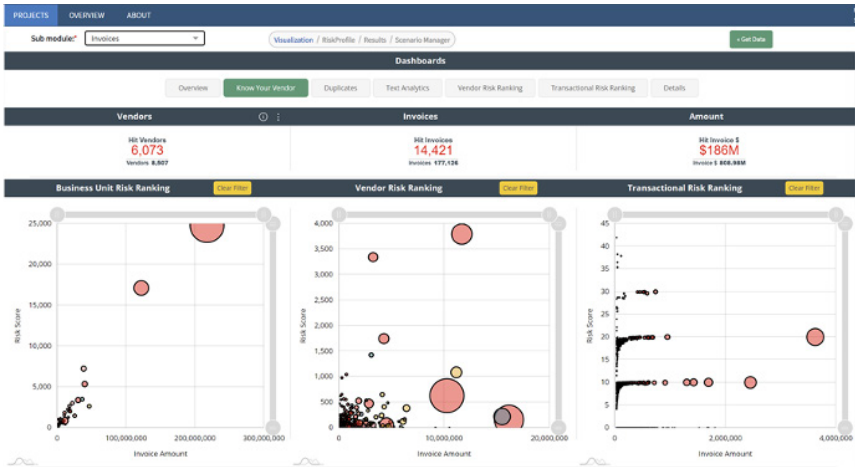
In partnership with the Massachusetts Institute of Technology, we launched a non-profit organization – Integrity Distributed – focused on improving algorithms to detect supply side corruption in accounts payable and third-party management systems used by multi-nationals. These algorithms use machine learning and artificial intelligence solutions to draw inferences from past investigations into third-party conduct to improve over time. The algorithms operate off a distributed ledger network that allows for the improvement of algorithms drawing experiences from member organizations without sharing any underlying commercial or proprietary data.



What steps did you take to implement the technology and what hurdles did you encounter in the process? What factor supported implementation?

Algorithms will only work across companies with data harmonization across the underlying data set. We have invested in technology that allows for the efficient and low-cost extraction and harmonization of data in partnership with Kona AI. This allows us to pull and organize the relevant company data from each system to operate the system in under ten days.

Once deployed, we use algorithms that have been developed over the past six years (taking into account tens of thousands of transactions) designed to identify indicators of fraud, corruption, and evasion of control across organizations. These algorithms have been measured to have an F1 score of over 40, as well as improved false negative and false positive rates, in trials within a single company. The application of measurements to assess algorithm performance is a critical step in measuring platform success. Each organization shall deploy a workflow that creates a training set which will be used to train models specific to each member organization.



To facilitate the collaboration among companies, we are using distributed ledger technology that will allow member organizations to improve algorithms independently, and then upload these algorithms onto an exchange that allows a central hub to compare and improve algorithms using the algorithms contributed by each member organization. The result will be that member organizations simultaneously build algorithms that improve performance which are specific to the feedback of the member organization while contributing to, and receiving, super-algorithms that are built from the algorithms from each member of the collective.

What do you think is necessary for management and staff buy-in at the corporate level?

In large part because Integrity Distributed is a non-profit organization, the project has been designed to be relatively inexpensive by multinational standards. At this stage of development, companies can license the requisite platform from Kona AI (or another provider) for less than $150K and participate in the collective with a $30K subscription.

The key challenge is obtaining the commitment of management. The deployment of any technological solutions requires management of stakeholders across compliance, legal, IT and control organizations. So, while the platform is not expensive, we have experienced delays in deployment from managing these stakeholders. What is more, because the platform will augment an organization's ability to identify wrongdoing, participating organizations are committing resources to investigating and remediating issues identified by the platform.

From your point of view, how can governments support the uptake of digital solutions in companies? Should government and private sector collaborate, and if yes, in what manner?

Governments can endeavor to set objective standards (e.g., algorithm performance) and communicate them as acceptable standards for evaluating compliance programs. Governments should educate corporate compliance departments on technologies, incentivize the use of such technologies, and where possible, provide grants and other financial assistance to subsidize such technologies. As technology to detect and deter corruption becomes more accepted, it should also become more accessible, better understand and less expensive. Governments can accelerate this progress by incentivizing organizations to meet such standards with reduced sentencing in event of corporate malfeasance.

How are you managing acceptance across stakeholders to ensure successful adoption of and trust in the technology?

The use of algorithms as a core component of compliance risk management has the advantage of being measurable. No compliance program is perfect, but this approach allows organizations to manage the effectiveness of their compliance activity. We deploy a variety of metrics that are generally accepted ways of evaluating algorithm performance. For example, every algorithm should not only produce a risk and confidence level for the algorithm, but also an F1 score (measurement of accuracy and precision), False Positive Rate, False Negative Rate, User Acceptance Metrics (including Net Promoter) and Data Quality Ratings. These scores ensure transparency into model effectiveness, help incorporate real time user feedback to ensure a quality adoption rate, and help facilitate adoption across stakeholders.

Additionally, algorithm-based compliance programs help senior compliance personnel evaluate and communicate compliance risk to boards and other senior level non-compliance stakeholders in a visually meaningful and digestible way. This facilitates broader acceptance and unity of purpose.

Tech for the management of third-party risk and stakeholder engagement - Merck

What specific issue related to anti-corruption is your company/organization aiming to address with digital technology and what technology are you deploying in this regard (the solution)?

As a science and technology company operating across healthcare, life sciences and electronics, we continually leverage technology to manage corruption risks. In this regard, we have outlined below our approach to managing corruption risks across two of our high-risk areas; third parties and healthcare stakeholders (healthcare professionals - HCP and healthcare organizations - HCO).

Third parties:

Combining technology, compliance, and risk management elements, we developed a tool that helps us unify our third-party risk management processes across the globe. We have set out below our approach in this area:

From a risk management perspective, we initially defined criteria based on which third parties could be risk-rated and classified into different risk categories (low, medium, or high). We also defined different procedures and workflows for each of the risk categories.

From a technology perspective, these criteria and workflows are defined in our tool which are utilized in the following manner:

1.

The tool applies the criteria on the on-boarding information shared by the third parties and accordingly assesses the third parties' risk categories.

2.

Using the pre-defined workflows, the tool ensures that the third parties are subject to the correct workflows. For example, a high-risk third party could be approved subject to additional checks, approvals, and documentation.

Further, we are in the process of bringing the third parties on a new cloud-based platform (Aravo) with a low-code admin cockpit which allows us to update or create new risk-criteria and workflows and stay abreast with the changing regulations, risk environment and policies.

Healthcare stakeholders:

As a business we are often required to interact with HCPs and HCOs while being mindful of complying with the anti-corruption laws and abiding by our Code and values.

In this respect, we are upgrading our HCP/HCO engagement tool (a tool that documents all kinds of interactions between Merck and HCPs / HCOs) as well as our reporting tool, to have a more efficient and transparent end to end view of such interactions. This will also help us in our transparency reporting, monitoring and other compliance requirements. Similar to our third-party risk management tool, the interactions tool also has the flexibility of a low-code platform and advanced analytics capabilities which allows us to adapt quickly to the changing regulations, risk environment and policies.

Overall stakeholder management

In addition to third parties and HCPs / HCOs, we are also experimenting with machine learning, chatbots and Microsoft 365 enterprise tools to enhance stakeholder management.

The objective is that the business stakeholders can approach chatbots with routine compliance questions and can engage compliance colleagues for more complex compliance and ethical dilemma situations. This will allow the compliance colleagues to focus on more important matters and play the role of a strategic advisor and enabler to business stakeholders.

What steps did you take to implement the technology and what hurdles did you encounter in the process?

What factor supported implementation? Before any technology was implemented, we first identified the problem that needed to be solved and understood the potential role of technology in solving this problem. This included identifying pain points from previous processes, risks and challenges and accordingly defining processes and procedures that could help remediate these problems.

Some of the key hurdles were as follows:

1.

Understanding the requirements of the business stakeholders while ensuring compliance requirements are met. This often meant bringing business and compliance perspectives together without having to compromise both the stakeholders' requirements and objectives.

2.

Updating or developing processes and procedures, particularly in a dynamic environment with changing risk landscape.

The key factors that supported the implementation were that we were solution-oriented and ensured that the proposed solution brings inefficiencies and helps all stakeholders achieve their respective objectives. Communication as well as designing the processes considering the end user perspective was key, so that compliance processes/workflows do not seem like a separate, siloed task but as something that is embedded in the business and eventually helps us achieve our business objectives while being consistent with our values.

What do you think is necessary for management and staff buy-in at the corporate level?

Right stakeholder involvement and change management at each stage of the project is very essential. The adoption rate is higher if business is brought into the project at the initial stages to get the user centric view early in the design phase and there is a well thought through communication and change management plan from the beginning of the project itself. As mentioned earlier, if we can showcase that the solution will help the business rather than complicate, it becomes easier to obtain buy-in from the business stakeholders.

From your point of view, how can governments support the uptake of digital solutions in companies? Should government and private sector collaborate, and if yes, in what manner?

Governments could use integration tools like Application Programming Interfaces (APIs) to ensure seamless integrations between companies and government portals. Additionally, as part of a wider inter-government collaboration, governments could consider streamlining diverse reporting requirements across different countries and easing the reporting process.

How are you managing acceptance across stakeholders to ensure successful adoption of and trust in the technology?

Regular check-ins with the end users via drop-in calls or knowledge sharing sessions. Additionally continuous improvements within the tool/platform, addressing the users' problems and bottlenecks without delays, and providing new features from time to time are some of the key factors.

For example, reports and dashboards are essential for businesses so that they can fulfill their compliance requirements efficiently. Once they experience the benefits, they not only trust the technology but also willingly collaborate and support such technology initiatives in the future.

Leveraging digital technology for the timely detection of falsified medicines in the field – Novartis

What specific issue related to anti-corruption is your company/organization aiming to address with digital technology and what technology are you deploying in this regard (the solution)?

'Falsified' medicines are those that deliberately and fraudulently misrepresent their identity, composition or source[18]. The Pharmaceutical Security Institute reported a 38% increase in incidents of falsified medicines, also called "pharmaceutical crime", between 2016 to 2020 with an all-time high number of recorded incidents in 2021[19].

Falsified medical products may contain harmful chemicals, no active ingredient, undeclared active ingredients and excipients or the wrong dosage of the correct active ingredient. They impact all geographies and all therapeutic areas.

For patients that are usually unable to distinguish between authentic and falsified medical products, the health risks are enormous, as a falsified medicine may not only cause an obvious adverse reaction. It will often fail to properly treat the disease or condition for which it was intended and can lead to therapeutic failure or death.

In addition to threatening patients' safety, falsified medical products represent a serious and growing problem for public health (e.g., anti-microbial resistance), healthcare systems (e.g.,

[18] WHO, Substandard and falsified medical products, 31 January 2018. available at: Substandard and falsified medical products (who.int) (Oct. 2022).
[19] psi-inc.org

access and social security fraud), governments (e.g., tax) and pharmaceutical manufacturers (e.g., reputation and intellectual property).

Novartis is committed to protecting patients' safety and our reputation as well as expanding access to quality medicines worldwide. Digitalizing, localizing, and ultimately accelerating the detection and reporting of falsified medicines locally is one of the company's key strategic priorities.

In 2019, to significantly accelerate the authentication of falsified medicines Novartis initiated a paradigm shift and decided to leverage the latest digital technologies to move from regional authentication capabilities (i.e., 5 locations) to local ones (i.e., 96 countries in scope).

First piloted in 2019, Authentifield by Novartis is a pocket sized, mobile and application enabled spectrometric drug sensor which detects falsified medicines by performing noninvasive testing of a suspect sample which is compared to the library of genuine Novartis products. These are near infrared spectrometric sensors, not medical devices. The vision of this multi-year project is to roll-out 500 sensors to empower 96 countries with fast and mobile detection technology enabling the timely reporting of falsified medicines to health authorities, law enforcement and the World Health Organization. These sensors are primarily destined to be used by Novartis associates. Subject to the successful roll out of the solution, empowerment of external stakeholders will also be considered.

What steps did you take to implement the technology and what hurdles did you encounter in the process? What factor supported implementation?

Since 2018, several key steps have been taken to implement the solution

Benchmark: Novartis conducted several benchmark studies to evaluate the available technologies on the market.

Integrated solution evaluation: Novartis conducted an independent evaluation of the sensor & IT components.

Feasibility study: Novartis conducted an in-depth analysis of the selected solution.

Compliance: Ensured 100% compliance with the highest company quality and security standards.

Proof of concept and accuracy: In 2019, Novartis piloted 55 sensors in 15 countries to test the solution in the field — resulting in an accuracy rate of 97%.

Governance: Novartis established a robust governance (cross-functional steering committee) responsible for guiding and supporting the project working group.

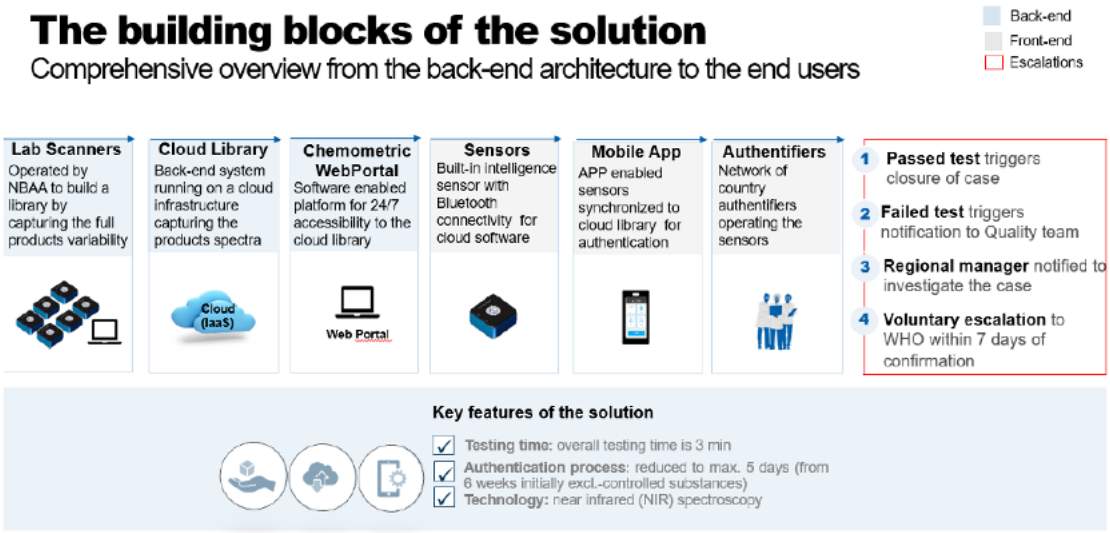
Global roll-out: Established a multi-year plan to roll-out the solution globally (i.e., 500 sensors/96 countries).

Hurdles

Navigating the complexities of developing a secure back-end and front-end architecture: see a diagram of the building blocks of the solution.

Resistance to changes: Business environment and stakeholder alignment/ changes.

Regulatory challenge and compliance (i.e., radio electronic certifications, health and safety and IT security requirements)



What do you think is necessary for management and staff buy-in at the corporate level?

There are three key components to obtain management and staff buy-in at the corporate level:

1.

Clearly communicate the project purpose and vision: for Authentifield by Novartis, the purpose and vision of the project which is rooted in the patient safety impact. Accelerating the detection of falsified medicines enables both faster reporting and faster removal of suspected products from the market — significantly improving patient safety outcomes.

2.

Establish a robust governance and engage with key company stakeholders: Authentifield by Novartis is supported by both a cross-functional steering committee and working group. The project has also been supported by the key company stakeholders.

3.

Maintain engagement with associates: Building, training, and maintaining engagement with a community of end-users (i.e., Authentifiers) is an important component of the successful adoption of the solution.

How are you managing acceptance across stakeholders to ensure successful adoption of and trust in the technology?

The following enabled the acceptance, successful adoption, and trust of the solution:

Implementation activities (i.e., as outlined in Q2) such as the benchmark, feasibility study, proof of concept and accuracy study.

Continuous training of end users to ensure a good user experience (i.e., a user having 100% confidence in operating the tool).

Successful integration and compliance with the Novartis quality and security standards

From your point of view, how can governments support the uptake of digital solutions in companies? Should government and private sector collaborate, and if yes, in what manner?

Governments can enable the uptake of digital solutions by promoting strategic partnerships with companies and other public sector actors. One good example of such partnerships in the field of detection is the PharmaLedger blockchain use case which brings together experts from both the pharmaceutical and technology sectors as well as patients and hospitals — making it a unique cross-sector, multi-disciplinary public-private partnership. Promoting such public-private partnerships would allow for more collaboration and harmonization of initiatives in the detection space.

Governments are also in the position to promote a stronger and more harmonized legislative and regulatory environment.

Enhancing due diligence through centralized resources– Rolls Royce

What specific issue related to anti-corruption is your company/organization aiming to address with digital technology and what technology are you deploying in this regard (the solution)?

With making the Rolls-Royce Code of Conduct and Group Policies (including our Know Your Partner Procedures) accessible through our website and a digital app these resources are made globally available in the public domain and thereby supports Rolls-Royce in achieving transparency on what Rolls-Royce stands for on Ethics & Compliance matters. When we focus in more detail on the implementation of digital technology in our Third-Party Due Diligence Procedures (Know Your Partner Procedures) Rolls-Royce aims to achieve simplification, standardization, accessibility, and enhanced oversight within the whole corporation.

Solution: Know Your Partner Portal

1.

Simplification and standardization – by using a centralized web-based solution Rolls-Royce was able to simplify and digitalize all due diligence steps of the Know Your Partner. It meant relevant policy and guidance documents, Partner related data, bribery and corruption risk rating, due diligence steps (including screening), approvals, mitigation steps and monitoring are encapsulated in the Know Your Partner Portal. This also enabled Rolls-Royce to standardize the due diligence steps across all business units within the Group.

2.

Accessibility–implementing a web-based solution allowed Rolls-Royce to make the Know Your Partner Portal easily available and accessible to all relevant internal and external stakeholders. For example, third parties can complete questionnaires and submit documentation required through the due diligence process and Rolls-Royce can assign mitigation tasks (for example training material or compliance certifications) to the third party via the Know Your Partner Portal.

3.

Oversight – the digital Know Your Partner Portal furthermore allowed Rolls-Royce greater visibility and oversight of its third-party population across the Group as well as its ABC risk profile. It enables the monitoring of the due diligence programme i.e., status of a Partner, its mitigation tasks and renewal dates. Helping the company to better manage our Bribery and Corruption risk related to Partners that are acting on behalf of Rolls-Royce.

What steps did you take to implement the technology and what hurdles did you encounter in the process? What factor supported implementation?

Early stakeholder engagement is key to the successful implementation of a new digital solution. Rolls-Royce IT was brought in as part of the procurement and selection process to ensure the selected digital solution will meet our strict security standards. Other stakeholders included Data Privacy, Export Control and member of our business Ethics and Compliance teams. All training, user guide and process materials were available digitally from the start, which meant that we were already well positioned when the COVID pandemic hit, and we had to implement the new process remotely. Establishing a governance forum with the business Ethics and Compliance teams to review KPIs, monitor progress and provide a forum to raise any difficulties was another key success factor to help drive the implementation.

What do you think is necessary for management and staff buy-in at the corporate level?

Clearly articulating and demonstrating the benefits to management and other internal stakeholders is key. In the case of Rolls-Royce, it was simplification (one policy and procedure to manage our third-party programme), digitalization of the due diligence process and empowerment of the businesses i.e., linking approval levels to the ABC risk and focusing our time, effort and money on those relationships that pose the highest ABC risks. One of the biggest benefits has been the power of data, providing management with greater visibility and insight into the third-party population in their business and across the Group.

From your point of view, how can governments support the uptake of digital solutions in companies? Should government and private sector collaborate, and if yes, in what manner?

Governments can push for more transparency around the increasingly important topic of Ultimate Beneficial Ownership (UBO) by providing better access to UBO registers. On top of that collaboration between the private sector and government using digital solutions can be beneficial in the prevention of bribery and corruption. Easy electronic access UBO registers and linking these registers into digital due diligence solutions can allow the private sector to do due diligence based on the information in these UBO registers. More collaboration between governments and between private sector parties that operate within the same supply chain can also improve using digital solutions. It is in the end all about a collective responsibility for both governments and private parties.

How are you managing acceptance across stakeholders to ensure successful adoption of and trust in the technology?

A key success factor is to embed the KYP due diligence process within existing business processes and linking the digital compliance solutions to existing systems where possible, avoiding the risk of circumventing the compliance requirements. However, linking systems can be challenging and complex where a group doesn't operate on the same systems, but you can still be effective by referencing the KYP due diligence requirements into existing processes and standard operating procedures, for example in procurement and commercial process documents. Another element is to try to keep the process lean and make it easy for stakeholders to complete the requirements.

An example here is for procurement and commercial teams to have easy access to Anti-Bribery and Corruption clause templates that can be used in procurement and commercial contracts. This contributes to adopting the digital process and keeping the trust in the used technology by the organization.

Real-Time, Proactive Ethics and Compliance with Artificial Intelligence – Sanofi

As a world leading life sciences company, Sanofi is pioneering real-time and proactive ethics and compliance with a cutting-edge artificial intelligence program. In addition to evolving traditional and often reactive approaches to compliance, the impact of this program goes far beyond to include reductions in bureaucracy, process improvements, and smart cost reallocation. In sum, a novel digital technology that supports the fight against corruption, patient care, and enterprise growth.
The dedicated App leverages real-time data to serve as one single source that enables instant correlation across Sanofi's activities. The AI program's outlier detection capabilities transform the organization's corruption prevention approach across diverse areas such as in healthcare professional engagement, off-label promotion, expense monitoring and fraud detection and training adherence by employees. Live insights are generated to continuously strengthen Sanofi's ability to identify risks and act quickly. Relevant content on a variety of issues is also pushed live to specific individuals across the organization to further drive a culture of ethics and business integrity.

For example, in the area of travel and expense monitoring, the App aims to eliminate the initial human review process of each submission, allowing Sanofi employees to focus only on AI-rejected reports. Not only is this estimated to increase accuracy, but simultaneously results in a 90 percent time savings. This AI-enabled automation allows Sanofi ethics and compliance staff to dedicate more time where it is needed most.

Primary challenges to overcome included the quality of the data and connecting in-house IT tools. With the assistance of data experts, Sanofi then elaborated AI models in order to design Proof of Concepts and Minimal Valuable Products on a targeted set of data.
Tone from the top is crucial to upholding high standards of ethics and business integrity, including in the adoption and implementation of the App. As a company with an integrity-first culture that not only views ethical decision-making as vital to upholding patient trust, the App receives full support from Sanofi's Ethics and Compliance Committee, which includes our entire c-suite team. This leadership buy-in is crucial in fostering program support and trust across Sanofi's managers and their respective teams around the world. The continued demonstration of the App results over time will also drive trust in the technology.

Governments and multi-lateral bodies are well positioned to support the uptake of AI-driven ethics and compliance regimes, particularly in health-related sectors, by recognizing the benefits they can provide not only to the prevention of corruption and unethical conduct, but in the reduction of waste and inefficiencies that benefits patients and their care. Such recognition could take the form of incentives across diverse public processes, including procurement and regulatory review, that recognizes enterprises investing in such corruption prevention technologies. Further collaboration between governments, healthcare providers, and life sciences firms to deploy similar technologies in their daily ethics and compliance practices could also drive positive results across the health ecosystem. More broadly, governments can also support the uptake of digital solutions by working with companies and civil society to implement legislative frameworks that are clear, risk-based, and encourage digital innovation.

Tech for Suppliers Compliance Monitoring - SNAM

What specific issue related to anti-corruption is your company/organization aiming to address with digital technology and what technology are you deploying in this regard (the solution)?

Since 2020 our company has developed a process called "Supplier's Compliance Monitoring" aimed at having a full picture of our suppliers not only in terms of reputational reliability or performance quality, but also in terms of health, safety, environment and quality (HSEQ) adequacy and financial consistency/stability.

By means of 4 streams of due diligence (one for each item above mentioned) the competent functions carry out their analyses to identify any potential red flags.

The process is supported by a software, which is very user friendly, and which is linked to the Vendor list, and also the SAP registry. Any function in charge (i.e., Legal and Security for the reputational, Supply chain for the performances, HSEQ for the relevant matters and Finance for the check on the economic status), conducts its analysis and in case it intercepts some red flags, it puts the supplier in stand-by, in order to proceed with further insights, also directly engaging the suppliers of interest.

The software has an easy functioning, based on a "traffic light system". Any time a red flag is intercepted, no matter from what stream, the system blocks the access of such suppliers to our vendor list and requires further insights.

It could be not so intuitive, but a red flag in terms of HESQ or financial status of the suppliers, could be an alert of many potential risks, such as criminal infiltration or accidents at work.

The added value of our digital solution is that all the involved functions have full visibility of all the vendors' status and can act directly on the system, reporting any signal of alarm.

In addition, the system is designed to re-perform the analyses on all suppliers within a certain time period, so as to have a rolling monitoring of the entire supply chain and not just on some suppliers, in the case of awarding contracts or qualification.

What steps did you take to implement the technology and what hurdles did you encounter in the process? What factor supported implementation?

We have opened a Working Group, coordinated by the Organization function, in which all the functions involved – including the digital & Technology one - have been involved to give their own contribution to the realization of the project. We did set the priorities and the drivers which moved the implementation of the system and, with the help of a consultant, we identified critical paths and potential inefficiencies of some parts of the process, especially within suppliers' onboarding and qualification, in order to prevent gaps in the tuning phase and avoid slowdowns during the implementation.

The implementation was supported by the competence of the people involved and the full knowledge of their own processes and issues. In addition, the software we decided to adopt was perfectly designed to be integrated with the other applications available in the company, and it proved to be highly user-friendly.

We encountered some difficulties, but they were mainly linked to the designing of users' requirements, since anyone on the table was raising different and multiple needs.

What do you think is necessary for management and staff buy-in at the corporate level?

It is very important to show WHY, before HOW.

The added value of this system is undisputed, but during the designing and implementation of the same, a lot of commitments, efforts, time, and patience have been required.

The simplicity of use of the software, the immediacy and completeness of the information, as well as the possibility of having a repository over time (and therefore a database with which to monitor the path of a supplier and have a long-time view) has allowed rapid appreciation by all users directly involved and an inevitable return to the company, in terms of strengthening controls.

From your point of view, how can governments support the uptake of digital solutions in companies? Should government and private sector collaborate, and if yes, in what manner?

They surely should, for example by opening tables of discussion.

Governments could be very helpful in providing regulations that would impose (and therefore) accelerate the adoption of technology systems within companies aimed at strengthening controls and preventing offences. And besides, they could give to the most compliant companies incentives or rewards, for instance by taking them as an example in public documentations and events.

Companies (covering different sizes and perspectives of the business sector) should give governments feedback on their own needs and on the feasible solutions, in order to prevent that some regulations might not consider the costs or the operational difficulties of some implementations or requirements.

How are you managing acceptance across stakeholders to ensure successful adoption of and trust in the technology?

Our process has been fully disclosed to our suppliers and to our stakeholders in general. The added value of our Suppliers' Monitoring system is undisputed and is in line with the future provisions included in the draft of the European Directive on Corporate Sustainability Due Diligences.

Tech for third-party screening and advanced gifts and hospitality reporting tools - Telefonica

What specific issue related to anti-corruption is your company/organization aiming to address with digital technology and what technology are you deploying in this regard (the solution)?

The Telefonica Group is certainly committed to enhancing a compliance culture throughout the organization. To that effect, it counts on material resources, independent headcount, and a wide range of tools which contribute to efficiency in the development of compliance functions; and, among the latter, the most relevant ones are directly addressed at approaching tangible needs in the anti-corruption program. Digitalization, as it cannot be otherwise, is the main catalyst of such tools.
Aside from sophisticated systems that come to rationalize the compliance activity (automatization of processes, e-learning, conflicts of interest tool, etc.), Telefonica considers it convenient to highlight a couple of use cases which, in themselves and furthermore if generalized, could play a definitive role in the global fight against corruption:

(a) third parties screening and (b) an advanced gifts and hospitality (G&H) reporting tool.

First, Telefonica's live due diligence system (obviously complemented with enhanced reviews for specific risk scenarios), whilst simple prima facie, is the outcome of huge efforts to find out the best possible solution (including the fine-tuning of algorithms) to recurrently (in some cases, daily) match all the ongoing Group activity and all the relevant hits of any nature and wherever: not only sanctions or Politically Exposed Persons (PEPs), but a wide range of contingencies, remarking, among them, those related to bribery and corruption.

On the other hand, Telefonica's exposure in all its footprint made it necessary to develop an in-house highly developed system which lands into a genuine and easily accessible and usable tool all and each of the material and formal elements of its ABC internal regulations (registration, internal accountability, limits, prohibitions and approvals, and all genre of requirements).

What steps did you take to implement the technology and what hurdles did you encounter in the process? What factor supported implementation?

As a telecommunication provider, technology is placed at the very core of Telefonica's processes; and, beyond the complexity of the work itself, nothing hurdled the company's ambition. On the contrary, many factors supported implementation, but the most definitive one was the decisive will of Telefonica to extend its evolving compliance practices and anti-corruption efforts to its whole private and public environment.

What do you think is necessary for management and staff buy-in at the corporate level?

Investing in control functions and tools is always challenging, as it can legitimately trigger management's reasonable doubts on when to reach the point where an adequate control model does not need more one-off investments. Therefore, it becomes essential to balance the needs, making clear and visible the risks that are being prevented, and even assessing the impact and likelihood of such risks. In the field of ABC, beyond the eventual affectation to internal culture and external reputation (which takes time and money to be reverted), the vast regulatory exposure in terms of sanctions, business prohibitions or sensible (criminal) liabilities -even higher in the case of Telefonica as bound by FCPA regulations-, designs a playing field where it is difficult that management is not fully convinced.

From your point of view, how can governments support the uptake of digital solutions in companies? Should government and private sector collaborate, and if yes, in what manner?

Governments should definitely support these initiatives.

For instance, in the case of third parties review, public authorities could promote an enhanced ecosystem of due diligence provided that there is appropriate cautions and a legitimate interest supporting such legal justification considering that the deployment of these systems by big players of the bandwidth of Telefonica may play a straightforward role in the goal of fighting against corruption.

Needless to say, when it comes to Gifts& Hospitality, public sector awareness is key to completely prevent improper practices or bad doing. Private sector tools contribute to pushing such conscientization. Telefonica's experience shows that when public servants are informed of the application of, for instance, privacy rules, there is still a surprise reaction). A direct application by governments of those tools to their regular activity, albeit less sophisticated than those used by the private sector, would clearly support the common objective.

How are you managing acceptance across stakeholders to ensure successful adoption of and trust in the technology?

It is not difficult for Telefonica to ensure its stakeholders' acceptance and trust in the technology, as Telefonica is at the center of the technology supply chain. This could be a challenge for players of other sectors; in those cases, again, resistance should be combated with numbers, and efficiency (both in terms of tasks automatization and risk prevention) should be the main driver.

Tech for centralized, smart risk management processes – Unilever

Unilever wanted to improve its anti-corruption risk assessment by departing from the chaos of spreadsheets, complicated methodologies and simplistic insights. The solution? An innovative in-house IT tool developed with the users in mind and with a strong bias for action.

The first consideration was to use technology that was already integrated within the business. This led to designing a tailor-made Microsoft platform using their Forms, SharePoint and Power BI applications to form a centralised risk management centre. The backbone of the platform is an activity, risk and control matrix that helps ethics and compliance officers conduct consultations with employees in the frontline to form their understanding of the country risk and controls status for each activity. Officers then complete a questionnaire connected with a prioritisation algorithm that helps focus the subsequent assessment of the activities of highest concern. Users finally determine actions to enhance controls and all data is then visualised in an intuitive dashboard that is shared with business leaders and key functions like audit and finance.

The impact of this digital solution has been significant. The insights and results of the assessment have helped the ethics and compliance function to improve KPIs and prioritize global initiatives such as new written standards, risk clinics, bespoke trainings and enhanced monitoring plans. The greatest impact, however, has been the increased anti-corruption awareness and oversight by business leaders at all levels within the organization.

A key lesson from the adoption of this new assessment is the importance of design thinking in the conception and development of the methodology and system platforms. By bringing users to the forefront the company was able to create an engaging exercise that reinvigorated the relevance of risk assessments as decision-making tools. Also, the project demonstrated that digital tools are best when they are simple, familiar to employees and that integrate well with other existing tools and platforms.

Collaborating for the promotion of tech to improve licensing and permitting processes, the Digital Tools for Rule of Law and Recovery (DT4RR) project - WALMART

Aside from inherent inefficiencies in paper-based application procedures, offline payments for licensing and permitting (L&P) services and unlinked, siloed government databases have a tendency for leaks within the system, since fees are collected at various stages by different agencies. This obscures accountability, and increases the opportunity for corruption.

In order to tackle this issue and other challenges related to traditional paper-based processes, Walmart leads a multi-stakeholder initiative, Digital Tools for Rule of Law and Recovery (DT4RR), which promotes digitalization in key regulatory areas, including L&P. As part of these efforts, Walmart works with governmental partners and global economic institutions, both bilaterally

and through multilateral engagement within the Asia-Pacific Economic Cooperation (APEC) forum, the Summit of the Americas, and others, to promote digitalization, and identify and support enablers for digitalization of L&P processes. It advocates digital L&P as the nexus between inclusion, economic recovery, digital resilience, and transparency.

Walmart has a successful case use in Costa Rica, where Walmart and other companies, worked with the Federated College of Engineers and Architects (CFIA) to identify bottlenecks in institutions and processes related to the construction sector. CFIA then launched a digital platform, the Administrador de Proyectos de Construcción (APC), that comprehensively covered most permits required for construction projects. APC acts as a single point for L&P application, tracking, payments, and approval. Most municipalities and relevant national institutions have adopted the APC. While users are predominantly corporate industry stakeholders – the architects and engineers, efforts are underway to democratize and expand the use of APC. To support ease of use and inclusion, a mobile version of APC has been made available.

Factors for Success

With Costa Rica, strong support from industry – engineers and architects – who understand first-hand the benefits and ease of a digitalized L&P process, played a key role in bringing government stakeholders on board. The latter are key to successful implementation because they set the country's direction. Government can facilitate the uptake of digital solutions by: (i) making clear relevant information and rules online for consistency and transparency; (ii) streamlining the digital L&P process and integrating corporate/individuals' data; (iii)requiring online disclosure of required mitigation to ensure transparency, accountability and engender trust; and (iv) enacting policy and / or legal reforms support digitalization (e.g.,, accepting applications / requests through online means, making digital solutions cheaper, promoting inter-department or inter-agency collaboration, or adopting international or regional standards).

Corporates, in turn, should supplement such government efforts through: (i) sustained commitment and direction from senior management; (ii) consultations with stakeholders in the design and implementation of their digital solutions; (iii) education & training on the use, and intangible benefits (e.g., saving time & money); and (iv) incentives for users.

Working hand-in-hand, governments and the private sector can further increase the odds of success of digital solutions by collaborating in: the design of the digital solution, since ultimately the private sector are key stakeholders and users; education and training in the use of the technology and on its benefits; and incentives at the macro level to encourage companies to adopt digital solutions.

LITERATURE AND RESOURCES

A Nurkey , A Mukasheva and D Yedilkhan in IOP Conference Series: Materials Science and Engineering (2022). Models and methods of digital mechanisms in anti-corruption, their advantages and disadvantages, and applications. https://iopscience.iop.org/article/10.1088/1757-899X/1216/1/012015

Adam, I., & Fazekas, M. (2021). Are emerging technologies helping win the fight against corruption? A review of the state of evidence. Elsevier, 57, pp. 1-14 https://doi.org/10.1016/j.infoecopol.2021.100950

Adamopoulou, E., & Moussiades, L. (2020). An Overview of Chatbot Technology. IFIP International Conference on Artificial Intelligence Applications and Innovations, 584, pp. 373-383. https://doi.org/10.1787/ba682899-en

ACCA, (2020). Economic crime in a digital age

Alliance for Integrity, (2018). Compliance And Digitalisation - How Technology Can Foster Transparency In African Countries

APEC, (2022). Digital Permitting and E-Government Measures to Advance the Post-COVID-19 Economic Recovery

Business at OECD, & International Organisation of Employers (2020). Connecting the anti-corruption and human rights agendas: A guide for business and employers organisations

B20. (2020). Integrity & Compliance - Policy Paper

Basel Institute on Governance. (2017). New perspectives in e-government and the prevention of corruption. Working Paper No. 23.

Carlos Santiso for the World Economic Forum, (2019). Here's how technology is changing the corruption game.

Cercle Montesquieu, AFJE (2021). La digitalisation des processus de compliance. *Livre Blanc.*

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ). (2018). Embracing Digitalisation: How to use ICT to strengthen Anti-Corruption.

E-Estonia (2022). E-Idenfity. Retrieved from: ID-card - e-Estonia

European Commission (2019). Blockchain for digital government.

European Commission (2022). European Digital Identity. Retrieved from: European Digital Identity | European Commission (europa.eu)

G20 Anti- Corruption Working Group. (2021). Anti-Corruption Action Plan 2022-2024

Kramer, S. (2020). Technology As A Risk Tool: Using Blockchain in the Supply Chain to Manage Compliance Risks - Global Supply Chain Compliance (bakermckenzie.com)

OECD. (2016). Preventing Corruption in Public Procurement. *Brochure.*

OECD. (2019a). Analytics for Integrity: Data-Driven Approaches for Enhancing Corruption and Fraud Risk Assessments

OECD. (2019b). Hello, World: Artificial Intelligence and its Use in the Public Sector. *OECD Working Papers on Public Governance No. 36*

OECD. (2021a). AI in Business and Finance - OECD BUSINESS AND FINANCE OUTLOOK 2021

OECD Development Matters Blog, (2021). Digitalisation as an anti-corruption strategy: what are the integrity dividends of going digital?

Per Aarvik for U4 (2019), Artificial Intelligence – a promising anti-corruption tool in development settings?

UNDP (2020), The role of technology and anti-corruption measures in fighting COVID-19

World Bank Group. (2016). Digital Dividends

World Economic Forum Global Future Council on Transparency and Anti-corruption (2019-2020), Hacking corruption in the digital era: How tech is shaping the future of integrity in times of crisis

World Economic Forum (2019), Here's how technology is changing the corruption game

Business at OECD
13-15 Chaussée De La Muette
75016 Paris
France
Tel: +33 (0)1.42.30.09.60
Email: contact@biac.org

Established in 1962, *Business at OECD* stands for policies that enable businesses of all sizes to contribute to growth, economic development, and societal prosperity. Through *Business at OECD*, national businesses and employers' federations representing over 7 million companies provide and receive expertise via our participation with the OECD and governments promoting competitive economies and better business.

This report was drafted with inputs from the *Business at OECD* (BIAC) Anti-Corruption and Digital Economy Policy Committees, under the lead of Ina Sandler, Policy Manager, and Maylis Berviller, Digital Policy Advisor, with the great support of Christina Schultheiss, Policy Intern.


BUSINESS at OECD