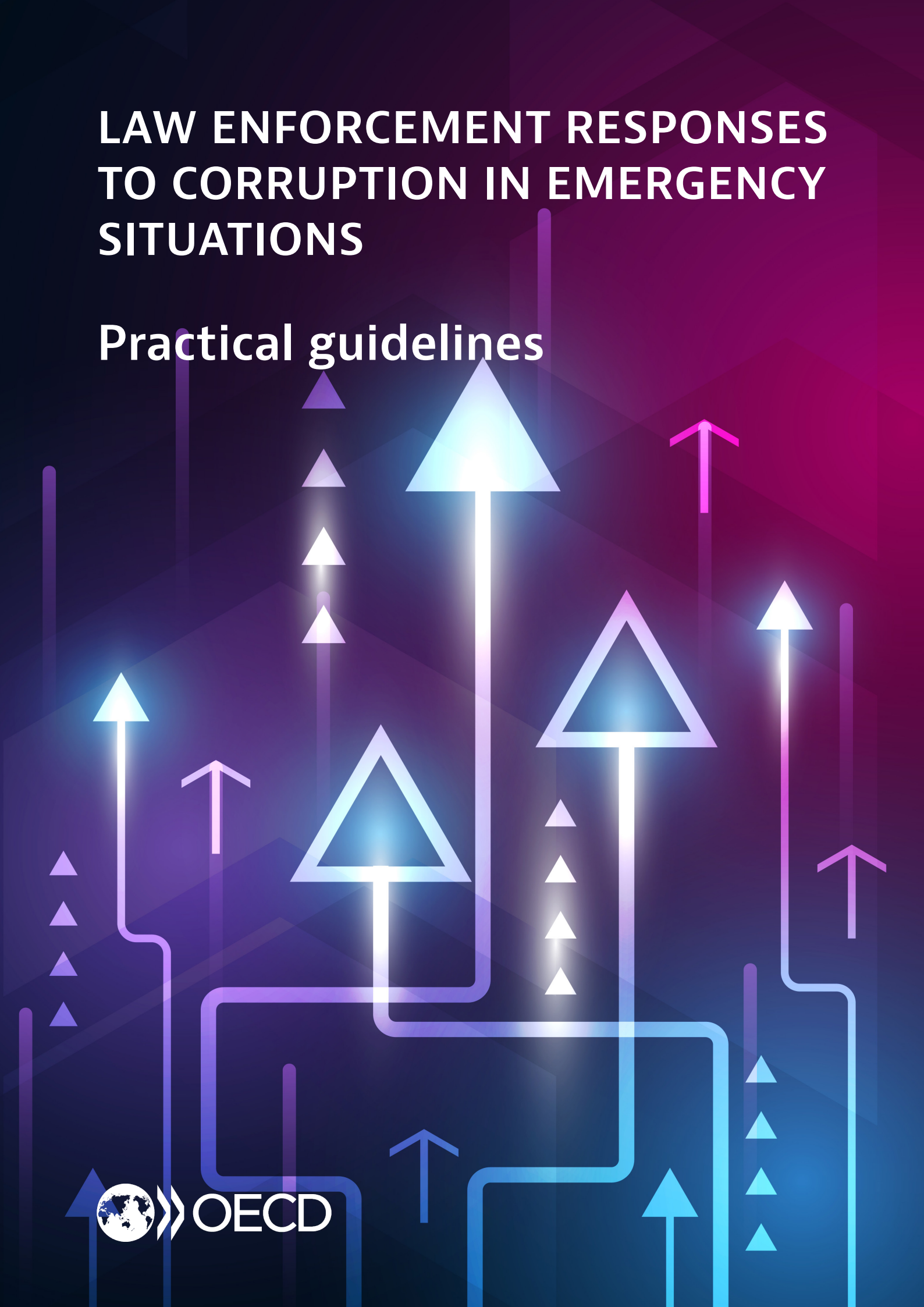
# LAW ENFORCEMENT RESPONSES TO CORRUPTION IN EMERGENCY SITUATIONS

## Practical guidelines



OECD

Please cite as: OECD (2023), *Law enforcement responses to corruption in emergencies: Practical guidelines*, OECD Business and Finance Policy Papers, OECD Publishing, Paris, https://doi.org/10.1787/b2e5344f-en.

These guidelines seek to strengthen the capacities of law enforcement practitioners to combat corruption related to the COVID-19 pandemic and other emergency situations. In particular, they aim to: (i) provide law enforcement practitioners with practical advice on the challenges law enforcement faces in an emergency crisis; (ii) illustrate good detection, investigation and prosecution practices during emergency situations and identify key challenges that may arise in future crises, including through international co-operation mechanisms; (iii) inform law enforcement practitioners about the benefits of emerging technologies and innovative institutional developments identified during COVID-19 that can assist with combating corruption.

© OECD 2023.

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Member countries of the OECD.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Cover: © ForYou13 / Getty Images.

# Acknowledgements

The OECD wishes to express its appreciation to the Government of the United States of America for their generous support to the project “Global Law Enforcement Response to Corruption in Crises”, which served as the framework for the development of these Guidelines. This report was prepared by OECD consultant Pedro Gomes Pereira, as well as by Andrii Kukharuk, Balázs Garamvölgyi and Martha Monterrosa, Anti-Corruption Analysts in the Anti-Corruption Division of the OECD Directorate for Financial and Enterprise Affairs. Elodie Beth, Senior Manager in the OECD Anti-Corruption Division, provided valuable guidance.

We are also grateful to the law enforcement practitioners who participated in a series of OECD webinars and subsequent meetings of Law Enforcement Networks in Eastern Europe and Central Asia, Latin America and the Caribbean, Asia-Pacific, and Africa, as well as meetings of the OECD Global Law Enforcement Network against Transnational Bribery, which took place during 2019-23 in the framework of the project. Many jurisdictions shared their experiences during those events which laid the foundation for this report. Additionally, we appreciate the comments from representatives of Bosnia and Herzegovina, Brazil, Chile, Costa Rica, Denmark, Lithuania, Mauritius, Nigeria, Peru, Poland, Romania, South Africa, the United Kingdom, as well as from the World Bank, the African Development Bank and the Inter-American Development Bank with respect to their experiences and which are reflected in the report. Other jurisdictions referenced have raised no objection to the substance and publication of the respective materials.

Finally, we would like to express our gratitude to Amelia Godber, Communications Officer, and Mariana Cecillon, Project Assistant, for their helpful support with the formatting, design, and promotion of this report.

# Table of contents

# Acronyms

| | |
|---|---|
| 1988 Vienna Convention | Vienna United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances |
| 4AMLD | 4th Anti-Money Laundering Directive |
| AML | Anti-money laundering |
| BiH | Bosnia and Herzegovina |
| BRL | Brazilian Real |
| CCTV | Closed-circuit television |
| CEO | Chief Executive Officer |
| CGN | Carrier grade network address translation |
| CJEU | Court of Justice of the European Union |
| COVID-19 | Severe Acute Respiratory Disease 2019 |
| DNFBPs | Designated non-financial businesses and professions |
| DPA | Deferred prosecution agreement |
| ECtHR | European Court of Human Rights |
| EFCC | Economic and Financial Crimes Commission of Nigeria |
| ESP | Electronic service provider |
| ETS 182 | Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters |
| EU | European Union |
| EUR | Euro |
| EUROJUST | European Union Agency for Criminal Justice Co-operation |
| FATF | Financial Action Task Force |
| FCIS | Financial Crime Investigation Service of Lithuania |
| FIU | Financial intelligence unit |
| FIU-NL | Financial intelligence unit of The Netherlands |
| IBA | International Bar Association |
| IberRed | Red Iberoamericana de Co-operación Jurídica Internacional |
| ICU | Intensive care unit |
| IFI | International financial institution |
| IIASB | International Audit and Assurance Standards Board |
| INL | Bureau of International Narcotics and Law Enforcement Affairs of the US Department of State |
| IPv4 | Internet Protocol version 4 |
| ISA | International standards on auditing |
| ISP | Internet service provider |
| JIT | Joint investigation team |
| MLA | Mutual legal assistance |
| NACC | National Anti-Corruption Commission of Thailand |
| NGO | Non-governmental organisations |
| NRA | National risk assessment |
| NTR | Non-trial resolution |
| OECD Anti-Bribery Convention | Convention on Combating Bribery of Foreign Public Officials in International Business Transactions |
| OECD/ACD | Anti-Corruption Division of the Organisation for Economic Co-operation and Development |
| OECD/WGB | Working Group on Bribery of the Organisation for Economic Co-operation and Development |

| | |
|---|---|
| OSINT | Open-source intelligence |
| OSP | Online service provider |
| PEP | Politically exposed person |
| PPE | Personal protective equipment |
| PPP | Public-private partnership |
| SAI | Supreme audit institution |
| SAR | Suspicious activity report |
| SIT | Special investigative technique |
| SOE | State-owned enterprise |
| SPoC | Special point of contact |
| STR | Suspicious transaction report |
| STT | Special Investigation Service of Lithuania |
| UNCAC | United Nations Convention Against Corruption |
| UNTOC | United Nations Convention against Transnational Organised Crime |
| US | United States |
| USD | United States Dollar |
| VAT | Value-added tax |
| VND | Viet Nam Dong |
| WHO | World Health Organization |
| ZAR | South Africa Rand |

# Executive summary

Law enforcement responses to corruption in emergencies come with a specific set of challenges and require devising creative solutions. Building on the lessons learned from the recent COVID-19 health crisis, the Guidelines take stock of the challenges faced during the pandemic by enforcement authorities and map out solutions and good practices that can be used in emergency situations.

The information for the Guidelines was primarily collected through a number of peer-learning webinars for law enforcement practitioners and meetings of its regional law enforcement networks and the Global Law Enforcement Network against Transnational Bribery organised by the OECD in 2020-23.

The Guidelines cover the whole spectrum of law enforcement work and the overall changes in operations of law enforcement bodies due to an emergency. This includes the detection, investigation and prosecution of corruption offences, with particular attention to high-profile corruption, and international co-operation in corruption cases. The paper's analysis is supported by case studies and practical experiences of different jurisdictions and international institutions or initiatives.

Looking forward, the Guidelines offer a range of measures that can be implemented by governmental authorities, law enforcement agencies, and in certain cases, private sector entities, to strengthen law enforcement responses to corruption in times of emergency. Where the suggested actions go beyond the mandate of law enforcement authorities and may require the involvement of other governmental bodies, they are formulated as guidance for governments.

Additionally, an Annex to the Guidelines contains a training curriculum, which puts together advice to support training centres and initiatives decide on the content and format of training courses for law enforcement officials on combatting corruption related to emergencies and develop its syllabi and study plans.

## Key findings

The restrictions imposed by the COVID-related emergency impacted the investigative work carried out by law enforcement and judicial authorities, often delaying new or ongoing investigations. Among the most common reasons for these delays were the introduction of special working regimes, the limitations of in-person contact, interruptions in the work of other public institutions and constrained international co-operation.

Certain patterns of corrupt behaviour changed or intensified during the pandemic, particularly cases of bribery, trading in influence and abuse of office in emergency-related public procurement, taking advantage of emergency exemptions and relaxed safeguards. Other regular forms of corruption were embezzlement and abuse of office linked to the allocation and implementation of support measures. In the later stages of the pandemic, there were many incidents of bribery or trading in influence for providing or obtaining falsified vaccination certificates or priority treatment in hospitals, as well as for circumventing travel and other restrictions.

These changes serve to underscore the need for law enforcement to quickly adapt to new circumstances in times of emergency to continue its proper functioning and appropriately react to new criminal patterns. The limits of human intelligence for detecting corruption highlighted the importance of strengthening in-house analytical capacities by law enforcement authorities, while the need for specific knowledge due to the nature of the crisis showed the critical role of robust inter-agency co-operation.

At the same time, emergency situations often require going beyond conventional solutions, which may trigger sustainable positive developments. For instance, the COVID-19 pandemic has accelerated the digitalisation of procedures, the introduction of remote hearings and online access to important databases in many jurisdictions.

Despite the challenges posed by the COVID-19 pandemic, jurisdictions have managed to maintain co-operation with each other. However, the imposed restrictions hindered their ability to take necessary actions, resulting in delays in cases that required in-person contact, and limited informal professional networking initiatives.

## Key guidance

### *For governments:*

- Elaborate a risk assessment specific to corruption during the emergency, to map out risks and mitigating measures, evaluate the law enforcement system and allocate resources to prioritise investigative and prosecutorial work respectively.
- Introduce legislative amendments to facilitate the undisrupted functioning of investigations and prosecutions, e.g. by the employment of new technological solutions, the extension of the statute of limitations.
- Identify and resolve legal, regulatory or operational challenges for effective and efficient inter-agency co-operation and information sharing.
- Raise awareness about the existing whistleblowing and reporting mechanisms, strengthen the whistleblowers protection measures.
- Establish or strengthen existing specialised anti-corruption law enforcement and judicial authorities.
- Strengthen the external independence of law enforcement and judicial authorities dealing with high-profile corruption cases and the internal independence of investigators and prosecutors working on such cases; provide them with necessary resources.

### *For law enforcement authorities:*

- Review case prioritisation to ensure it is aligned with the emergency-related risks.
- Develop guidelines on the use of new technological solutions, such as remote interviewing, to execute procedural steps during emergencies.
- Identify the public institutions that may possess and share emergency-related information potentially useful for detection purposes and establish or strengthen existing mechanisms for co-operation with them.
- Focus analytical efforts on the examination of emergency-related public procurement procedures.
- Examine the results of audits of emergency-related funds without delays and hold necessary consultations with Supreme Audit Institutions.

- Establish reporting channels enabling the public to make complaints or report suspected corruption allegations related to the emergency.
- Identify the forensic expertise required during the investigation planning stage, e.g. forensic auditing, preserving, collecting, and reviewing electronic evidence, while taking into account the nature of the emergency and related corruption offences.
- Review communication and public relations strategies to be able to counter illicit pressure and influencing attempts.
- Strengthen the use of law enforcement and judicial co-operation platforms as a mechanism to verify and confirm lines of inquiry in investigations, prior to the submission of requests for MLA.

***For private sector actors:***

- Raise awareness among private sector employees on the complaint, reporting and whistleblowing mechanisms available to them to report suspicions of corruption.
- Update internal controls regarding the direction and supervision of auditing teams.
- Conduct self-assessment and anti-corruption compliance audits to minimise corruption-related risks in their supply chain and day-to-day business.

# 1 Introduction

## Purpose

The general objective of these practical guidelines is to strengthen the capacities of law enforcement practitioners to combat corruption in emergencies, building on the lessons learnt during the COVID-19 pandemic. To this end, the guidelines seek to:

- Provide law enforcement practitioners with practical advice on the challenges law enforcement faces during emergencies.
- Illustrate good detection, investigation and prosecution practices during emergencies and identify key challenges that may arise in future emergencies.
- Inform law enforcement practitioners about the benefits of emerging technologies and innovative institutional developments identified during COVID-19 that can assist with combating corruption.

The practical guidelines have three sections: (i) sources of detection, (ii) investigation and prosecution, and (iii) international co-operation. Items (i) and (ii) set forth the various aspects influencing the development of a corruption-related case from the beginning until the indictment. Item (iii) outlines overarching aspects of international co-operation which can significantly impact the ability to initiate and advance a corruption-related investigation.

## Background

The restrictions imposed worldwide due to the outbreak of COVID-19 in early 2020 brought unprecedented challenges, human suffering, uncertainty and significant economic disruption on a global scale. Many governments around the world took decisive action aimed at ensuring the health of their citizens. Many also introduced economic stimulus packages to limit wide-scale lockdowns' negative social and economic consequences.

Moreover, due to the enormous demand for medical supplies and equipment at the onset of the pandemic, governments around the world used simplified or accelerated public procurement procedures, often relaxing traditional oversight mechanisms, which unintentionally created opportunities for corruption and other types of misconduct. Previous emergencies have demonstrated that they can lead to suspending or bypassing basic control systems and weakening accountability and oversight. The result is increased risks for mismanagement of public resources and corruption (INTOSAI, 2020, 4).

The G20 High-Level Principles on Preventing and Combating Corruption in Emergencies, adopted in 2021, acknowledge the increased threat the COVID-19 pandemic brought about, creating an environment where corruption may thrive. The High-Level Principles spell out the dimensions along which countries can design and implement anti-corruption responses during crises.

### Box 1.1. G20 High-Level Principles on Preventing and Combating Corruption in Emergencies

Principle 1. Enhance legislation, administrative and financial rules and regulations in preparation for crisis and ensure their maintenance during emergencies.

Principle 2. Ensure transparency, integrity and accountability of the public sector to better prevent and combat corruption in times of crisis.

Principle 3. Ensure transparency, integrity, and efficiency of public procurement processes and aid disbursement to enable prompt responses to crisis and emergencies.

Principle 4. Ensure that competent anti-corruption authorities have the proper resources and means to continue performing effectively their duties during emergencies.

Principle 5. Implement international anti-corruption obligations and strengthen international co-operation to counter corruption risks in times of crisis and emergencies.

Principle 6. Ensure transparency and integrity of the private sector to better prevent and combat corruption in times of crisis.

Principle 7. Support the positive role played by stakeholders outside the public sector in preventing and combating acts of corruption during crisis and emergencies.

The principles are further accompanied by specific measures for their application.

1. https://www.unodc.org/documents/corruption/G20-Anti-Corruption-Resources/Principles/2021_G20_High-Level_Principles_on_Preventing_and_Combating_Corruption_in_Emergencies.pdf

During the pandemic, law enforcement authorities faced significant challenges due to lockdown measures. It impacted their ability to gather evidence, meet with witnesses, liaise with relevant national authorities, and communicate with international counterparts to advance informal and formal co-operation. It also affected the traditional procedures used in pre-trial and trial proceedings.

The Anti-Corruption Division in the Directorate for Financial and Enterprise Affairs of the Organisation for Economic Co-operation and Development (OECD/ACD) launched a project in September 2020 to strengthen the capacities of law enforcement practitioners to combat corruption related to the COVID-19 pandemic and other emergencies. The United States (US) Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL) supports the initiative.

The project conducted a series of peer learning webinars for law enforcement practitioners on the following topics: (i) combatting corruption related to emergency procurement and stimulus packages, (ii) whistleblower reporting on corruption and their protection, and (iii) interagency co-operation and co-ordination at the national and international levels. While the project is a global initiative, a peer-learning framework was split by the following regions: Africa, Eastern Europe and Central Asia, Asia Pacific, Latin America and the Caribbean. The 2022 meeting of the OECD Global Law Enforcement Network against Transnational Bribery (GLEN) provided a forum for the exchange of relevant practices and experiences at the global level.

Building on these law enforcement sessions, the OECD/ACD developed these practical guidelines to facilitate the broad-based application of good practices. They further consider the lessons learned and practical solutions used by law enforcement in the detection, investigation and prosecution of corruption during emergencies, including COVID-19.

## Emergencies

While these practical guidelines take examples from the COVID-19 pandemic, they present practical advice and good practices for *emergencies in general*. These practical guidelines define *emergencies* as situations when rapid response policies are adopted by jurisdictions to address significant adverse economic or social impacts, or both, resulting from an actual or imminent natural or man-made crisis or disaster. For the purpose of these practical guidelines, the scope excludes armed conflict from *emergencies* due to the distinct nature of such conflicts, which requires a separate analysis.

The definition proposed in these practical guidelines is broader than the term *state of emergency*, which implies giving governments extraordinary powers to address existential threats to public order and allowing them to limit or derogate certain rights. These practical guidelines took this approach since not all jurisdictions have imposed states of emergency during the COVID-19 pandemic. Providing a specific definition for *emergencies* enables the guidelines to cater to a wider audience of law enforcement and prosecutorial authorities, thereby remaining relevant to a broad base by acknowledging that an emergency may not always result in a government-mandated state of emergency.

## Beneficiaries

The **direct beneficiaries** of these practical guidelines are law enforcement and prosecutorial authorities responsible for detecting, investigating, and prosecuting corruption-related offences. If the guidelines mention law enforcement authorities, this includes prosecutors as well. While several models and constitutional arrangements characterise the organisation of Prosecution Services around the world, regardless of the model followed, they are an integral part of the criminal justice system and criminal proceedings. While their role and powers may differ during the investigation, due to their mandate, prosecution services are also the primary target audience of these guidelines.

The **indirect beneficiaries** are decision-makers responsible for implementing policies related to emergencies and designing procedures to deal effectively with corruption-related offences in emergencies. The respective parts of these guidelines are also relevant for representatives of governmental bodies that are key counterparts of the law enforcement system in providing an efficient response to emergency-related corruption (tax authorities, FIUs, public officials responsible for review and verification of asset disclosures, public procurement processes, auditors in supreme audit institutions, investigative journalists, and the private sector.

# 2 Changes to operational practices

### Guidance 1. Changes to operational practices

**For governments:**

- Elaborate a risk assessment specific to corruption during the emergency, to map out risks and the respective mitigating measures.
- Evaluate the law enforcement system and allocate resources to prioritise investigative and prosecutorial work based on the risk assessment.

**For law enforcement authorities:**

- Review case prioritisation to ensure it is aligned with the emergency-related risks.
- Develop guidelines on the use of new technological solutions, such as remote interviewing, to execute procedural steps during emergencies.
- Modify working regimes to ensure the continuity of the operation and introducing necessary protection measures for staff members if required by the nature of the emergency.

The OECD collected information through surveys regarding the challenges and responses law enforcement had during the COVID-19 pandemic. The responses showed that the restrictions imposed by the emergency impacted the investigative work carried out by law enforcement and judicial authorities, often delaying new or ongoing investigations.

The response received from the surveyed jurisdictions regarding the impact of the COVID-19 pandemic on law enforcement and prosecutorial work is divided into four categories: (i) organisational changes, (ii) amended legal procedures, (iii) prioritisation of law enforcement activities, and (iv) international co-operation.

*Concerning item (i),* a common cause cited by the surveyed jurisdictions was the challenge in conducting investigative actions involving persons, e.g. interviewing witnesses and suspects, or conducting searches. Many jurisdictions overcame those challenges by introducing the use of remote investigative tools to conduct interviews, e.g. videoconferencing or written procedures. In doing so, such measures enabled law enforcement to continue collecting evidence and advancing in their investigations. Nevertheless, the surveys also showed that in other jurisdictions, law enforcement either continued to carry out in-person investigative activities, where possible, or had to postpone such measures.

Moreover, to ensure the safety of staff, the surveyed jurisdictions noted they adopted special working regimes which allowed non-essential personnel to work remotely. Shifts were organised for staff that continued to work on-site. Some jurisdictions, however, did not adopt special working regimes and continued to operate at full capacity while enforcing additional protective measures.

*Concerning item (ii),* to ensure the continuity of the work of the judiciary, surveyed jurisdictions amended court procedures to facilitate virtual proceedings, e.g. videoconferencing or written procedures. However, because some jurisdictions did not have legal provisions for remote court hearings, challenges may arise regarding, among others, the admissibility and authenticity of evidence. Finally, some jurisdictions suspended or extended procedural deadlines for criminal cases that did not qualify as urgent. Other jurisdictions suspended or extended statutes of limitation for the duration of the emergency measures.

*Concerning item (iii),* the surveyed jurisdictions prioritised investigations by (a) suspending all preliminary investigations except when the custody period of a suspect had expired; while continued the procedure (b) when the investigation was at an advanced stage; or (c) the investigative activities were considered urgent. The response to the survey further noted that the number of preliminary investigations decreased during the emergency due to new priorities set in response to the COVID-19 pandemic.

*Concerning item (iv),* surveyed jurisdictions noted that the COVID-19 pandemic had an impact on both the issuing and on the execution of requests for mutual legal assistance (MLA) and other forms of international co-operation, e.g. joint investigation teams, extradition.[1] These practical guidelines note, however, that jurisdictions continued to co-operate with each other despite the emergency but were limited in their actions due to the imposed restrictions.

Compounding the information received from the participating jurisdictions, one can conclude that in emergencies such as the COVID-19 pandemic, factors beyond the control of law enforcement, e.g. natural or man-made disaster, operational necessities, and safety protocols in place to deal with the emergency, result in a delay or suspension of investigations, due to reprioritisation of the activities of law enforcement, prosecutorial and judicial authorities, and due to challenges resulting from the emergency itself.

The effective detection and investigation of corruption-related offences requires a permanent evaluation of risks[2] and threats[3] to the system. Therefore, an emergency should be viewed as a risk resulting in threats to the investigative activity conducted by law enforcement. To that end, it is recommendable that national authorities conduct a risk assessment arising from the emergency and determine mitigating measures to reduce the impact generated by the risk.[4]

Taking the COVID-19 pandemic as an example of an emergency, the risks arising to investigation and prosecution can be divided into three broad categories:

- **Situational:** governmental response to the emergency, e.g. emergency procurement procedures, expansion of social security, furlough schemes and reallocation of resources.
- **Operational:** the ability of law enforcement to conduct their core activities in detecting, investigating and prosecuting criminal offences due to restrictions imposed by the emergency.

---

1 See Chapter 5 of these practical guidelines for more detail on the issues faced by jurisdictions during emergencies concerning their international co-operation efforts.

2 These practical guidelines understand *risk* as an effect of uncertainty on objectives, where *effect* is a deviation from the expected, whether positive or negative and can address, create or result in opportunities and threats (ISO, 2018).

3 These practical guidelines understand *threats* as elements in the external environment that can endanger the activity of law enforcement and their ability to operate effectively.

4 See, e.g. Box 3.2. Lithuania case studies – abuse of office and trading in influence in procuring COVID-19 tests

- **Specific:** the ability of national authorities to detect and identify the risks arising from the situational response from the government vis-à-vis the operational limitations imposed by the emergency.

To facilitate the work and speed of elaborating a specific risk assessment for the emergency, jurisdictions should take the lessons learnt from previous emergencies to build a template risk assessment whose methodology can be applied, and its results updated based on future emergencies. Additionally, the results from the risk assessment for the emergency need to be implemented in practice. This requires law enforcement and prosecutorial agencies to review their case prioritisation and resource allocation to ensure they address the specific risks arising from the emergency, e.g. scale or criminality or corruption, types of crimes under investigation, seniority of the PEPs involved, level of transnationality.

In particular, the risk assessment would benefit from the analysis of typologies of corruption offences committed in previous emergencies. Even though previous corruption schemes will not necessarily be fully replicated in each next emergency, there may be a high probability of similar patterns of criminal activity, especially in emergencies of the same nature.

Based on the analysis of information from open sources and information shared by law enforcement practitioners during peer learning activities organised under this project, it is possible to identify typologies of relevant corruption schemes specific to the COVID-19 pandemic.

Generally, these corruption offences can be classified into the following three kinds of corruption practices:

- Bribery, trading in influence and abuse of office in emergency-related public procurement when the vendors were awarded contracts for the purchase of overpriced or substandard medical and protective equipment. The public officials involved in or being able to influence the procurement process were asking for or accepting bribes in exchange for a positive decision. Often the selected suppliers had no or little experience in medical products trade or production.
- Embezzlement of public funds allocated to support business and households or provide necessary public services during the emergency period, abuse of office when making decisions on the allocation of resources or implementation of support measures.
- Bribery or trading in influence for providing or obtaining falsified vaccination certificates or priority treatment in hospitals, as well as for circumventing travel and other restrictions.

### Box 2.1. Thailand case study – risk assessment at the onset of the COVID-19 pandemic

The National Anti-Corruption Commission of Thailand (NACC) published a report at the onset of the pandemic to analyse COVID-19 corruption situation and identify corruption risks based on the NACC's study on COVID-19 crisis in Thailand, as well as related information collection e.g. the Government's responses, provincial-based corruption case statistics, and interviews of local anti-corruption experts. The report included policy recommendations for the government on regulations and practices in administering its recovery fund and encouraging citizen and media reporting via existing reporting mechanisms and prioritising whistleblower protection.

The report produced the following outputs:

(i) *A case study research on corruption in the COVID-19 pandemic.* The case study research analysed corruption circumstances which arose during the COVID-19 pandemic in Thailand and facilitating factors for corruption during the COVID-19 pandemic. It enabled the NACC to establish corruption prevention scenarios for the COVID-19 pandemic and other emergencies.

(ii) *Corruption risk mapping in the COVID-19 pandemic in Thailand.* The risk mapping sought to produce a nationwide database on corruption, as it identified risk areas vulnerable to corruption on a provincial basis. The exercise included the participation of the public in every province around Thailand. The preliminary analysis identified opportunities for corruption during the COVID-19 pandemic and allowed the NACC to better control and prevent corruption, that might occur in government projects in relation to: 1) COVID-19 prevention; 2) remedial action for affected persons; and 3) the implementation of other programmes not directly related to the COVID-19 pandemic but taking advantage of the situation where public attention was diverted to COVID-19 related corruption, e.g. to corruptly expedite execution of non-COVID-19 related projects.

(iii) *Guidelines on effective corruption prevention during the COVID-19 pandemic and in other emergencies that may arise.* According to the research categorising the patterns of corruption into 6 main scenarios (corruption in budget administration, corruption in the public procurement process, corruption in facilitating benefits for private entities, corruption in stockpiling commodities and trading excessive profit, corruption risks in providing remedial action for affected persons and corruption of donations and donated items for affected persons), the NACC proposed four main lines of action for effective prevention and combating of corruption-related offences: revision of legislation and preparation of practical guidelines in emergencies, integration of data, proactive inspection, and participation of civil society.

The report sought to prevent and combat corruption in an efficient, holistic and knowledgeable manner, and to be the model for proactive corruption prevention and suppression during emergencies and normal times.

The NACC utilised pre-COVID-19 communication channel between the Interior Ministry and its 76 provincial offices to publish the report and ensure that the government agencies follow its guidelines included therein.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

### Box 2.2. Spain case study – inter-agency co-operation through the analytical support units within the special prosecution service against corruption and organised crime

The special prosecution service against corruption and organised crime of Spain has established in-house two new support units, one from the tax administration (*Agencia Estatal de Administración Tributaria* – AEAT) and another from the Comptroller General of the State (*Intervención General de la Administración del Estado – IGAE*). Pursuant to the collaboration agreement (Interior et al., 1995), the support units provide advice to the special prosecution service against corruption and organised crime on financial, accounting and fiscal matters, and, more generally, on economic matters.

Public officials seconded by the AEAT and the IGAE staff the support units. This allows the seconded officials to share with the special prosecution service information available in their respective agencies, e.g. tax, commercial and procurement information. The information and analyses prepared by the support units enable the special prosecution service to further their investigations and request relevant information from financial institutions.

Having the AEAT and IGAE support units further allow the special prosecution service to have a comprehensive overview of tendering procedures, from the perspective of both the public and private sectors. During the COVID-19 pandemic, the support units were critical to review the correctness and lawfulness of tendering procedures, and whether offences concerning public funds occurred. It also enabled the special prosecution service to engage in international co-operation regarding Spanish companies allegedly committing foreign bribery.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project and (España, 2022, 534-535).

# 3 Sources of detection

As stressed in the OECD study on the Detection of Foreign Bribery, detecting the crime is the first step, and a challenge, to any effective enforcement of the OECD Anti-Bribery Convention.

The study found that a number of potential detection sources under review were largely untapped and that much could be done by Convention Parties to improve the use of these sources to improve the detection of foreign bribery. It also highlights that adequate legal and institutional frameworks are the first step to promote detection by a given source, and that, in many instances, awareness and training are also key to detection. In addition, the study shows the complexity of the process of detecting foreign bribery.[5]

While these findings and conclusions are explained by certain features of the foreign bribery offence that make the difficulty of identifying it more significant, the detection of many other corruption-related offences, especially at times of crisis, may also be quite problematic and complex, and features similar issues.

Successful detection of corruption requires that law enforcement bodies are aware of the potentials of a wide range of different sources of information, have well-established channels of communication for receiving information, and have sufficient resources and expertise to process and analyse it properly.

The absence of these conditions leaves law enforcement with the significant challenge of uncovering corruption. Emergencies further compound this challenge. Restrictions they impose mean that law enforcement may be unable, or severely restricted, to ensure the adequate performance of its detection function. Moreover, the features of crisis-related corruption offences, the proper reaction to which is often among the priorities for law enforcement during an emergency, may require quick adjustments to usual detection practices.

This chapter of the practical guidelines lists the most relevant sources (including methods, technological solutions, relevant institutions etc.) of information in the context of detecting corruption related to emergencies.

[5] The OECD Study of the Detection of Foreign Bribery, p. 9, https://www.oecd.org/corruption/anti-bribery/The-Detection-of-Foreign-Bribery-ENG.pdf

## Criminal intelligence

### Guidance 2. Criminal intelligence

**For law enforcement authorities:**

- Review their processes for gathering human intelligence to minimise the risks arising from the emergency while ensuring the safety of their officers and human intelligence assets.
- Use technological solutions to obtain human intelligence while minimising face-to-face interaction and ensure the safety of their informants and co-operating witnesses.

Intelligence is the enhancement of raw information, providing additional knowledge about the activities of perpetrators; it is information designed for action (EUROPOL, 2003, 9; Brown, 2007, 338). The term *criminal intelligence* refers to how law enforcement approaches the detection and investigation of an alleged crime and its perpetrators by using the intelligence and information collected concerning them (UNODC, 2011, 7). The success of an investigation rests upon the choice of investigative tools[6] and powers[7] and their re-evaluation as facts and evidence come to light during the investigation (Monteith and Gomes Pereira, 2015, 146).

The primary sources of information related to the detection of a criminal offence are (i) data, (ii) objects and (iii) persons. Law enforcement and prosecutors may later transform these sources of information into evidence through an investigation.

However, in corruption-related offences, persons with knowledge about the alleged crime may not be willing to come forward due to fear of retaliation. Witnesses may be unaware of or alert to the offence occurring before them and may need to be made aware of the importance or existence of reporting channels[8] (OECD, 2017, 9). The suspects may not be readily identifiable either because they can use complex corporate structures to hide their identity or because complex management structures in legal entities do not allow assigning the responsible person. Physical evidence may be insufficient to substantiate all elements of a corruption offence.

Detection thus relies on additional sources of information, including (i) information from hotlines or the public (see Box 3.17. Nigeria case study – Eagle Eye application); (ii) informants; (iii) surveillance and other types of covert operations; (iv) public surveillance systems (e.g. closed-circuit television – CCTV); (v) information from previous investigations, convictions, traffic databases, etc.; (vi) information from other law enforcement agencies (see Box 3.6. South Africa case study – the ); (vii) telecommunications records.

However, several challenges to obtaining criminal intelligence emerge during an emergency. The use of informants or surveillance may be limited. During the COVID-19 pandemic, the restriction of movement of persons imposed by many jurisdictions limited the ability of law enforcement to engage with sources of human intelligence.[9] On the other hand, emergencies bring corruption risks that require

6 The term *investigative tools* refers to the devices and software used by law enforcement and prosecutors to conduct an investigation.

7 The term *investigative powers* refers to legal authority law enforcement and prosecutors have to conduct investigations and implement their investigative tools and techniques.

8 See section regarding whistleblowers/reporting persons.

9 (See: Intelligence, 2011, 53-54)The term *human intelligence* refers to the collection of information, orally or via documentation, provided directly by a human source. It is the only type of intelligence collected by speaking

co-operating with informants in specific sectors. Thus, law enforcement and prosecutorial agencies might find appropriate to undertake efforts to identify the factors affecting their ability to collect criminal intelligence, in particular human intelligence, depending on the type of emergency, and adapt their practices and allocation of resource respectively.

## Financial intelligence

### Guidance 3. Financial Intelligence

**For law enforcement authorities:**

- Request FIUs to prepare strategic analyses that guide the emerging patterns of criminality resulting from the emergency and use it for adapting detection practices.
- Routinely utilise operational analyses prepared by FIUs as a source of information to better detect the commission of corruption and its ancillary offences during an emergency.

The flow of assets through the financial system leaves an audit trail record, which can be tracked and detected by financial investigators. Perpetrators of corruption-related offences will attempt to break this audit trail by disguising their proceeds' true origin, nature and ownership.

To do so, they will use different money laundering methods[10] and typologies.[11] The perpetrators may thus set up accounts in different jurisdictions held in the name of legal persons[12] or legal arrangements,[13] allowing them to distribute the proceeds of their crimes among different accounts nominally held by different legal entities. They may likewise use third parties not involved in the commission of the predicate offence to launder the proceeds of crime (FATF, 2018a, 111; FATF, 2018b, 10). Law enforcement must thus build a financial profile of the perpetrators while tracing their assets (Monteith and Gomes Pereira, 2015, 147).

The financial intelligence unit (FIU) is an essential component of any anti-money laundering (AML) regime, particularly during the detection, pre-investigation and intelligence-gathering stages (OECD, 2017, 85). The FIU acts as an interface between the private sector and law enforcement, assisting with the flow of relevant financial information between them. They are a national centre for the receipt and analysis of suspicious activity reports (SARs) and other information relevant to money laundering and associated predicate offences and for disseminating the results of their analysis (FATF, 2019). FIUs support law enforcement action in three main ways:

- *National risk assessment (NRA).* The NRA is essential for efficiently allocating resources across the AML regime. The Financial Action Task Force (FATF) requires jurisdictions to identify,

to the sources of information. Human intelligence can obtain access to information that is not obtainable in any other way (Intelligence, 2011, 53-54).

10 The three main methods used by perpetrators laundering the proceeds of crime are through the (i) use of the financial system, (ii) physical movement of money, and (iii) movement of goods and services (FATF, 2006, 1).

11 The term *money laundering typologies* refers to the techniques used by perpetrators to launder money. These methods vary from place to place and over time.

12 The term *legal persons* refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property (FATF, 2019, 122).

13 The term *legal arrangement* refers to trusts or other similar legal arrangements (FATF, 2019, 122).

assess and understand the money laundering risks for the jurisdiction (FATF, 2019). Based on that assessment, the jurisdiction should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering are commensurate with the risk identified.

- *Strategic analyses.*[14] It is the process of developing knowledge to be used in shaping the work of the FIU in the future. Strategic analyses are not related to individual cases but to issues and trends. Thus, it may consist of identifying evolving criminal patterns or providing broad insights into emerging patterns of criminality at the national level.
- *Operational analyses.* SARs filed by reporting entities[15] with the FIU enable it to analyse them and disseminate their operational analysis reports with suspicions to the competent authorities (FATF, 2019, 97).

Linking financial information to possible underlying forms of crime is one of the critical challenges in this process (OECD, 2017, 85). Together with other sources of information, law enforcement can more effectively detect the commission of corruption-related offences. Thus, law enforcement should seek to co-operate with FIUs to obtain relevant financial intelligence to support their criminal and financial investigations (FATF, 2018a, 78).

However, risks associated with the emergency may increase corruption-related risks associated with the large amounts allocated to deal with the emergency. Thus, during the COVID-19 pandemic, risk assessments conducted by FIUs have demonstrated an increased risk associated with procurement contracts in the health care sector. These include, for example, the infiltration of criminal organisations in the supply chain of medical equipment or collusion between suppliers and retailers to inflate the price of essential products (Group, 2022, 7).

During the COVID-19 pandemic, FIUs faced institutional and operational challenges. From an institutional perspective, an emergency creates, among others, challenges related to business continuity, maintaining information confidentiality and professional development of staff (Group, 2022, 5). Moreover, lockdowns and movement restrictions required FIUs to adopt continuity plans for their functions while adapting to reduce person-to-person contact. The continuity plans included switching to remote work, establishing strict shifts and dividing usual work shifts (Group, 2022, 7).

14 The term *strategic analysis* refers to available and obtainable information, including data that other competent authorities may provide, used to identify money laundering-related trends and patterns. This information is also used by the FIU or other entities to determine money laundering threats and vulnerabilities. Strategic analysis may also help establish policies and goals for the FIU or other entities within the anti-money laundering regime (FATF, 2019, 97).

15 See FATF Recommendations 20 and 22. The term *reporting entities* encompass financial and designated non-financial businesses and professions (DNFBPs) (FATF, 2019). DNFBP encompasses casinos, real estate agents, precious metals and stones dealers, lawyers, notaries, independent legal professionals and accountants, and trust and company service providers.

### Box 3.1. The Netherlands case study – awareness raising regarding risks generated by the COVID-19 pandemic

The Dutch Government put in place an emergency package of measures to compensate for the damage to the economy. The emergency led to various forms of financial and economic crime, including fraudulent purchases through fictitious parties of medical protective equipment, fraudulent payment of crisis benefits, CEO and invoice fraud, and changes in common ways of money laundering.

The FIU of The Netherlands (FIU-NL) sought co-operation with law enforcement and the public prosecution service to combat these new money laundering risks. To assist reporting entities in detecting these new risks, the FIU-NL communicated COVID-19-fraud-specific indicators through a newsletter. Additionally, the FIU-NL requested reporting entities to mark COVID-19-related reports. These actions enabled the FIU-NL to assemble a team to analyse the newly reported unusual transactions daily.

Furthermore, the FIU-NL sent three newsletters to obliged entities containing alerts, anonymised cases and risk indicators (red flags). The communication strategy allowed the reporting entities to set up transaction monitoring to detect unusual transactions such as aid scheme fraud.

Source: Egmont Group (2022).

From an operational perspective, while money laundering reporting processes did not experience particular delays given their reliance on electronic reporting methods (Group, 2022, 5-6), the number of on-site inspections decreased due to lockdowns or other movement restrictions (Group, 2022, 6). The lack of on-site supervision could have resulted in criminals attempting to manipulate financial systems. Nevertheless, FIUs reported that stakeholder co-operation and communication increased despite decreased on-site inspections (Group, 2022, 6).

Emergencies like the COVID-19 pandemic generated various government responses, from social assistance to tax relief initiatives and movement restrictions of persons. These movement restrictions and the restriction of services provided by financial institutions in person, in turn increased the number of remote transactions through online banking activities (FATF, 2020, 8). In contrast, financial institutions increased online customer onboarding and identity verification, postponing some aspects of customer identity verification throughout the emergency. At the same time, the increase in the use of online banking platforms, including by certain population segments less familiar with such platforms, made them more susceptible to fraud.

According to the Egmont Group, FIUs overcame the challenges presented by the COVID-19 pandemic by (2022, 5-7):

- Applying new IT tools and methodologies to the business model of the FIUs, embedding new forms of communication into existing business practices with reporting entities and competent authorities, e.g. communication campaigns via email, newsletters, documents and educational guides to educate reporting entities on how to detect risks and prevent money laundering during the pandemic.
- Engaging stakeholders through virtual meetings, conducting compliance reviews aimed at building relationships and providing compliance advice and guidance that created familiarity with the statuses of reporting institutions without negatively affecting their work quality.
- Enacting and implementing emergency plans or protocols to ensure adequate staff working conditions.

### Box 3.2. Lithuania case studies – abuse of office and trading in influence in procuring COVID-19 tests

In Lithuania, the Financial Crime Investigation Service (FCIS) and the Special Investigation Service (STT) opened an investigation into alleged abuse of office involving the procurement of COVID-19 test kits by the National Public Health Surveillance Laboratory (NPHSL).

The case relates to the allocation of a contract valued at EUR 6 million in March 2020 to a small Lithuanian biopharmaceutical company by the NPHSL and, indirectly, the Ministry of Health, despite the company not having found a supplier and other operators making significantly cheaper offers. In addition to the alleged overpricing of the test kits, they were deemed unsuitable for diagnosing acute COVID-19 infections.

The FCIS launched its pre-trial investigation following the receipt of the information on suspicious financial transactions (STR). The company transferred around EUR 6 million to a Lithuanian consultancy firm created two days before the transfer of the funds, and then purchased the test kits from an Austrian company for only around EUR 1 million.

A high-ranking public official resigned in August 2020 following the FCIS naming the official as a suspect and subjecting this person to a departure prohibition order. The official was later charged with abuse of office. Five other persons were also being investigated in connection with the case, including the company's chief executive officer (CEO) and chief operations officer (COO).

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

## Information received through other inter-agency co-operation channels

### Guidance 4. Inter-agency co-operation

**For governments:**

- Identify and resolve legal, regulatory or operational challenges that institutions may encounter when collaborating.

**For law enforcement authorities:**

- Identify the public institutions that may possess and share emergency-related information potentially useful for detection purposes.
- Verify whether existing inter-agency platforms may be used or repurposed to deal with the emergency or establish a specific inter-agency platform to deal with the emergency.

### *Overall co-operation considerations*

Emergencies require government and law enforcement agencies to co-operate, communicate and co-ordinate their actions closely. During the COVID-19 pandemic, governments allocated extraordinary funds to address the emergency and applied special rules to allocate and spend such funds. The purpose was to ensure celerity and effectiveness in addressing the emergency. Moreover, different authorities were assigned with specific tasks to organise an efficient response.

However, the exceptional measures enacted during emergencies created new risks and opportunities for perpetrators to commit corruption-related offences but also brought challenges for law enforcement to detect, investigate and prosecute such offences effectively. Law enforcement must understand the tasks assigned to those authorities during the emergency and learn what and which kind of information they may possess. This allows law enforcement to have a full overview of the information available, gaps in the information chain and the potential risks arising from the measures taken to address the emergency.[16]

In this context, the relevant counterparts are intelligence agencies, anti-corruption and integrity authorities, regulators, other law enforcement agencies and tax authorities. Also, the situation during the COVID-19 pandemic made evident the importance of co-operation with 1) *comptrollers and procurement bodies* responsible for initiating or reviewing (simplified) procurement procedures, their legal bases and requirements for the delivery of goods and services by the contractor; 2) *National audit agencies and supreme auditing institutions* responsible for conducting audit indicating the use of public funds; 3) *National health services:* in the context of health crises, responsible for establishing the needs for and distribution of medical equipment, e.g. PPEs, ventilators, information on vaccines and percentage of the population vaccinated. Finally, co-operation with private sector actors, especially those dealing with emergency-related supplies or possessing financial information, may represent additional detection opportunities.

There are several challenges associated with enabling inter-agency co-operation. They range from privacy concerns regarding the information held by a specific institution to legal limitations for sharing information available to them. At the operational level, challenges to inter-agency co-operation include a perceived or actual threat to the autonomy of an institution or the resources of an institution. They also include issues on a lack of trust among institutions.

Jurisdictions should establish legal gateways to enable information sharing among law enforcement, government agencies and the private sector. These legal gateways may provide different arrangements to apply in different circumstances (OECD, 2013, 14-15). Under all types of co-operation[17] concerning sharing information among different agencies, it is essential to protect the confidentiality of the information and the integrity of work carried out by other agencies (OECD, 2013, 15). Enabling these legal gateways results in faster and more successful prosecutions and increases the likelihood of the proceeds of crime being recovered (OECD, 2013, 14).

The list below includes some legal gateways law enforcement and government agencies may wish to consider:

- *Inter-agency task forces.* A dynamic and proactive manner to detect and investigate corruption-related offences is to form topic-specific task forces.
- *Signing Memoranda of Understanding (MoUs)*. Information sharing among relevant law enforcement and government agencies may be restricted or otherwise unregulated. In such cases, they should strive to enter into MoUs to determine the type of information to share in specific circumstances and how different agencies may use it. Such MoUs can be prioritised and established based on identified risks.

16 See, e.g. Box 3.2. Lithuania case studies – abuse of office and trading in influence in procuring COVID-19 tests.

17 The OECD has identified four different types of co-operation with respect to sharing of information among different agencies (OECD, 2013, 15): (i) direct access to the information contained in the agency records or databases, (ii) an obligation to provide information spontaneously, i.e. reporting obligation, (iii) the ability, but not the obligation, to provide information spontaneously, and (iv) an obligation or ability to provide information only on request.

- *Collaboration on a case-by-case basis*. Where collaboration is not possible or desired at the institutional level, law enforcement and government agencies may wish to consider setting up collaboration mechanisms for specific cases.

These possibilities are available and applicable to inter-agency co-operation not only during emergencies, but also during regular times. However, where inter-agency co-operation mechanisms are already in place, it becomes quicker to act vis-à-vis the emergency. Thus, South Africa was able to use an existing inter-agency mechanism – the Fusion Centre – and to use it for the specific risks associated with the COVID-19 pandemic (see Box 3.6. South Africa case study – the ). On the other hand, the UK used existing mechanisms – the National Economic Crime Centre (NECC) to set up a specific inter-agency initiative – the Fusion Cell – to detect criminal activity seeking to exploit the COVID-19 pandemic for financial gain (see Box 3.7).

### Box 3.3. Italy case study – Special subgroup of prosecutors dealing with COVID-19-related cases

In Italy, the prosecution service noted that the COVID-19 pandemic presented the following characteristics: (i) Decision making at the central level, while (ii) procurement, selection of tenderers and awarding of contracts were done in a decentralised manner.

To identify wrongdoing, the special subgroup took a threefold approach in their methodology:

(i) The analysis of financial flows, in collaboration with the Italian FIU, to detect anomalies.

(ii) The analysis of products supplied by the contractors, to verify their appropriateness.

(iii) Background verification of the contractors, in collaboration with the Financial Police (*Guarda de Finanza*), to identify any anomalies.

The methodology above allowed the special subgroup to identify three main typologies: (i) false declarations, (ii) non-compliance and (iii) illicit intermediation between public and private actors to access public contracts. Critically important to the work of the special subgroup was to determine whether the wrongdoing stemmed from a mistake, or whether it constituted a criminal offence.

In an actual case, the public authority handling a simplified tender filed the complaint. They identified anomalies found in the documentation produced by the contractor. The analysis of the corporate history of the contractor showed fictitious sale of shares between shareholders. This had been done because of previous convictions of one of the directors of the company, and the company sought to circumvent the prohibition of participation in the tender for companies with members with previous convictions. During the investigation, the prosecution service conducted special investigation techniques,[18] i.e. wiretapping, to demonstrate the fraudulent intentions of the defendants. Convictions have been obtained in the first instance and on appeal.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

[18] See section on Special investigative techniques of these practical guidelines.

### Box 3.4. Kazakhstan case study – misappropriation of funds by director of morgue

The case involved a corruption scheme in a morgue in Kazakhstan. It was detected by law enforcement authorities through the monitoring of state funds allocated to combat the COVID-19 pandemic.

The morgue entered into a contract in 2020 to purchase vehicles to transport biological waste. The director of the company that won the tender was the morgue director's driver. The investigation showed that the management of the company later changed to a different person, a friend of the driver. However, the services were provided by companies other than the contracted company. Ultimately, the director of the morgue obtained funds originating from the state budget by having it withdrawn in case that had been deposited into the funds via his driver's bank account.

Moreover, a worker in the morgue who participated in the scheme requested payments from the families of victims of COVID-19 to provide services that were never rendered. At the same time, the services for which the worker in the morgue requested payment were already being paid through the state budget. The case was initiated from information provided by the families of the victims of COVID-19.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

### Box 3.5. Kenya case study – KEMSA case

The case involves irregular procurement and alleged fraudulent payments concerning the purchase and supply of COVID-19 emergency commodities by the Kenya Medical Supplies Authority (KEMSA), amounting to USD 68.5 million, in 2020. High-ranking officials were suspended over suspicions of corruption in the procurement of PPE. A former PEP allegedly influenced the award of tenders to certain private companies.

The first phase of investigations centred around the alleged misuse of USD 7.8 million meant to purchase emergency PPE for health care workers and hospitals across Kenya. The second phase of investigations focused on companies alleged to have improperly benefitted from the tenders.

The case demonstrates robust inter-agency co-ordination and co-operation, as the Ethics and Anti-Corruption Commission (EACC) of Kenya co-operated with multiple national agencies during its investigation:

- *The Office of the Auditor General (OAG)* undertook a special audit on the utilisation of COVID-19 funds by KEMSA. Some key findings include an irregular reallocation of funds and overpayment of the PPEs supplied. The EACC incorporated these findings into its investigation.
- *The Kenya Revenue Authority (KRA)* verified compliance with tax obligations for the suppliers. EACC considered the KRA's report during the investigation.
- *The Public Procurement Regulatory Authority (PPRA)* evaluated the procurement process and prepared an expert report. This report assisted EACC with technical issues during its investigation.
- *Parliamentary committees (Public Investments Committee – PIC, and Public Accounts Committee – PAC)* also prepared reports on KEMSA.
- *The Financial Reporting Centre (FRC)* monitored and provided reports on suspicious financial transactions related to persons of interest in the investigation. The EACC used these reports in its financial investigation.
- *The Office of the Attorney General (OAG)* advised the EACC on applicable procurement procedures concerning COVID-19-related emergency procurement.
- *The Office of the Director of Public Prosecutions (ODPP)*, in co-ordination with EACC, appointed a joint team to expedite investigations into COVID-19-related corruption cases.

The enforcement action against the alleged perpetrators is ongoing at the time of publication.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

### Box 3.6. South Africa case study – the Fusion Centre

**Background**

The Fusion Centre brings together relevant law enforcement agencies to share information and resources to combat fraud and corruption in procuring COVID-19-related goods and services. The Fusion Centre has had multiple investigations and prosecutions, resulting in millions of South African Rands (ZAR) in public funds being preserved or recovered.

The South Africa Anti-Corruption Task Team (ACTT) approved the establishment of the Fusion Centre in 2018 as a collaborative and intelligence-driven platform for addressing national priority crimes related to money laundering and terrorist financing, and related activities. In 2020, it received the mandate to investigate all allegations of unlawful conduct concerning COVID-19. It is, among others, a primary response co-ordination mechanism to focus on corruption, fraud and theft concerning the response to COVID-19.

**Relevant national authorities**

During COVID-19, South Africa implemented institutional and operational measures to detect and investigate corruption through inter-disciplinary teams and inter-agency co-ordination.

The Fusion Centre is made up of designated officials from the (i) Directorate of Priority Crime Investigation (DPCI), Financial Intelligence Centre (FIC), National Prosecuting Authority (NPA), South African Police Service (SAPS) Crime Intelligence and Detective Service, South African Revenue Service (SARS), Special Investigating Unit (SIU), State Security Agency (SSA) and National Intelligence Co-ordinating Committee (NICOC).

In addition, the FIC, financial institutions and their supervisory body, the South African Reserve Bank (SARB), have launched the public-private partnership (PPP): the *South African Anti-Money Laundering Integrated Taskforce* (SAMLIT). The SAMLIT platform was used as a basis to establish the Fusion Centre, whereby the priority focus has been on allegations of corruption and procurement fraud linked to COVID-19.

The four pillars of the Fusion Centre are:

1. *Prevention:* engagement with financial institutions for proactive reporting and key government departments vulnerable to fraud and corruption (Auditor General, National Treasury, Public Protector and Department of Labour).
2. *Early Detection:* performing daily media scans and reviewing financial intelligence, public complaints, auditor general reports, SIU proclamations, national treasury reports, and intelligence reports, among others.
3. *Investigation:* The Fusion Centre has previously reported looking at over 200 matters, including over 15 cases in court.
4. *Prosecution and resolution:* a variety of measures are reported due to inter-stakeholder collaboration, including the freezing of bank accounts, recoveries, criminal prosecution and referrals for municipal officials.

In the COVID-19 pandemic context, the SIU received authorisation to investigate allegations of unlawful conduct concerning COVID-19 procurement by all state bodies. The SIU finalised investigations into at least 164 contracts with a total value of ZAR 3.5 billion approximately USD 204 million).

Overall, the Fusion Centre provides a good practice on operational effectiveness by engaging with relevant stakeholders (financial institutions, FIC, SARB) and collaborating with law enforcement authorities to combat financial crime and illicit financial flows.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

### Box 3.7. UK case study – the Fusion Cell and purchase of ventilators by the NHS

In May 2020, the National Crime Agency (NCA) launched an initiative bringing law enforcement and government together with the private sector to detect criminal activity seeking to exploit the COVID-19 pandemic for financial gain.

This Fusion Cell, led by the National Economic Crime Centre (NECC) and co-sponsored by the private sector brings together experts from across sectors, including the financial sector, insurance companies, trade bodies, law enforcement and the broader public sector. The Fusion Cell works to rapidly share information on changes to the economic crime threat related to COVID-19 and to proactively target, prevent and disrupt criminal activity, protecting businesses and the public.

The Fusion Cell works on the existing public-private partnerships that exist in the NECC. It remained as a virtual body during lockdown, convening regularly to discuss the economic crime threat picture related to COVID-19. The Fusion Cell produces a weekly public-private threat dashboard, including high-level suspicious activity report (SARs) trend data, to inform areas for proactive tactical development and disruptive action. Insight from developing the Fusion Cell has the potential to inform a longer- term ambition to develop the capability to spot and stop economic crime before it happens, with real-time insight and disruptive activity through public-private data sharing.

During the COVID-19 pandemic, the Fusion Cell co-ordinated with the National Health Service (NHS) and the banking system on conducting verification and background checks. In a specific case regarding the purchase of ventilators by the NHS in a contract worth GBP 4 million, the NCA conducted background and criminal intelligence checks and requested the NHS to put a hold on the transaction for the purchase of the ventilators. However, the NHS had already disbursed the funds. The NCA then worked with the banking sector to ensure the freezing of the funds.

Source: *Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project, (UNODC, 2020, 40-41) and (NCA, 2020, 5)*

### *Information from tax authorities*

### Guidance 5. Co-operation with Information from tax authorities

**For governments:**

- Include tax authorities in any inter-agency co-operation mechanism to detect, investigate and prosecute corruption-related offences arising from emergencies.
- Discuss, identify and agree on the detection and investigation objectives of tax authorities and law enforcement to fully explore synergies between them.

Tax administrations have an important role to play in combating bribery and corruption. In the course of their activities tax examiners and auditors are in a very strong position to identify indicators of possible bribery and corruption, and the tax administration has a responsibility to exercise its duties and powers to assist other government agencies in fighting these crimes.[19]

Corruption can affect all processes conducted by a state's tax administration (e.g. registration and removal of taxpayers from the national registry, collection of tax dues, identification of tax liabilities, inspection and prosecution of tax offences). Tax authorities have a wealth of information related to payments of taxes, e.g. income tax and value-added tax (VAT). It thus enables law enforcement authorities to cross-reference with other sources of information to assess their accuracy or to identify the possible commission of wrongdoing.

Data collected by or available to tax authorities generally are from a variety of sources, including (Brun et al., 2022, 8) tax registration information and filed tax returns, accounting books and records of legal entities, periodic returns from businesses, custom declarations, exchange of information with foreign governments, including information supplied via automatic, spontaneous or upon-request channels and whistleblower complaints[20] or tax evasion petitions.

Where suspicions of tax fraud arise, tax authorities may initiate a (criminal) tax investigation. Still, evidence of the commission of other criminal offences, such as corruption-related offences, may be detected at this stage. Additionally, the role that the tax administrations play in criminal investigations may vary, depending on the model of the tax administration.[21] Thus, jurisdictions should consider setting up inter-agency co-operation mechanisms[22] with the tax authorities to ensure their timely participation in detecting and investigating corruption-related offences during an emergency.

During an emergency such as the COVID-19 pandemic, many tax authorities took on new roles to assist in providing wider government support. These new roles included financial assistance to citizens and legal entities, and information assistance by sharing information or using its data analytics capabilities (OECD, 2020, 3). In doing so, tax authorities faced several challenges, e.g. fraud risks, data protection issues (OECD, 2020, 3-4).

Perpetrators have sought to defraud financial assistance measures provided during emergencies. Tax authorities should thus consider balancing pre-payment and post-payment compliance measures (OECD, 2020, 6). Tax authorities should consider conducting a risk assessment to determine the risk

---

19 https://read.oecd-ilibrary.org/taxation/bribery-and-corruption-awareness-handbook-for-tax-examiners-and-tax-auditors_9789264205376-en#page11

20 See section *Information from whistleblowers/reporting persons* of these practical guidelines.

21 The OECD has identified four different organisational models based on the extent of the tax administration's involvement in criminal tax investigations (OECD, 2017, 70):

- **Model 1:** the tax administration has the responsibility for directing and conducting criminal tax investigations.
- **Model 2:** the administration has the responsibility for conducting criminal tax investigations under the direction of the public prosecutor.
- **Model 3:** A specialist tax agency, under the supervision of the Ministry of Finance but outside the tax administration, has the responsibility for conducting criminal tax investigations.
- **Model 4:** law enforcement or the public prosecutor has the responsibility for conducting investigations, including into tax crimes.

22 See section Information received through other inter-agency co-operation channels of these practical guidelines and Box 4 Spain case study – inter-agency co-operation through the analytical support units within the special prosecution service against corruption and organised crime.

factors surrounding the added responsibilities arising from the emergency. Risk factors may include (OECD, 2020, 6-7):

- Previous tax non-compliance by the applicant.
- Lack of previous contact with the tax authorities or other government agencies.
- Recent establishment of a business.
- Significant increase in the number of previously reported employees.
- Recent change of details, e.g. address or bank account.
- Old identification documents.
- The use of the same internet protocol (IP) or physical address for multiple applications.

Furthermore, the information on large parts of the population and economy that tax authorities hold can be useful during emergencies (OECD, 2020, 10). Income and revenue information can be used to determine eligibility of benefits or supports offered by governments during emergencies. However, challenges arise when affording such information to law enforcement and other government agencies while maintaining confidentiality and data protection (OECD, 2020, 10). These challenges may be overcome by establishing a proper legal framework that allows for inter-agency co-operation.[23]

### *Information from supreme audit institutions and internal auditors*

#### Guidance 6. Co-operation with information from supreme audit institutions

**For law enforcement authorities:**

- Examine the results of audits of emergency-related funds without delays.
- Hold consultations with SAIs with respect to the features of the allocation and disbursement of emergency funds and respective risks, and the possibilities to initiate audits of certain programmes/projects.

A supreme audit institution (SAI) is an independent body responsible for examining the financial information of a public entity or state-owned enterprise (SOE) to verify its public accounts, assess regulatory compliance and ensure the highest standards of financial integrity (Evans, 2008, 2). SAIs oversee government revenue and expenditures, giving them an important role in deterring and detecting corruption-related offences.

Audits are an indispensable part of a regulatory system aimed at revealing deviations from accepted standards and violations of the principles of legality, efficiency, effectiveness and economy of financial management (INTOSAI, 2019).

According to the INTOSAI Lima Declaration, SAIs should have the power to access all records and documents relating to financial management. Furthermore, they should have the authority to request, orally or in writing, any necessary information (2019). Although SAIs must carry out post-audits, the legislation of each jurisdiction will determine whether the SAI also conducts pre- or real-time audits.

Because emergencies require urgent actions, they can lead to basic control systems being suspended or bypassed, thereby weakening accountability systems and oversight (INTOSAI, 2020, 4) and eroding trust in the management of public funds. Moreover, the disbursement of emergency funds may result

[23] See section Information received through other inter-agency co-operation channels of these practical guidelines.

in a lack of clarity surrounding the role of the SAI in auditing them, further compounding misunderstandings and reduced accountability (INTOSAI, 2020, 4).

During the COVID-19 pandemic, jurisdictions identified several issues concerning public finance management: procurement proceedings not prepared to deal with emergencies,[24] inadequate management or purchase of substandard medical equipment,[25] and duplicate or improper payments.

24 See, e.g. Box 3.10. Chile case study – ChileCompra.

25 See, e.g.

### Box 3.13. Bosnia and Herzegovina (BiH) case study – the ventilators case (2020)

In April 2020, the Civil Protection of the Federation of BiH purchased ventilators aimed at responding to the needs of COVID-19 patients in intensive care units (ICUs). The company which won the tender was neither registered to import medical equipment into BiH nor had experience in the field. The company purchased ventilators from a foreign company through a complex commercial scheme involving numerous intermediaries in five jurisdictions. An associated group, including high-level public officials from BiH, allegedly orchestrated the transaction to obtain unlawful material benefit. They delivered ventilators were not suitable for ICU treatment of COVID-19 patients and were purchased at an inflated price.

An investigative journalist first triggered the case and disclosed the purchasing contract. The State Prosecutor's Office took over the investigation from local prosecutors under high public scrutiny. Investigators gathered evidence, including searching mobile phones and collecting data from telecommunication providers.

One of the first investigative steps taken by the prosecution service was to conduct an expert analysis of the acquired medical ventilators, more specifically regarding their purpose. The expert analysis showed that the acquired medical ventilators were not meant to be used in intensive care units (ICUs) to treat COVID-19 patients. Thus, the equipment purchased did not meet the criteria required under the procurement proceeding.

The investigation concluded that the company was selected regardless of its ability in the field. The licence to trade medical equipment was provided through a faster procedure due to the emergency after being awarded the contract. The head of the Civil Protection of the Federation of BiH allegedly approved the arrangement. Investigators also sought assistance from several jurisdictions.

Two high-level defendants and one involved entrepreneur were convicted by a first instance court and given different prison sentences, while one high-level defendant was acquitted.

***Role of media reporting***

A media report triggered this investigation, with the latter benefiting from media support. Nevertheless, this support raised challenges as prosecutors came under intense public pressure due to the sensitive nature of the COVID-19 pandemic and the publication of the indictment by media outlets. This case highlights the importance of the role of the media in detecting corruption in emergencies while raising the difficulties of undertaking an investigation coupled with the loss of investigative secrecy and the expectations of civil society.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project, https://apnews.com/article/bosnia-corruption-conviction-prison-covid-207e1a96b2bed6632cc715acf37eaef4

.

SAIs can support law enforcement, prosecutors and other government agencies by conducting, e.g. real-time audits of the implementation of government programmes addressing the emergency. These real-time audits may show unanticipated costs, the acquisition of substandard assets, or poorly drafted contracts between the government and legal entities, which may be the indicators of corrupt activity.

Additionally, SAIs are uniquely positioned to assist law enforcement and prosecutors during emergencies by, among others (INTOSAI, 2020, 13-23): alerting about the risks generated by the emergency and the needed safeguards; ensure dialogue on the situation and expectations; consider audits that can add value as the crisis unfolds; ensure timely reports with balanced conclusions.

### Box 3.8. Kazakhstan – co-operation with auditors at the detection stage

In Kazakhstan, special procurement procedures were adopted for the urgent purchasing of IT equipment to ensure remote learning in public schools and other educational institutions. Under these procedures, the contracts should have been awarded to the bidders who were able to organise the speediest supply of the equipment, with the timeline of the supplies used as the main criterion. According to the procedure, regional authorities under the supervision of the Ministry of Education were dealing with the allocation of funds, and the management of respective educational institutions was purchasing the equipment using single-source contracts.

Inspections carried out by the Anti-Corruption Agency in co-operation with state auditors found signs of collusion between the companies awarded the contracts, the regional authorities, and educational institutions. The audit identified many discrepancies and shortcomings in the technical specifications of the required equipment, which allowed unfair selection of the vendors and the purchase of improper quality equipment. As a result of the audit, complemented by criminal intelligence data, 5 cases of embezzlement of public funds were opened.

The case was pending trial at the time of publication.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

### Box 3.9. Costa Rica – co-operation with internal auditors

Based on media reports, the Prosecutor's Office for Integrity launched an investigation into wrongdoings in the purchase of personal protection masks by the Social Security Department. There were allegations of public officials involved in a corruption scheme due to the inflated prices of the purchased masks (the total price of the contracts was above USD 5 mln) from suppliers who had no previous experience in providing goods to the government and did not comply with the national procurement law.

Fruitful co-operation with internal auditors of the Social Security Department, who conducted their own internal investigation, allowed the prosecution service to obtain important evidence, including documents and electronic information. Raids have been completed and the evidence is under analysis.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

## *Public procurement information*

### Guidance 7. Public procurement information

**For governments:**

- Ensure that law enforcement agencies have access to continuous, timely, accurate and verifiable information regarding government expenditures arising from the emergency.

**For law enforcement authorities:**

- Focus their analytical efforts on the examination of emergency-related public procurement procedures.

Public procurement refers to procedures governments and state-owned enterprises (SOEs) use to purchase goods, services and works (OECD, 2022a). Because public procurement accounts for a substantial amount of public funds, it is expected governments carry them out efficiently and with high standards of probity to ensure high service delivery and safeguard the public interest.

Jurisdictions allocate resources programmatically to deal with situations arising from emergencies. This may include allocating extraordinary funds to address the emergency and applying special rules to govern the allocation of such extraordinary funds, thereby ensuring the timely provision of public goods and services, the continuity of critical services such as health care, and the implementation of economic measures to ensure the stability of the jurisdiction (International, 2020, 2).

During the COVID-19 pandemic, public procurement was at the frontline of the response of governments. Such an emergency, however, created a radically new purchasing environment with fierce competition between public buyers for the same vital products and services, severe disruptions in the supply chain, unexpected market responses, price inflation as demand across the globe far exceeded supply, and higher risk for counterfeit products, among others (OECD, 2022c).

Additionally, many jurisdictions granted contracts through direct contracting procedures as part of the exceptions provided under procurement rules for emergencies (OECD, 2021). This approach reduced transparency and accountability in the process of procuring good and services, with limited checks and balances to ensure integrity in service delivery and to safeguard the public interest. As a result, jurisdictions identified several challenges, including:

- Tenders being awarded to suppliers with no technical or operational capacity, often without a respective license from regulators or created just before the start of the respective procurement processes (see Box 3.2).
- Increase in the number of fraudulent bids.
- Awarding of new government contracts where existing ones could have been supplemented.
- Overpricing in bids and challenges in setting reference prices.

Ensuring that resources used for public emergencies are detailed, continuous, timely, accurate and supported by verifiable information allows law enforcement agencies to assess their accuracy or to detect the possible commission of offences. Moreover, such information should be expressed in plain language and published in open data formats, making them accessible to different types of audiences (International, 2020, 2).

The mentioned risks and experiences emphasise the significance of utilising law enforcement's in-house analytical resources to monitor emergency-related procurements. It is also crucial to establish and promote channels for reporting wrongdoings in this area.

### Box 3.10. Chile case study – ChileCompra

ChileCompra is the public procurement agency in Chile created in 2003. It is responsible for administering the electronic platform and the procurement needs of all government agencies. ChileCompra signed a collaboration agreement with the Public Prosecution Office in 2009.

During the COVID-19 pandemic, ChileCompra faced the following main challenges:

- Specificity of the demand generated by the emergency.
- Ability to respond quickly: procurement procedures were not prepared for emergencies such as the COVID-19 pandemic. *Ad hoc* procedures were thus adopted.
- Large amounts of public spending needed to be disbursed in short periods.
- Lack of proper regulation. In Chile, the legislation for emergency procurement was not prepared for an emergency of the magnitude of the COVID-19 pandemic. This resulted in the adoption of ad hoc regulation, which is not the ideal solution.
- Increase of direct (non-competitive) awards.
- Lack of transparency. It was challenging to follow every transaction and to place it in the platform.
- Limited monitoring.

During the COVID-19 pandemic, ChileCompra published two guidelines which contained recommendations. The first guideline sought to reduce the amount of bureaucracy needed for tendering procedures, to lessen the impact on SMEs during the emergency. The second guideline dealt with transparency and measures to ensure the publicity of tendering procedures and its outcomes.

ChileCompra also sought to co-ordinate procurement processes to align them with demand. Thus, ChileCompra would launch a call for tender and another public institution would grant the contract.

Additionally, ChileCompra modified the tendering platform to require the public institutions to indicate if the purchase was related to the COVID-19 pandemic. This enabled ChileCompra to monitor much more closely those transactions.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

### Box 3.11. Brazil case study – Operation Sangria

Operation *Sangria* began in 2020 after the local press published information that a Governor had purchased 28 ventilators from a wine importing company, a contract awarded with an exemption for a public tender. The Brazilian Federal Prosecutor's Office sought to investigate alleged procurement fraud and misappropriation of public funds intended for use to combat the COVID-19 pandemic.

The Brazilian Federal Police began investigating misappropriation of funds related to the purchase of ventilators. Further investigations revealed that a health supplier company with a government contract sold ventilators to the wine company for BRL 2.48 million. The wine cellar, in turn, sold the same ventilators to the government on the same day for BRL 2.976 million, and later transferred the funds received to the health supplier company.

The investigation also revealed a conspiracy between public officials and the owners of both the health supplier and wine import companies to defraud the government. The investigation also showed that a high-ranking official allegedly directly influenced the decisions taken by the health authorities.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

## *Asset disclosure information*

### Guidance 8. Asset disclosure

**For governments:**

- Prioritise the verification of asset declarations of public officials who work in the risk areas dealing with mitigating the consequences of the emergency.
- Seek technological solutions to receive and process asset disclosures from public officials to limit face-to-face interactions.

The main aims of asset disclosure regimes may include (OECD, 2011a, 12):

- Increasing transparency and the trust of citizens in public administration.
- Helping heads of public institutions prevent conflicts of interest among public officials.
- Monitoring wealth variations of individual public officials.

Apart from serving as a preventive measure, the disclosure of assets by public officials is also an important detection tool as it may uncover unexplained assets that may have been acquired through corrupt or illegal means. To effectively utilise asset declarations for detection purposes, it is essential to establish a strong verification system and foster collaboration between the verifying agency and law enforcement.

There is no uniform standard regarding which public officials should be obligated to submit asset disclosures. Jurisdictions should consider and balance between a broader system, which is more burdensome and costly, or a narrower system (OECD, 2011a, 14). Moreover, the scope of information disclosed depends on the purpose of the asset disclosure system. Conflict of interest control requires information about interests that have the potential to influence the discharge of official duties, rather than an all-encompassing picture of all assets, businesses and activities of a public official (OECD, 2011a, 14).

During emergencies, challenges may arise concerning the timeliness of the submission of asset disclosures by public officials. The issue arises due to movement restrictions or limited workforce available to receive the asset disclosures. To mitigate these issues, consideration should be given to enable public officials to file their asset disclosures electronically, reducing the need for face-to-face contact and better streamlining the process.

There are four main reasons for moving to electronic filing (Kotlyar and Pop, 2019, 4-5):

1. *Convenience for declarants.* Electronic filing simplifies and streamlines the process of submitting asset declarations. It further guides the declarant to enter correct data through automated processes, thereby minimising errors.
2. *Better data management and increased security*. Managing paper-based asset disclosures can be resource and time intensive. They require collection, organisation and secure storing. On the other hand, electronic filing enables uploading and saving the declarations in a central data repository, thereby preventing the loss of data. They thus ensure higher quality of data and guarantee data integrity.
3. *More effective review and enforcement*. Working with accurate and complete data reduces the time needed to review asset declarations. It allows for easier identification and retrieval of information from asset declarations and facilitates comparison between filed asset declarations.
4. *Increased transparency and public accountability*. Electronic filings allow for increased public transparency and accountability, as it enables civil society, the media and other members of the public to scrutinise the information submitted by the declarants. Furthermore, electronic filings make it easier to manage different access regimes to the information contained in the declarations.

## Information from investigative journalists, media and social media platforms

### Guidance 9. Information from investigative journalists, media and social media platforms

**For law enforcement authorities:**

- Take steps to proactively monitor the media and use it as a source of detecting corruption.
- Take steps to enhance co-operation with the media for the purposes of receiving timely information on alleged corruption and proper follow-up.

### *Media reporting and investigative journalism*

Media reporting and investigative journalism are among the most important sources of public awareness-raising on corruption (OECD, 2017, 57).The media's role in exposing corruption is vital as they offer information that may initiate a criminal investigation by law enforcement agencies, prompt inspections or audits by other governmental authorities, or urge companies to conduct their internal investigations. Additionally, anti-money laundering reporting entities are encouraged to make suspicious transaction reports (STRs) based on the media's findings.

Media and investigative journalists face many challenges during emergencies. During COVID-19, the media and investigative journalists encountered two primary issues: (i) finding space in the media to discuss corruption when the emergency was the primary focus, in terms of both resources and attention, and (ii) having to turn to technology to cultivate human sources, when this is typically done in person.

Building relationships of mutual assistance and trust between (investigative) journalists and law enforcement can have several benefits. Unlike law enforcement, (investigative) journalists can cross national borders to collect information more swiftly (OCCRP, 2020). Also, the media can be a powerful tool to effect political change and raise awareness, especially when combating corruption and funding law enforcement agencies are not the priority of governments. Furthermore, certain whistleblowers may opt to share information with investigative journalists instead of filing a report with the authorities to not get exposed or due to other varying factors.

At the same time, both (investigative) journalists and law enforcement should understand the inherent tension in their collaboration. These include, e.g. preserving the source of information provided to (investigative) journalists. Thus, some (investigative) journalists believe they should not share any information with law enforcement or government officials beyond what they can make public. Others, in turn, believe in closer co-operation between trusted media and competent law enforcement agencies. Ultimately, this tension is healthy and should be maintained not to undermine the public trust in either party.

### Box 3.12. OCCRP and investigative journalism

During the OECD capacity building activities, the representative of the Organised Crime and Corruption Reporting Project (OCCRP) highlighted the role investigative journalists have in investigating whistleblower leaks without exposing the whistleblowers. To do so, investigative journalism builds their investigation using other (publicly) available sources, so that the whistleblower is not on the frontline, and proving the veracity of the allegations is not reliant on the whistleblower.

The sources of information an investigative journalist may use to prove the veracity of allegations range from information available in the public domain, e.g. records on land, mining, customs, trade, tax, court, non-profit, corporate and shareholder, valuation of assets, vehicles (aviation, maritime, land, import/export data. An investigative journalist may also use satellite imagery to verify maritime information, e.g. showing the movement of vessels, cargo, and land routes used by trucks.

These sources of information seek to corroborate the information provided by the whistleblower and contextualise the complex structures used by perpetrators of corruption and organised crime to launder funds and engage in their unlawful activity.

Another representative of the OCCRP highlighted that investigative journalists are not confined to national borders. Further, corruption-related and organised crime cases bear many similarities. Thus, the OCCRP seeks to investigate the underlying infrastructures used by perpetrators. They do this through open-source intelligence and direct observation.

The OCCRP is also enhancing its efficiency by implementing technology in their work. The expertise gained by its investigative journalists is also shared through capacity building and awareness raising with law enforcement and compliance department of financial institutions.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

### Box 3.13. Bosnia and Herzegovina (BiH) case study – the ventilators case (2020)

In April 2020, the Civil Protection of the Federation of BiH purchased ventilators aimed at responding to the needs of COVID-19 patients in intensive care units (ICUs). The company which won the tender was neither registered to import medical equipment into BiH nor had experience in the field. The company purchased ventilators from a foreign company through a complex commercial scheme involving numerous intermediaries in five jurisdictions. An associated group, including high-level public officials from BiH, allegedly orchestrated the transaction to obtain unlawful material benefit. They delivered ventilators were not suitable for ICU treatment of COVID-19 patients and were purchased at an inflated price.

An investigative journalist first triggered the case and disclosed the purchasing contract. The State Prosecutor's Office took over the investigation from local prosecutors under high public scrutiny. Investigators gathered evidence, including searching mobile phones and collecting data from telecommunication providers.

One of the first investigative steps taken by the prosecution service was to conduct an expert analysis of the acquired medical ventilators, more specifically regarding their purpose. The expert analysis showed that the acquired medical ventilators were not meant to be used in intensive care units (ICUs) to treat COVID-19 patients. Thus, the equipment purchased did not meet the criteria required under the procurement proceeding.

The investigation concluded that the company was selected regardless of its ability in the field. The licence to trade medical equipment was provided through a faster procedure due to the emergency after being awarded the contract. The head of the Civil Protection of the Federation of BiH allegedly approved the arrangement. Investigators also sought assistance from several jurisdictions.

Two high-level defendants and one involved entrepreneur were convicted by a first instance court and given different prison sentences, while one high-level defendant was acquitted.

***Role of media reporting***

A media report triggered this investigation, with the latter benefiting from media support. Nevertheless, this support raised challenges as prosecutors came under intense public pressure due to the sensitive nature of the COVID-19 pandemic and the publication of the indictment by media outlets. This case highlights the importance of the role of the media in detecting corruption in emergencies while raising the difficulties of undertaking an investigation coupled with the loss of investigative secrecy and the expectations of civil society.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project, https://apnews.com/article/bosnia-corruption-conviction-prison-covid-207e1a96b2bed6632cc715acf37eaef4

## Information from whistleblowers/reporting persons

### Guidance 10. Information from whistleblowers/reporting persons

**For governments:**

- Raise awareness about the existing whistleblowing and reporting mechanisms afforded by law enforcement authorities and other relevant agencies to help detect corruption-related offence.
- Update legislation to ensure it envisages adequate protection to public and private sector whistleblowers/reporting persons.
- Develop technologies that allow the public to submit complaints in anonymised, electronic channels that can be collected and analysed by law enforcement.

**For law enforcement authorities:**

- Establish reporting channels enabling the public to make complaints or report suspected corruption- allegations related to the emergency.

**For private sector actors:**

- Raise awareness among private sector employees on the complaint, reporting and whistleblowing mechanisms available to them to report suspicions of corruption.

There is no internationally accepted definition of a *whistleblower/reporting person* (OECD, 2017, 30).[26] The term encompasses (OECD, 2017, 30): (i) any person who reports suspicion of bribery to law enforcement authorities,[27] (ii) an employee who reports internally to a legal entity,[28] or (iii) a third person who reports to law enforcement or the media.

Whistleblower reporting is an important source of detection of corruption (OECD, 2017, 29). Whistleblowers/reporting persons foster transparency, promote integrity and detect misconduct. However, effective whistleblower reporting also requires effective whistleblower protection mechanisms. Reporting persons are the ultimate line of defence for safeguarding the public interest (OECD, 2016, 11).

Recommendation XXII(ii) of the 2021 Revised Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions (2021 OECD Anti-Bribery Recommendation) recommends that jurisdictions (OECD, 2022b, 14-15):

> *"[A]fford protection to the broadest possible range of reporting persons in a work-related context, including as appropriate to those whose work-based relationship has ended, to persons who acquire information on suspected acts of foreign bribery during advanced stages of the recruitment process or the contractual negotiations, and who could suffer retaliation, for instance in the form of negative employment references or blacklisting, and consider extending protection to third persons connected to the reporting person who could suffer retaliation in a work-related context."*

26 The 2021 OECD Anti-Bribery Recommendation uses the term *reporting person* (OECD, 2017, 30). Notwithstanding, these practical guidelines will use the more commonly known term, *whistleblower*.

27 See section Information from whistleblowers/reporting persons of these practical guidelines.

28 See section Self-Reporting of these practical guidelines concerning internal investigations in the context of self-disclosure.

The main challenge faced by jurisdictions relates to insufficient or inadequate measures enabling whistleblower protection (Resimić, 2021, 2). This, in turn, impacts a legal person's ability to apply internal processes to detect and initiate internal investigations into the alleged wrongdoing effectively.

### Box 3.14. Honduras case study – mobile hospitals case

The Honduran authorities detected this case via complaints from COVID-19 patients, civil society and a medical association working at the mobile hospitals. Honduras purchased seven mobile hospitals and seven waste treatment plants between March and April 2020.

The investigation showed that the two public officials responsible for the procurement to purchase the mobile hospitals and waste treatment plants colluded with the legal representative of the winning bidder, a private company that did not have the technical capacity to build, produce and equip the procured mobile hospitals and waste treatment plants.

The investigation additionally showed that, although the importation value of the mobile hospitals and waste treatment plants was approx. 17.6 million, the private company charged the public institution approx. USD 47.5 million.

The investigation relied on inspecting the procured goods, seizing documents relevant to it and the use of special investigative techniques,[29] i.e. wiretapping. Law enforcement also collected witness statements, conducted financial profiling and investigations, and sought international co-operation[30] to seize USD 4.1 million in bank accounts abroad.

In June 2022, the public officials were found guilty of aggravated fraud and violation of the duties of public officials. They received prison sentences, debarment from becoming public officials and fined to pay the amount defrauded, approx. USD 47.4 million.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

29 See section Special investigative techniques of these practical guidelines.

30 See section Freezing, seizure and confiscation and Chapter 5 of these practical guidelines.

### Box 3.15. Romania case study – corruption scheme detected through a whistleblower report

A state-owned enterprise (SOE), whose sole shareholder is the Ministry of Health, sought to purchase surgical masks from a supplier. In the course of this process, an intermediary met with the SOE's manager regarding the sale of the surgical masks. Although the offered price was not inflated, the intermediary requested EUR 1.2 million in exchange for their influence in obtaining the contract.

Subsequently, it was discovered that the intermediary and the owner of the supplier company were business partners in another company. Further, the supplier company had no experience in the medical industry.

The manager of the SOE called the supplier company and solicited a bribe of EUR 760 000 for the purchase of surgical masks and PPE. The supplier company proceeded to purchase the surgical masks and PPE and, before its receipt by the SOE, 60% of the supplier company was sold to a third person.

The third person proceeded to report the matter to law enforcement when they discovered that their business partner in the supplier company had agreed to pay a bribe of EUR 1.2 million to obtain the contract with the SOE. This whistleblower co-operated and helped uncover that the intermediary paid EUR 760 000 to the manager of the SOE.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

Upon identifying wrongdoing, employees in the public or private sectors may be uncertain of what to do with the information. They may not know where or to whom to turn or whether they are protected by whistleblower protection mechanisms (OECD, 2016, 12). An effective whistleblower protection mechanism requires clear and effective communication by informing both employers and employees of their rights and responsibilities. A challenge remains, however, where the same whistleblower reports the facts to multiple law enforcement or government agencies, putting an additional strain on their resources when processing reports.

### Box 3.16. Australia case study – a new framework for whistleblower protection in the private sector

A new amendment, which took effect in January 2020, has been issued to ensure greater protections for whistleblowers and to expand the type of person that can claim this status (e.g. one need no longer work for the company or report the misconduct to the company in question to receive protection). The new legislation also sets out obligations for companies to implement protected reporting frameworks, and sanctions for those who retaliate against whistleblowers. The changes in legislation have led to a dramatic increase in the number of reports being made to the designated authority – the Australian Securities and Investments Commission (ASIC) – which developed a ranking guide to determine the severity of complaints to ensure those complaints are addressed quickly.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

Moreover, during emergencies such as the COVID-19 pandemic, jurisdictions face additional challenges, including being unable to:

(i) Offer adequate protection to whistleblowers/reporting persons against retaliation. The lack of adequate protection ranges from inadequate legislation on whistleblower protection, to

lack of resources to effectively implement whistleblower protection – even when legislation is in place. In turn, these elements generate reluctance for whistleblowers to report to law enforcement authorities due to the lack of effective legal protections.

(ii) Receive complaints and allegations of irregularities from the public due to lockdowns and movement restrictions.

Many jurisdictions addressed the issue by developing specific complaint channels using specialised technology, enabling them to mitigate the challenges imposed by lockdowns and movement restrictions. This in turn reduced and even eliminated the need for direct person-to-person interface while ensuring the confidentiality of the information and identification of the reporting person.

### Box 3.17. Nigeria case study – Eagle Eye application

Seeking to complement the existing channels for reporting corruption-related offences and other economic crimes, the Economic and Financial Crimes Commission (EFCC) of Nigeria launched in 2021 the application Eagle Eye, designed to ease the process of reporting economic and financial crimes in Nigeria.

The application eliminates a direct person-to-person interface in the reporting process and guarantees anonymity, an added incentive to effective whistleblowing. With the application, reporting persons can report cases from any part of the world with full assurance of secrecy and anonymity. The Eagle Eye application can be downloaded to a mobile device, allowing the reporting persons to follow up on a complaint.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

### Box 3.18. South Africa case study – investigations into stimulus and relief funds

The FIC reported that through the operational capacity of the Fusion Centre, the task team acted promptly on a matter related to fraudulent claims and theft of funds associated with the Unemployment Insurance Fund (UIF). During the COVID-19 pandemic, the UIF provided funds to furloughed workers. The task team investigated and secured the proceeds of crime, including arresting the involved perpetrators.

The quick response of the task team also led to the freezing of 28 bank accounts, the identification of the criminal actors and the recovery of just over ZAR 2 million (approx. USD 116 thousand) and assets purchased with the proceeds of crime of ZAR 5.7 million (approx. USD 332 thousand).

In another case, the UIF examined payments of ZAR 111.9 million (approx. USD 6.52 million) to a company that had claimed Temporary Employer/Employee Relief Scheme (TERS) Funds. Subsequent to inquiries by the UIF, the bank decided to block the funds.

When the suspect realised that he could not access the money, he called an official of the UIF and requested the unblocking of the funds. The suspect offered the official a bribe of ZAR 10 thousand (approx. USD 586) and promised the official a further ZAR 500 thousand (approx. USD 29.2 thousand) upon access to the money in the account of the accused's company.

A sting operation led to the arrest of the accused. The accused is facing charges of corruption, fraud and money laundering and the matter has been remanded to a future date for further investigation. The Asset Forfeiture Unit (AFU), using the financial intelligence supplied by the SAMLIT, obtained a preservation order for ZAR 111.1 million (approx. 6.48 million).

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

## Information from the private sector

### Guidance 11. Information from the private sector actions

**For private sector actors:**

- Update their internal controls regarding the direction and supervision of auditing teams.
- Conduct self-assessment and anti-corruption compliance audits to minimise corruption-related risks in their supply chain and day-to-day business.

The private sector plays an important role in the detection of corruption-related offences. Companies and professional advisors are in a unique position to assist law enforcement and prosecutors to detect corruption-related offences.

### *Information from accountants and auditors*

Accountants and auditors are in a position to provide reasonable assurances that the books and records of their clients or employers accurately reflect the commercial reality of a legal person (OECD, 2017, 148).

Art. 8 of the OECD Anti-Bribery Convention requires its member countries to adopt accounting standards prohibiting the (i) establishment of off-the-books accounts, (ii) making of off-the-books or inadequately identified transactions, (iii) recording of non-existent expenditures, (iv) entry of liabilities with incorrect identification of their objects, and (v) use of false documents (Pieth et al., 2014, 455). This article is further complemented by the 2021 OECD Anti-Bribery Recommendations. Recommendation XXIII(A)(i) and (iii) requires legal persons to disclose in their financial statements the full range of material contingent liabilities and prohibits, among others, off-the-books accounts, the recording of non-existent expenditures and use of false documents (OECD, 2022b, 14-15). In turn, Recommendation XXIII(B)(i) requires the submission of accounts to an external audit (OECD, 2022b, 15).31

The South African Independent Regulatory Board for Auditors (IRBA), with the International Ethics Standards Board for Accountants (IESBA) and the International Auditing and Assurance Standards Board (IAASB) released a publication highlighting the heightened risks of fraud arising from the COVID-19 pandemic (IESBA et al., 2020). It acknowledges that the COVID-19 pandemic carries unique challenges, included more opportunity for fraud and corruption. These, in turn, may lead to risks of material misstatement of financial statements.

During emergencies, auditors should continue to comply with the required standards. These may necessitate different and enhanced considerations by auditors, including developing alternative procedures to gather sufficient appropriate audit evidence to support their audit opinion, or to modify it. This may include using new technology resources.

Because an emergency may change how and where auditors undertake their work, legal entities should consider updating their quality control policies and procedures regarding the direction and supervision of auditing teams.

Additionally, auditors should identify and assess risks of material misstatement (ISA 315) to consider the impact of the emergency on the planned audit approach or revise risks arising from the emergency. When responding to the assessed risks from the emergency (ISA 330), auditors should seek alternative procedures, and provide greater focus on the financial statement closing process, the auditor's evaluation of the overall presentation of the financial statements (including whether adequate disclosures have been made), and the auditor's conclusion on whether sufficient appropriate audit evidence has been obtained. The findings made by the auditor should be made available, where applicable, to law enforcement authorities, in line with Recommendation XXIII(B)(v) of the 2021 OECD Anti-Bribery Recommendation.

### *Self-reporting*

Self-reporting involves a company informing authorities of something of which they were unaware, with the legal entity either accepting wrongdoing or indicating that it may accept wrongdoing (depending on the stage of the investigation) (OECD, 2017, 13).

Incentivising self-reporting requires jurisdictions to have in place several elements:

(i) Development of clear and transparent criteria regarding voluntary self-reporting of misconduct, co-operation with law enforcement with law enforcement authorities and remediation measures (Recommendation XVIII(ii) of the 2021 OECD Anti-Bribery Recommendations).

31 See section Information from supreme audit institutions and internal auditoris of these practical guidelines regarding the role of SAIs.

(ii) Provision of clear and publicly accessible information on the advantages that an alleged offender may obtain when self-disclosing.

Such incentives may include allowing for non-trial resolutions (NTRs) for legal entities which fully co-operate with law enforcement in a timely manner, and appropriately remediates deficiencies (OECD, 2019). Thus, self-reporting and whistleblowing[32] are increasingly considered to be fundamental to and indicative of the culture of an organisation (Seddon and Ivanovs, 2022, 46). Timely voluntary self-disclosures can be among the signs that a company is effectively addressing misconduct and prioritizing compliance.

In emergencies, legal entities must adapt to meet the new challenges they face regarding corruption. Due diligence through in-person interviews of relevant parties, e.g. customs brokers, transport management officials, may not be viable. Instead, legal entities may wish to consider applying self-assessments internally and to its vendors to identify risk and provide data to evidence compliance with corporate policies, procedures and initiatives (Fratto et al., 2020).

Legal entities should also consider conducting anti-corruption compliance audits to help uncover and remediate issues and risks. During these audits, legal entities should review financial information to ensure that expenditures for government-related services are appropriate and accurately recorded in the books and records of the legal entity (Fratto et al., 2020). Moreover, because of the heightened risks during an emergency, legal persons should also consider maintaining adequate resources to their compliance departments.

## Integrity testing as a detection technique

### Guidance 12. Integrity testing

**For governments:**

- Consider implementing targeted integrity testing for public officials who work in the risk areas dealing with mitigating the consequences of the emergency.

Integrity testing discourages malpractice and corruption (DCAF, 2020, 5). It simulates corruption opportunities to detect corrupt behaviour or corruptible public officials. During an integrity test, a public official unaware that a test is being carried out is placed in a monitored situation that offers an opportunity for unethical or unlawful behaviour. Integrity tests aim to replicate the everyday challenges and pressures encountered by public officials in which opportunities for misconduct are prevalent (DCAF, 2020, 5).

Integrity testing seeks to (Hoppe, 2016, 6): (i) encourage officials to follow their obligation to report bribery, (ii) increase the perceived risk of detection and thus prevent corruption, (iii) identify public officials prone to corrupt practices, (iv) collect evidence for disciplinary proceedings, (v) identify public officials who are honest and trustworthy and (vi) identify the training needs of public officials.

However, integrity testing is an intrusive detection technique involving undercover agents who create situations where a public official may commit a criminal act, i.e. a corruption-related offence. The undercover agent must not violate the provisions of fair trial and must not become an *agent provocateur* i.e. being the only source of the *mens rea* of the targeted public official. The European Court of Human

[32] See section Information from whistleblowers/reporting persons and Self-reporting of these practical guidelines.

Rights (EctHR) has extensive case law on the matter, helping law enforcement to understand the limits imposed on illicit provocation of criminal conduct by the authorities.[33]

During an emergency, integrity testing can provide useful information regarding the commission of corruption or its ancillary offences. During the COVID-19 pandemic, the use of integrity testing in risk-prone areas, e.g. health care and procurement officials, could encourage those public officials to continue to engage in both an ethical and lawful manner.

However, testing units or public officials may have their movements restricted during an emergency, limiting the feasibility and effectiveness of integrity testing. The availability may also be restricted due to limited judicial availability, resulting in insufficient checks and balances for conducting integrity testing.

[33] (See: ECtHR, 1998, para. 38; ECtHR, 2008, para. 67; ECtHR, 2010 para. 47-48; ECtHR, 2014, para. 52-53)

# 4 Investigation and prosecution

Investigating and prosecuting corruption offences is one of the most difficult challenges law enforcement and prosecutorial authorities face, due to the inherent attributes of corruption offences like the collusion of the involved parties and the scarcity of objective and direct evidence. During emergencies these challenges become even more serious as additional operational or technical obstacles arise. Emergencies typically cause delays in executing procedural tasks thus the timeliness of investigations deteriorates, resulting in a potential loss of evidence, lapsing of procedural deadlines or even the statute of limitations.

These issues are further compounded when, e.g. courts may not be readily available to consider *ex parte* requests made during an investigation or review positions made by the defence, thereby holding law enforcement accountable and ensuring due process. In addition, investigations involving corruption-related offences often require law enforcement to sift through large volumes of material and data which might not be feasible in an emergency. Adding to these difficulties are, among others, defence strategies that challenge each and every action taken during an investigation and prosecution.

An investigation is normally opened by law enforcement or a prosecutor when the simple suspicion of an offence emerges, e.g. (i) they receive a complaint or a report made by a government agency, (ii) statements or reports of perpetrators detained *in flagrante delicto*, (iii) confession made by the perpetrator, (iv) information published by the media; and (v) elements of crime detected by law enforcement or the prosecutor. Each of these situations might be hindered by emergency-related causes, thus limiting the appropriate reaction of the law enforcement authorities.

This chapter of the practical guidelines presents several mechanisms available to law enforcement and prosecutorial authorities when investigating and prosecuting corruption-related offences during an emergency. They include elements of data gathering and managing case files during an emergency. The chapter also discusses the different (special) investigative techniques used to obtain evidence on individuals and facts during emergencies. Finally, it presents different mechanisms to conclude an investigation or prosecution, and considerations regarding safeguarding proceeds and instrumentalities of crime.

## Open-source intelligence and data collection

### Guidance 13. Open-source intelligence and data collection

**For law enforcement authorities:**

- Establish specific methods and guidelines applied to OSINT and data collection by defining their purpose for the investigation and establishing the sources, identifiers and datasets that will be used during an emergency.
- Validate and verify the information obtained through OSINT and data collection by collecting them from different sources, where possible.
- Avoid selection bias of the information collected through OSINT and data collection by having it verified by more than one person.
- Take steps to ensure that the information collected through OSINT and data collection is retraceable.
- Minimise the digital footprint of law enforcement personnel, especially those tasked with OSINT investigations.

Open-source intelligence (OSINT) and data collection from non-public databases available to law enforcement authorities remains relevant beyond the detection of an offence as they can lead to discovery of additional evidence, contribute to the verification and assessment of the proving as a whole. OSINT is a methodology for collecting, analysing and making decisions about publicly available data. It is intelligence produced from publicly available sources that are collected, exploited and disseminated promptly to an appropriate audience to address a specific intelligence requirement (Intelligence, 2011, 54-55).[34]

OSINT is not the mass collection of data. It is the targeted collection of specific data and the application of processes to further refine the search to focus only on the relevant information. It can consist of, e.g. research, technical data, economic reports, white papers, conference documentation, mass media, public data, and annual reports. However, the challenge with OSINT relates to the source and reliability of the information, given the issues related to information overload, selection bias, inaccurate or sensationalised information, and the unmediated nature of the data.

To effectively use OSINT and data collecting, law enforcement requires specific methods for information management, including collection, storage, validation, analysis and dissemination:

- *Define* the purpose, aim and scope of the OSINT and data gathering.
- *Identify* the sources which will be used, e.g. the internet, newspaper and magazines, and public or private databases.
- *Harvest* the data using different tools and techniques to gather the data from the target sources.
- *Process and verify* the data to verify uncertain data from more than one source where possible. Additionally, identify current or outdated data and exclude irrelevant data from further analysis.
- *Analyse* the data to find connections to formulate a complete picture of the target.

[34] These practical guidelines understand *data collection* as the gathering of raw information that will be used by analysts to prepare intelligence reports and products. In the data collection phase of the intelligence cycle, one systematically searches public and non-public data using the known identifiers and link the findings to produce results (Carter, 2009, 62; Böhm and Lolagar, 2021, 323).

- *Deliver the results* by presenting the findings in a report that can be used for effective law enforcement action by, e.g. potentially covering corruption-related offences, criminal networks and associates, and legitimate and unexplained assets.
- *Disseminate the results* to other government agencies for further action, e.g. tax authorities, customs and immigration agencies, and anti-money laundering authorities.

OSINT and data gathering is particularly well adapted to assist law enforcement in their investigations during emergencies since its collection can be undertaken remotely, using new technologies and various online platforms and encryption software.

When detecting, investigating and prosecuting corruption-related offences, there are several public and private databases which can be accessed by law enforcement. They can assist law enforcement in establishing e.g. (beneficial) ownership of legal entities,[35] ownership of real estate and land property, screening for national and foreign politically exposed persons (PEPs), etc. Additionally, many jurisdictions maintain public databases for public procurement processes. Ultimately, OSINT and data gathering helps investigators target the information they are after more effectively and protect classified sources by substituting them with publicly available ones.

Social media platforms are fertile ground for information collection and analysis. They can provide a wealth of information concerning the habits and activities of a person, allowing law enforcement agencies to build a profile regarding, e.g. assets (based on photos available on the social media platform), travel (checking-in through the social media account, photos taken during vacation), and relationships, etc.

The ability of law enforcement to obtain or use certain information in social media may be influenced by social media companies' policies and the rules of criminal procedure (CRS, 2022, 3). Some content is available to a broad audience without restriction, although users have some control over the intended audience with whom they share content. Other content contains access boundaries (CRS, 2022, 3). In addition to what is allowable or required by law, social media platforms establish internal policies. They may vary from platform to platform and may change over time, regarding information sharing with law enforcement (CRS, 2022, 5).

Conducting OSINT investigations, however, also carries security risks. The main risk is law enforcement exposing their identity or accidentally informing an individual that they are under investigation by leaving a digital footprint.[36] This may lead to perpetrators obtaining the personal information of law enforcement personnel, their families or co-workers for their use with malicious intent (GAC and CICC, 2016, 3). Exposure is especially problematic in investigations where the ability to map and track the activity of the alleged perpetrators over extended periods of time relies on anonymity. Accidentally tipping off the target(s) of an OSINT investigation may compromise an investigation as well as jeopardise the anonymity of the law enforcement personnel.

Law enforcement should use secure systems and effective means to identify cyber threats stemming from OSINT activities. Additionally, law enforcement personnel should take steps to remove their personal information available online by following opt-out procedures related to personal information. It is a continuous process whereby law enforcement personnel routinely and periodically track their digital footprint and review the amount of information available on themselves and their families online (GAC and CICC, 2016, 6).

---

35 See additionally section Identifying subjects: natural and legal persons of these practical guidelines.

36 The term *digital footprint* refers to the (personal) data that is left behind whenever a person uses a digital service, or whenever someone posts information about another person onto a digital forum, e.g. a social network (CPNI, 2016, 3).

## Electronic evidence

### Guidance 14. Electronic evidence

**For law enforcement authorities:**

- Enter into or reviewing existing MOUs with OSPs to address the challenges and identified risks during an emergency to ensure the retention of electronic evidence.

*Electronic evidence* means any evidence derived from data contained in or produced by any device, the functioning of which depends on a software programme or data stored on or transmitted over a computer system or network (CoE, 2019, 6).

During the COVID-19 pandemic, the restriction of the movement of persons resulted in an increase of using electronic means to conduct day-to-day activities, e.g. remote working, internet shopping and remote communication methods. The convenience of electronic interconnectivity through the internet facilitated the imposition of such restrictions and allowed persons to continue interacting and economies to remain functional.

However, the COVID-19 pandemic brought additional risks associated with the commission of offences through electronic means. The reduction of workforce at law enforcement and online service providers (OSPs) in turn required both to adapt existing processes. OSPs indicated that the restrictions associated with the pandemic led to temporary backlogs in processing requests for electronic evidence and required changes and flexibility in existing procedures, while having a large impact over staff (EUROPOL, 2021, 6-7).

The first challenge faced by law enforcement relates to loss of data (Europol and Eurojust, 2019, 5). To gather information and evidence, law enforcement requires primarily the ability of OSPs to retain data so that evidence can be secured. While jurisdictions may have legislation in place requiring OSPs and electronic service providers (ESPs) to retain data for a certain period of time, they depend on policies established by these private parties to retain the relevant data. To mitigate these issues, the European Convention on Cybercrime (CoE, 2001a) allows for a quick retention mechanism that ensures that the data is retained pending the submission of a request for MLA. The European Convention on Cybercrime has been ratified by more than 65 jurisdictions from all around the world, including e.g. the USA, Canada, Japan, Australia, Brazil, Israel, Nigeria.

Compounding to this challenge is the exhaustion of IP addresses under Internet Protocol version 4 (Ipv4). Internet service providers (ISPs) have consequently implemented carrier grade network address translation (CGN) technologies, which has led to a serious online capability gap in law enforcement to investigate (Europol and Eurojust, 2019, 6).

ISPs use CGN technologies to share one single public Ipv4 address among multiple end-users at the same time (Europol and Eurojust, 2019, 6). Thus, law enforcement needs to provide ISPs with the Ipv4 address, the precise time of the connection and the source port number (Europol and Eurojust, 2019, 10) to be able to technically identify an end-user behind a CGN based on a public Ipv4. Without a source port number, ISPs are unable to differentiate between end-users connected to the same ESP with the same shared Ipv4 at a given point in time.

The second challenge relates to encryption. An increasing number of investigations involve the use of some form of encryption to hide relevant data and communications content. Moreover, a number of ESPs implement encryption by default in their services. As a result, existing investigative techniques, e.g. interception of communication are becoming less effective or even technically impossible (Europol and Eurojust, 2019, 10).

The third challenge concerns the loss of location. The growing use of cloud-based storage and services means that parts of the data stored in the cloud may be physically located in different jurisdictions (Europol and Eurojust, 2019, 13). Thus, law enforcement may no longer be able to reasonably establish the physical location of the perpetrator, the alleged criminal infrastructure or the electronic evidence based solely on the physical location of the data. Additionally, the country with jurisdiction to investigate or prosecute may be unclear, as well as the legal framework that regulates the collection of evidence or use of special investigation techniques.[37]

Apart from the technical issues, law enforcement is additionally faced with a host of operational challenges when dealing with electronic evidence. Generally, law enforcement and judicial authorities rely on voluntary co-operation between them and OSPs, or on international co-operation mechanisms, e.g. mutual legal assistance (MLA) to request the disclosure of user data in the context of criminal investigations.

## Special investigative techniques

### Guidance 15. Special investigative techniques (SITs)

**For law enforcement authorities:**

- Conduct assessment pertaining to their SITs, to ensure their relevance regarding priority investigations while balancing it with the safety of law enforcement staff during emergencies and adjusting the SIT practice accordingly.
- Establish access to and receive information from newly created emergency-related databases for proper SIT planning.

There is no internationally agreed definition of what constitutes special investigative techniques (SITs) (Nilsson, 2005, 40). They refer to techniques applied by law enforcement in criminal investigations to detect and investigate serious crimes and suspects. Their application aims at gathering information, intelligence or evidence that does not alert the target persons (CoE, 2005). SITs include controlled deliveries, surveillance, interception of telecommunication, access to computer systems, and undercover operations.

SITs are very powerful and indispensable tools in corruption-related investigations. Through them law enforcement authorities are able to locate and verify already existing evidence, can follow, observe and document the commission of a still ongoing offence real time, resulting in very strong proving. However, given their intrusive nature and the fact that they necessarily limit certain fundamental rights of the alleged perpetrators and third persons involved, SITs must be provided in law defining the conditions under which law enforcement can use them. They must have strict oversight by the relevant judicial authority, i.e. prosecutor or judge, or both to ensure legality and proportionality. They must also be limited in time, and reasonable grounds for undertaking such SITs must exist. Observation of all these elements is crucial to ensure the admissibility of evidence obtained through or by the application of SITs.

During emergencies, law enforcement and prosecutors may be restricted or limited in applying SITs during their investigations. This may relate to limited or delayed access to the relevant judicial authority to apply for and obtain the necessary authorisation, since some jurisdictions may not allow for electronic filing or virtual hearings. It may also relate to limited staffing, obstacles to conduct in-person meetings,

37 See section Special investigative techniques of these practical guidelines.

or other, e.g. technical capacity bottlenecks. Additionally, the safety and health of law enforcement operating in covert operations, e.g. infiltration, should be considered. Finally, the prioritisation of cases may determine whether to restrict or halt the application of SITs for non-essential or non-priority investigations.

### Box 4.1. Romania case study – impact of the COVID-19 pandemic in the use of SITs

Romania imposed a lockdown due to the COVID-19 pandemic in March 2020, for a period of 60 days, followed by a state of emergency. As a result, the lockdown and state of emergency impacted the ability of law enforcement and prosecutorial authorities to conduct their investigations.

Many investigations initiated prior to the COVID-19 pandemic had to be suspended. Due to social distancing rules, law enforcement and prosecutorial authorities encountered that the public was reluctant to interact with them, even in an official context. Thus, many investigations were put on hold because parties to the proceedings or witnesses were in hospital, quarantine or self-isolation, or had no possibility to travel due to limitations on public transportation.

The COVID-19 pandemic additionally impacted the use of SITs, e.g. law enforcement and prosecutorial authorities faced challenges in entering premises to place surveillance equipment. In a specific case involving corruption in the health sector which was initiated prior to the COVID-19 pandemic, Romanian authorities were in the planning stage to enter a hospital to place surveillance equipment. However, with the COVID-19 pandemic, a general ban was put into effect on entering hospitals. As a result, law enforcement and prosecutorial authorities could not conduct their planned SIT activities.

Notwithstanding, the COVID-19 pandemic also allowed the law enforcement and prosecutorial authorities to innovate. The Romanian Ministry of Interior implemented a new functionality in the citizens' evidence database. Thus, when law enforcement and prosecutorial authorities queried the database regarding a natural person, the authorities would receive information on whether the person was quarantined, in self-isolation, or if the natural person had entered Romania from a dangerous geographic area and how much time had elapsed since their entry into Romania. This functionality assisted the law enforcement and prosecutorial authorities to plan ahead interviews in the context of ongoing investigations, or to determine whether it would be safe to conduct search of the premises.

Finally, to conduct interviews and hearings, the Romanian authorities summoned lawyers for in-person interviews, while the suspect or witness would join the interview virtually. This was possible because suspects and witnesses were more willing to agree to such an approach.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

### Box 4.2. Romania case study – bribery for issuing false vaccination certificates

The law enforcement authorities of Romania detected allegations of bribery, and the investigation took place between September-October 2021. They received information regarding the issuance of false COVID-19 vaccination certificates from the Ministry of Interior (General Anti-Corruption Directorate). The allegation concerned public officials operating a COVID-19 vaccination centre in Romania. Thus, the investigation began as a forgery case and later investigated as petty corruption. However, during the investigation, it became clear that the corruption scheme was bigger.

The perpetrators would issue the false COVID-19 vaccination certificates and record relevant data into the national electronic register of vaccination. The recorded data included personal data of the vaccinated person, data regarding the vaccine and time of vaccination. The investigation showed that persons would pay EUR 250-300 via intermediaries to obtain the falsified COVID-19 vaccination cards. Once the vaccination certificate had been issued, the person could then obtain the European certificate, thereby facilitating travel despite being unvaccinated.

Law enforcement, with the necessary judicial authorisation, conducted surveillance operations, interception, localisation and recording of phone conversations, audio-video surveillance and utilised undercover investigators. Additionally, law enforcement simulated their interest in obtaining false certificates, thereby allowing law enforcement to understand the corruption scheme and the organisation of the perpetrators. The investigation demonstrated that at least 1 000 false certificates were issued by the COVID-19 vaccination centre.

Ultimately, search operations were carried out and EUR 150 000 were found at the residence of the main defendants. Three suspects who committed bribery admitted guilt and concluded plea agreements with the prosecution.

After the takedown of the operation and its publicisation, many of the persons who had paid bribes under this scheme to obtain the vaccination certification came forward and admitted guilt. The Romanian prosecutor subsequently entered into a plea agreement with these persons, who were served suspended sentences.

The investigation is ongoing at the time of publication.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

## Forensic expertise

### Guidance 16. Forensic expertise

**For law enforcement authorities:**

- Identify the forensic expertise required during the investigation planning stage, e.g. forensic auditing, preserving, collecting and reviewing electronic evidence, while taking into account the nature of the emergency and related corruption offences.
- Hire *ad hoc* forensic experts related to the specific risks and typologies generated by the emergency situation, in particular when such expertise is neither available in-house nor at a partner agency.
- Share expertise with domestic and foreign partners regarding emergency-related investigations and prosecutions and learn about any forensic expertise programmes that foreign partners may have to support ongoing investigative and prosecutorial action during an emergency.

Conducting corruption investigations requires a multidisciplinary approach.[38] It is not uncommon to require forensic expertise related to facts under investigation to further derive meaning from fact. Thus, law enforcement should consider leveraging expertise in investigations by requesting it from specialised government agencies, e.g. forensic auditing or accounting from the Auditor-General. Where such forensic expertise is not available with a specialised government agency, consideration should be given to hire external, ad hoc forensic expertise.

There are different types of forensic expertise which may be required in a corruption-related investigation. These include, but are not limited to digital forensics, forensic financial analysis, forensic auditing and forensic accounting.[39] However, during emergencies, imposed restrictions may limit the ability of obtaining effective forensic expertise. This may be due to a reduction of in-person staff during the emergency, requiring forensics experts to perform tasks outside their job duties as well as inability to conduct the examinations. The reduced number of staff may also result in longer delays in obtaining the requested forensic analysis.

The relevant law enforcement or judicial authority should strive to share any relevant information from ongoing investigations proactively with foreign jurisdictions, subject to local laws, in particular when there is reason to believe that the other jurisdiction is not aware of an alleged crime being committed in its jurisdiction. Another aspect of multijurisdictional cases is the lack of locally available forensic expertise concerning issues connected to those elements of the offence which were committed abroad. These may involve scientific or technical problems not encountered before, e.g. medical issues, unknown digital encryption, etc. In these situations, sharing or making available forensic expertise between law enforcement authorities of the jurisdictions involved can be the key to effectively conduct investigation and prosecution.

In addition, the required forensic expertise may vary depending on the emergency situation and related corruption offences. For example, during the COVID-19 pandemic, many jurisdictions were in need of technical forensic expertise to evaluate the quality of purchased medical or protective equipment, as well as forensic accounting to determine if the prices of these goods were unreasonably inflated.

---

38 See section Information received through other inter-agency co-operation channels of these practical guidelines regarding inter-agency co-operation.

39 See Box 3.13Box 3.13. Bosnia and Herzegovina (BiH) case study – the ventilators case .

### Box 4.3. Mauritius case study – money laundering and corruption related to emergency procurement processes

The Independent Commission against Corruption (ICAC) of Mauritius initiated an investigation in July 2020 based on an anonymous complaint into alleged cases of money laundering and corruption related to emergency procurement processes launched during the COVID-19 outbreak and the award of such contracts.

During confinement, the Ministry of Health and a parastatal body that was set up to act as the Government's commercial arm resorted to emergency procurement procedures in order to acquire medical, pharmaceutical and non-pharmaceutical items, and for decontamination services. However, the emergency procedures for procurement of these supplies were allegedly abused, resulting in contracts being awarded to suppliers that had no experience or were newly incorporated companies that had close connections to politically exposed persons (PEPs) and that supplied substandard items. The corrupt schemes were made worse due to the emergency nature of the situation and the urgent need to procure supplies. The funds were advanced to the suppliers and these parties received economic gain despite not providing the items required or the quality expected.

The investigation included seizing and examining a variety of technological devices. A key part of this investigation was based on the outcome of the forensic analysis of technological devices conducted at the in-house digital forensic laboratory of the ICAC. One of the devices belonging to a contractor provided conclusive evidence that the documented price was significantly inflated compared to the real supplier price.

ICAC through informal co-operation thus established beneficial ownership links between two companies. Additionally, there was effective domestic co-operation between ICAC and law enforcement agencies as well as the FIU.

In the course of this investigation, 8 people were arrested. The investigation which involve public officials and suppliers is at an advanced stage at the time of publication.

Source: *Peer learning* activities, *Law Enforcement Response to Corruption in Emergencies Project*

## Identifying subjects: natural and legal persons

### Guidance 17. Identifying subjects – natural and legal persons

**For governments:**

- Establish and make available, at a minimum to law enforcement authorities, access to databases indicating beneficial ownership information of registered legal persons and legal entities.
- Take steps to provide and maintain an up-to-date lists of politically exposed persons (PEPs) accessible, at a minimum, to law enforcement authorities.

To avoid detection of corruption, perpetrators often attempt to disguise their identity and the proceeds of their crimes by using legal entities.[40] It is critical for any investigation to establish the *beneficial ownership*[41] of these legal entities to determine the alleged perpetrators of a criminal offence and the ownership of the proceeds of crime.

Legal entities used by perpetrators seeking to disguise themselves and the true nature, ownership and origin of their proceeds of crime without real economic performance are known as *shell companies*. They generally do not have employees and do not provide a product or service to the market. Many jurisdictions allow for the creation of shell companies for legitimate purposes, e.g. holding companies. However, these shell companies can also be used to perpetrate criminal offences. Shell companies become a threat when they cannot be traced back to the natural person(s) with effective control over them. Such companies may then become effective tools to veil ownership and illicit conduct (Findley et al., 2012, 7).

During the COVID-19 pandemic, jurisdictions saw corruption-related schemes involving the purchase of medical equipment which used a web of shell companies in the supply chain for their delivery, in an attempt to disguise those unlawfully profiting from a procurement contract,[42] or to inflate the cost for the delivery of goods.[43]

One way to counter this misconduct is by establishing and maintaining beneficial ownership registries. *Beneficial ownership* is a distinct concept from *legal ownership*. The latter refers to the natural or legal person who holds property not for his or her own benefit but that of the beneficiaries. The former, on the other hand, is the natural person who owns or controls the property and can benefit from it (Sharman et al., 2011, 18).

FATF Recommendation 24 requires countries to ensure adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities (FATF, 2019). In practical terms, this means that the following minimum information should be obtained and recorded from a legal person:[44]

- The company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (e.g. memorandum and articles of association), a list of directors.
- A register of its shareholders or members, containing the names of the shareholders and members and the number of shares held by each shareholder (including to the nominal owner of all registered shares) and categories of shares (including the nature of the associated voting rights).

---

40 See section Financial Intelligence of these practical guidelines.

41 The term *beneficial ownership* means the natural person(s) who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted. It also includes those who exercise ultimate effective control over a legal person or arrangement. *Ultimately owning or controlling* and the *ultimate effective control* refer to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control. The domestic law of a jurisdiction usually establishes the criteria for deciding who should be considered a beneficial owner (FATF, 2019, 113) (OECD and IADB, 2019, 4).

42 See e.g. Box 3.2Box 3.2. Lithuania case studies – abuse of office and trading in influence in procuring COVID-19 tests.

43 See e.g. Box 3.13.

44 The Interpretative Note to FATF Recommendation 24 additionally requires that the beneficial ownership information either (i) be obtained by the legal person and available at a specified location in the country; or (ii) have a mechanism that the beneficial ownership of the company can be determined in a timely manner by a competent authority.

Article 52 of the UNCAC defines PEPs as persons with prominent public functions and includes their close family members and associates. As indicated above, Art. 5 of the OECD Anti-Bribery Convention requires investigations into foreign bribery not to be influenced by considerations of the identity of the natural or legal persons involved.[45]

During emergencies, PEPs may abuse their position to take advantage of the reduce accountability mechanisms in place. They may also knowingly enter into a conflict of interest situation. Thus, mitigating factors include ensuring that relevant PEPs continue to disclose their assets while holding office. Moreover, steps should be taken to ensure continued transparency in decision-making to ensure accountability.

### Box 4.4. South Africa case study – investigation into politically exposed persons

South Africa's Financial Intelligence Centre (FIC) conducted an analysis on a politically exposed person (PEP) and established that a legal entity linked to the PEP received COVID-19 relief funds to provide the Department of Education in South Africa with personal protective equipment (PPE) without following the proper procurement processes. The entity was ordered to return the funds with interest to a South African Law Enforcement Department.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project and Box 9: Kenya case study – KEMSA case.

## Pre-trial and trial proceedings

### Guidance 18. Pre-trial and trial proceedings

**For governments:**

- Assess the impact of the emergency on pre-trial and trial proceedings and identify mitigating measures while preserving the rule of law and the right to a fair trial.
- Enable courts to conduct proceedings virtually during an emergency, to ensure business continuity.
- Take steps to digitalise cases and upgrade court management systems to enable court filings, the storage and transfer of information and evidence in digital format.
- Suspend or extend procedural timelines and even statutes of limitation to allow for proper investigation and prosecution of alleged corruption cases.

In the context of an emergency, the COVID-19 pandemic demonstrated the need to find ways to ensure the continuation of investigations and prosecutions despite the restrictions imposed by the emergency. This included moving to a paperless environment for the management of investigative and prosecutorial files, collecting oral evidence by remote link, while ensuring the relevance and reliability of the evidence at the same time. However, in some jurisdictions existing legislation may not allow for the use of electronic filing systems and would still require investigations and court proceedings to be carried out in paper. During an emergency this becomes a challenge when restriction of movement is imposed.

[45] OECD Anti-Bribery Convention.

Thus, these practical guidelines take the elements below into consideration when considering moving to an electronic filing and case management system during emergencies:

- **Oral evidence taken by remote link.** Taking statements by remote link from witnesses located outside a jurisdiction has been possible through international co-operation for some time. To lessen the impact of movement restrictions during emergencies, oral evidence should also be taken remotely in domestic cases as well, if the nature of the evidence so permits and if legislative frameworks are in place to allow this. Thus, law enforcement and judicial authorities should consider the following: (i) the significance of the evidence; (ii) the possibility to ensure the application of necessary procedural guarantees; (iii) the status of the person giving evidence; (iv) the security and integrity of the video link through which the evidence is to be transmitted; and (v) the costs and difficulties of bringing the relevant person to court.
- When taking evidence in this manner, law enforcement and judicial authorities need to ensure that the transmission of the oral evidence can be seen and heard by those involved in the proceedings and that the person being heard from a remote location can see and hear the proceedings to the extent necessary to ensure that they are conducted fairly and effectively. Finally, the procedure and technologies applied to the taking of evidence from a remote location should not compromise the admissibility of such evidence and the ability of the court to establish the identity of the persons concerned, including whether such testimony is recorded. To that end, the quality of the videoconference should be ensured and the video signal encrypted to protect it against interception.
- **Collection, seizure, storage and transmission of electronic evidence.** During emergencies, jurisdictions should review the legal framework regarding electronic evidence and consider enabling law enforcement and judicial authorities to collect, seize, store and transmit electronic evidence in its original electronic format, without the need to supply printouts. Electronic evidence should be stored in a manner that preserves readability, accessibility, integrity, authenticity, reliability and, where applicable, confidentiality and privacy. Moreover, electronic evidence should be stored with standardised metadata so that the context of its creation is clear. Finally, the readability and accessibility of stored electronic evidence should be guaranteed over time, considering the evolution of information technology.
- **Archiving.** Law enforcement and judicial authorities should archive electronic evidence per national law. It should meet all safety requirements and guarantee the integrity, authenticity, confidentiality and quality of the data and respect for privacy. Qualified specialists should carry out the archiving of electronic evidence. Finally, data should be migrated to new storage media when necessary to preserve accessibility to electronic evidence.

## Co-operating witnesses, plea agreements and non-trial resolutions. Witness protection

### Guidance 19. Co-operating witness, plea agreements and non-trial resolutions. Witness protection

**For governments:**

- Establish a comprehensive legal framework to enable witness co-operation, plea agreements and non-trial resolutions in corruption cases.
- Provide dedicated resources for law enforcement to ensure the continuity of ongoing co-operation agreement-based procedures.
- Ensure that witness protection programs have suitable funding to continue operating during emergencies.

**For law enforcement authorities:**

- Issue guidelines for investigators and prosecutors about identifying suitable cases and apply the co-operation agreements effectively.
- Encourage meetings with co-operating witnesses, co-operating perpetrators and defence counsels through secure telecommunication or videoconferencing facilities.

An effective way for law enforcement authorities to obtain strong, direct evidence about corruption is breaking the conspiracy and collusion of the involved by applying asymmetric consequences. Co-operating witnesses, plea agreements and non-trial resolutions are powerful legal tools in the hands of law enforcement authorities to negotiate the outcome of an investigation with culpable individuals.

Co-operating witnesses are individuals who obtained insider knowledge about the criminal conduct by either participating in the commission or assisting in its preparation or being involved in ancillary offences like money laundering. In exchange of their co-operation with the law enforcement authorities and disclosing vital evidence these individuals are granted immunity from prosecution (typically by a non-prosecution agreement) and are interviewed as witnesses throughout the criminal proceedings.

Another powerful tool law enforcement authorities may apply to the same end are plea agreements. In the case of plea agreement, a perpetrator of the offence admits guilt, co-operates with the authorities by disclosing information and evidence, in exchange of milder sentencing. Plea bargaining refers to the negotiation of an agreement between the prosecution and a defendant whereby defendants are permitted to plead guilty under more favourable terms than if they simply pleaded guilty to all charges filed against them(OECD, 2017, 55). These agreements include criminal liability, mutually agreed sanctions and typically require judicial approval which takes the form of sentencing.

In the case of legal persons, non-trial resolutions (NTR) are applied in similar situations, and are agreements between a natural or legal person and an enforcement authority to resolve a criminal, civil or administrative matter without a full trial on the merits of the case (OECD, 2019, 17). They can involve a conviction, e.g. plea agreement, or some type of non-conviction agreement, e.g. deferred or non-prosecution agreements, the design and implementation of an effective compliance programme.

NTRs have become a prominent means for resolving economic crimes, including corruption and bribery of foreign public officials or other related offences (OECD, 2019, 19). They are an efficient tool for resolving complex foreign bribery cases, as prosecutors have the option to resolve foreign bribery matters without engaging the full range of resources necessary to prosecute a case through a trial on the merits and any potential appeal proceedings (OECD, 2019, 21-22). The OECD Working Group on

Bribery (OECD/WGB) and the International Bar Association (IBA) found that at many jurisdictions used some form of NTRs to resolve approximately 80% of foreign-bribery-related cases (Makinwa and Søreide, 2018; OECD, 2019). Recommendation XVIII of the 2021 OECD Anti-Bribery Recommendation further requires jurisdictions ensure that NTRs follow the principles of due process, transparency and accountability.

During an emergency, the restrictions of movement and limitations concerning capacities and possibilities to engage and communicate with defendants and defence counsels poses a serious obstacle to proceed with negotiating agreements. As the timing and timeliness of these agreements are crucial, the emergency situation alone might render them unavailable.

Individuals helping the authorities (whistleblowers, witnesses and perpetrators engaging in plea agreements) might face retorsion, even threats to life, from their peers, organisation or the perpetrators of the disclosed offences. This pressure might result in loss of evidence and failure to prosecute criminal conduct. Law enforcement authorities can use the framework of witness protection regime to counter this phenomenon and to provide adequate protection for these persons.

During an emergency a related challenge is to ensure that persons under witness protection programmes remain financially stable during an emergency. As such, jurisdictions should consider extending financial support programmes afforded to the public during the emergency also to those under witness protection. Finally, where a person under witness protection must be relocated, emergencies such as the COVID-19 pandemic may face challenges if any lockdowns or movement restrictions are put in place.

To encourage culpable individuals to co-operate, co-operating defendants can be rewarded, where legal systems allow for it, with lighter sentences than those convicted of the same offences.

### Box 4.5. Costa Rica case example – witness protection during the COVID-19 pandemic

During COVID-19 pandemic, the prosecution service used the witness protection programme of Costa Rica.

In the first case, the co-operating witness worked in a public institution. The co-operating witness presented a report indicating embezzlement by the members of the board of the public institution. Because of this report, the co-operating witness was transferred to a remote location by the public institution. As a result, the co-operating witness filed a complaint with the office for the attention and protection of victims.

In the second case, the co-operating witness was working for an entity which opened a tender procedure for the construction of a building. However, the tender was rigged, and the entity was overbilled for the construction of the building. The co-operating witness provided information anonymously, as the co-operating witness did not want to be associated with triggering the investigation.

These cases demonstrate the fear that co-operating witnesses experience. It further shows challenges and risks they face, in particular retaliation and pressure. Mechanisms should thus be in place to ensure co-operating witnesses can present their complaints anonymously.

The law on the protection of victims, whistleblowers and co-operating witnesses of Costa Rica allows anybody to approach the office for the attention and protection of victims whenever they are, or fears they are at risk. They protection team helps the person to establish the level of risk they are under by using a group of criminologists, psychologists and social services.

There is another Bill before Congress to further protect whistleblowers and witnesses, providing protection at the administrative phases before the case becomes a criminal one.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project.

## Freezing, seizure and confiscation

### Guidance 20. Freezing, seizure and confiscation

**For governments:**

- Ensure that the seizure and confiscation regime is effective to deal with the specific corruption-related risks identified during the emergency and is applied in practice.

Provisional measures to freeze and seize assets are a key tool to ensure the preservation of those assets' value for any confiscation order that may be made post-conviction. FATF notes that a robust system of provisional measures and confiscation is an important part of an effective anti-money laundering and counter-terrorist financing regime. Countries should have measures in place to identify, freeze and seize property laundered, proceeds from money laundering or predicate offences, instrumentalities used or intended for use in the commission of these offences, or property of corresponding value.

Additionally, the FATF recommends that countries adopt legislative measures that enable them to confiscate (without prejudicing the rights of bona fide third parties): property laundered; proceeds from

or instrumentalities used in or intended for use in money laundering or predicate offences; property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or property of corresponding value. In addition, assets to be confiscated include property used in the commission of the offence (instrumentalities), direct proceeds, indirect proceeds, property part of which contains proceeds that have been intermingled with legitimate assets and any benefits or income from this property.

FATF Recommendation 4 also states that jurisdictions should consider introducing measures allowing for the confiscation of instrumentalities and proceeds without the need for a conviction (non-conviction-based confiscation) (FATF, 2019).

During emergencies, law enforcement and prosecutors may encounter challenges related to pre-trial and trial proceedings, particularly if the judiciary is temporarily closed or operating in a limited manner.

## High-profile corruption

### Guidance 21. High-profile corruption

**For governments:**

- Establish or strengthen existing specialised anti-corruption law enforcement and judicial authorities.
- Strengthen the external independence of law enforcement and judicial authorities dealing with high-profile corruption cases and the internal independence of investigators and prosecutors working on such cases.
- Provide adequate resources to law enforcement and judicial authorities dealing with high-profile corruption cases to enable them to conduct their procedure independently from other agencies.
- Review the legal framework of public immunities with the view of ensuring that immunities do not pose an obstacle to effective investigation and prosecution of high-profile corruption cases.

**For law enforcement authorities:**

- Review their communication and public relations strategies to be able to counter illicit pressure and influencing attempts.
- Strengthen internal guidelines and procedures to safeguard investigators and prosecutors from potential pressure via disciplinary or labour law related decisions of the management.

When dealing with high-profile corruption cases, these practical guidelines raise three main elements for operational consideration: (i) independence of investigations and prosecutions, (ii) relevant considerations for PEPs, and (iii) challenges of public (legislative or executive) immunity.

The first element refers to independence of investigations and prosecution and the risks of illicit interference by the executive or legislative branch in investigating and prosecuting high-profile corruption cases during emergencies. Since these cases may involve high-ranking public officials or considerable amount of public funds and attract significant public attention, they are exposed to potential interference and pressure.

Recognising this attribute of foreign bribery cases, Article 5 of the OECD Anti-Bribery Convention requires States Parties to ensure that investigations and prosecutions are not influenced by

considerations of national economic interest, the potential effect upon relations with another State or the identity of the natural or legal persons involved. Obviously, high-profile domestic corruption cases share this attribute and are exposed to risk of being influenced by similar considerations. Among the ways to counter such interference is the existence of independent specialised investigative and prosecutorial authorities, shielded from external influence. During emergencies these safeguards might be curtailed or suspended, which threatens the independence of investigation and prosecution.

Claims of shortage of resources due to emergency may cause inter-agency co-operation in sensitive cases to suffer setbacks as other agencies might be reluctant to provide assistance. Therefore, these specialised anti-corruption agencies should have their own resources to carry out investigative steps at least in their priority cases without having to rely on other agencies.

Due to the sensitive nature of these cases, illicit pressure may be exercised through media coverage offering one-sided narratives, based on the defendants' claims. Law enforcement and judicial authorities need to review their communication and public relations strategy and policies to be able counter these influencing attempts.

Another important aspect in this context is the system of internal safeguards in place within the authorities themselves. Investigators and prosecutors handling high-profile corruption cases must be equipped with appropriate tools and possibilities to counter and resist illicit pressure from their superiors as well. Considerations should be given to existing solutions, like prosecutorial and judicial councils as bodies able to ensure that e.g. disciplinary or labour law related powers of the management cannot be used to pressure those working on these cases.

The second element concerns the challenges with public immunity. Immunities based on legislative or executive functions provide persons or groups of persons some degree of protection against civil or criminal procedures. These provisions are in place to ensure the unimpeded performance of public functions and to avoid targeted prosecutions or political persecution. However, immunities can also be abused by officials who use it as a shield to avoid or at least delay liability for criminal offences, including corruption.

Most countries provide immunity protection for their high-ranking public officials. However, each jurisdiction varies in the range of officials covered, scope of immunity and rules regulating the procedures for lifting immunities.

- *Absolute immunity* – immunity for any acts committed by public officials, whether they are directly related to their official function or not. The UNODC highlights absolute immunity as the type most likely to be invoked in the context of criminal proceedings for corruption offences.
- *Functional immunity* – immunity for public officials for acts committed in the course of the performance of their function. Functional immunity is further subdivided into *non-liability*, which provides legal protection for opinion and votes cast in Parliament; and (ii) inviolability, which extends to any acts a public official performs in their function.

During emergencies, immunities can be an obstacle of effective investigation and prosecution in high-profile corruption cases, for various reasons. First, the immunity might already impede the collection of evidence itself, e.g. by limiting the application of certain investigative tools or powers. Second, the immunity is an obstacle to filing the indictment and often the prosecution has to disclose the full case file to the body or person entitled to decide on the lifting of immunity. In high-profile cases this disclosure can threaten the confidentiality of the investigation and lead to pressure and interference by the involved high-ranking officials. Third, the bodies or persons entitled to lift immunity may be hindered in their function and not available to make the required decision during an emergency, which will effectively stop the criminal procedure.

### Box 4.6. Peru case example – the Vacunagate scandal

The *vacunagate* refers to the alleged advantage or exclusivity for the acquisition of vaccines against COVID-19 to one supplier. The investigation alleges that the arrangement would have benefitted a former President of the Republic and close associates. Alleged perpetrators in the investigation into the *vacunagate* also include alleged conduct of former ministers. They allegedly committed extortion or abuse of authority and unlawful interests in public contracts.

The Government of began negotiating with the supplier in August 2020 to acquire an important quantity of COVID-19 vaccines as well as the entity that would co-ordinate clinical trials of the vaccine in the country. In turn, a health research facility was appointed, which indicated the need for 200 COVID-19 vaccines to cover the personnel of the clinical trials. Subsequently, the vaccine supplier requested clarification of the quantity of vaccines needed following additional requests by the health research facility. The Peruvian authorities confirmed the need for 3 200 COVID-19 vaccines, which the investigation alleges included special requests for vaccines to cater to government staff and businesspersons. The investigation further alleges that clinical trial vaccines were also distributed to a former President and close family members and associates.

As a result, approx. 500 persons, including the country's top officials and his wife were vaccinated, before the official vaccination in Peru began. The investigation has shown that there were four group of beneficiaries: (i) clinical trial researchers; (ii) persons not part of the clinical trial and their close family members, including high-ranking public officials; (iii) government officials, mainly staff from the Ministries of Health and Foreign Affairs; and (iv) consultants, mainly doctors working in private clinics in Lima and who had no direct links with the clinical trial.

The investigation has been unable to show, to date, where the other vaccines went. The investigation is ongoing in this regard at the time of publication. Finally, the Peruvian public prosecution office has opened a case of foreign bribery against the producer of the vaccines, which remains ongoing at the time of publication.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

# 5 International co-operation

The increase of cross-border movements of persons, goods and services throughout the 20th century and the increasing international visibility of corruption-related offences (Machado, 2004, 18; Currie, 2010, 19; Boister, 2012, 13-23) has required jurisdictions to enhance their abilities to co-operate and co-ordinate with each other. As a result of the increase of international exchanges and connections, situations where crucial information and evidence can be found in other jurisdictions became more and more prevalent. Thus, jurisdictions must engage in international co-operation to support their efforts to detect, investigate and prosecute corruption-related offences, among others, in a valid and timely manner.

The *validity* of information implies that the requesting jurisdiction must be able to utilise the evidence obtained through international co-operation in a manner that is admissible in its own proceedings. The admissibility of the evidence requires the requested jurisdiction to gather the evidence sought through a mechanism defined by the involved jurisdictions in advance, e.g. an international treaty, or through reciprocity undertaking. The *timeliness* of the exchange requires the requested jurisdiction to execute the assistance sought through international co-operation within the reasonable timelines. To meet these timelines, the involved jurisdictions need to communicate and collaborate in the steps prior to and during the execution of the assistance sought through international co-operation.

In criminal investigations, obtaining information or evidence that is not valid and admissible in pointless. Similarly, if the information does not arrive in time, it will be of little use to investigators and prosecutors.

Corruption-related offences and their investigations, especially in high-profile cases, rarely are purely domestic. Law enforcement and prosecutors will need to obtain information and gather evidence in other jurisdictions, e.g. communication from ISPs,[46] financial data,[47] beneficial ownership data,[48] or evidence substantiating self-reports.[49] Most of the crisis-related corruption cases and investigations cannot be solved without international co-operation due to supply chain considerations, involvement of foreign legal entities, money laundering considerations, and asset recovery efforts.

This chapter of the practical guidelines focuses on good practices related to different methods and channels of international co-operation, and how they can be used during emergencies.

46 See section Electronic evidence of these practical guidelines.

47 See section Financial intelligence of these practical guidelines.

48 See section Identifying subjects: natural legal persons of these practical guidelines.

49 See section Self-reporting of these practical guidelines.

## International financial institutions integrity and investigative units

### Guidance 22. International financial institutions' integrity and investigation units

**For law enforcement authorities:**

- Enter into MoUs with IFIs in cases involving IFI-funded projects to help expedite investigations and facilitate information sharing.

An *International Financial Institution* (IFI) is a financial institution that has been established by more than one jurisdiction and is subject to international law.[50]

The integrity units of IFIs investigate and pursue sanctions related to allegations of conflict of interest, abuse and misuse of resources, fraud, corruption, collusion, coercion and obstruction, among other prohibited practices, committed by individuals and legal entities involved in IFI-financed operations. IFIs also have units that investigate misconduct by their own staff.

To undertake such activities, the integrity units of IFIs conduct investigations into allegations of sanctionable practices in the IFIs' operations against individuals and legal persons.[51] An IFI may impose sanctions to against individuals and legal entities doing business with the IFI-financed operations should their investigations identify any wrongdoing. Moreover, IFIs may refer any evidence of misconduct by government officials to their national authorities for action.

Because the integrity units of IFIs investigate individuals that can be criminally investigated by national law enforcement authorities, they can assist law enforcement with detection by referring cases to a jurisdiction or providing information which enables law enforcement to conduct their own independent investigations. Where an MoU between the integrity unit of the IFI and law enforcement of a jurisdiction exists, the integrity unit of the IFI may assist law enforcement authorities in their investigations.

50 There are different types of IFIs: the Bretton Woods institutions, comprising the International Monetary Fund (IMF), the World Bank Group (International Bank for Reconstruction and Development (IBRD), International Finance Corporation (IFC), International Development Association (IDA), International Centre for Settlement of Investment Disputes (ICSID) and the Multilateral Investment Guarantee Agency (MIGA)), and the World Trade Organisation (WTO).

The term also encompasses multilateral development banks (MDBs), which include the Inter-American Development Bank (IADB), the Development Bank for Latin America (CAF), the European Investment Bank (EIB), the European Bank for Reconstruction and Development (EBRD), the African Development Bank (AfDB), the Asian Development Bank (ADB) and the Islamic Development Bank (IsDB).

51 IFIs will typically handle allegations concerning (i) misuse of IFI funds; (ii) abuse of position for personal gain, (iii) fraud, (iv) corruption, collusion, coercion, conflict of interest, and (v) misconduct of IFI-financed operations or in the administration of the IFI business.

### Box 5.1. IFIs – Typologies of cases identified during the COVID-19 pandemic

During the COVID-19 pandemic, some IFIs identified the following typologies in their operations:

- Fraudulent procurement, with inexperienced legal entities being awarded contracts.
- Undisclosed conflicts of interest.
- Payments to non-existing companies.
- Embezzlement of funds by public officials.
- Diversion of products.
- Substitution of products.
- Substandard products.
- Price gouging.
- Bid rotations.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

During the COVID-19 pandemic, IFIs saw an increased time for complaint assessments and determinations, diminished interaction with parties, inaccessibility to full time records, reduced real time data flow, and reduced complaint reporting. These issues were compounded by flight and travel disruptions that, while mitigated by introducing the use of third parties to assist with their investigations, remote audits, remote meetings, utilising staff at country offices, and collaboration with partners and relevant authorities with which they have MOUs, slowed the pace of investigations. IFIs work with national law enforcement authorities through MOUs. It implies that IFIs work directly with law enforcement and do not require MLA to share information with one another.

The MOUs between IFIs and national law enforcement authorities are negotiated based on identified mutual interest, e.g. information gathering. IFIs may have information on relevant project documentation they are financing, and information on the legal entities involved. The MOUs also enable the IFIs to provide some training support to the national law enforcement authorities. These MOUs formalise the terms of exchange between the IFI and the national law enforcement agency and sets out how the information will be exchanged in combating corruption-related offences.

### Box 5.2. IFIs – Change in practice during the COVID-19 pandemic

- *Remote interviews.* Due to lockdowns and movement restrictions, IFIs moved to conducting remote interview to mitigate challenges in conducting their investigations. However, remote interviews also posed their own challenge, since IFI investigators had limited control over the environment, e.g. witnesses' behaviour, connectivity issues, time differences and maintaining confidentiality.
- *Off-site inspections*. Due to lockdowns and movement restrictions, IFIs delayed conducting missions and opted for reviewing information remotely. The challenge under such circumstances included the inability to inspect physical documents given the lack of access to full records, objects and sites. Moreover, the absence of on-ground presence resulted in diminished (human) information gathering.
- *MOUs with national law enforcement authorities.* To mitigate challenges arising from movement restrictions, IFIs intensified previous efforts to enter into MOUs with national law enforcement authorities to expedite their investigations.
- *Use of third parties*. To further mitigate challenges arising from movement restrictions, some IFIs outsourced elements of their processes to third parties, e.g. law firms to conduct due diligence relevant to an inquiry.
- *Providing advance preventive support to operations*. Recognising the need for broad-based, in-time advice for operational staff, IFIs developed new guidance documents that summarised the most salient integrity risks in the sectors supported by the pipeline of emergency operations.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project and (World Bank, 2020, 37)

### Box 5.3. IFI case study – corruption in infrastructure projects

Local authorities and an IFI conducted a parallel investigation concerning the construction of a street drainage system in a Latin-American jurisdiction. One year after the construction, there were heavy rains, and the street was flooded. The investigation discovered that drainages were only partially installed, contrary to what was claimed by the company and the local government supervising the construction – constituting a significant fraud. The investigation also revealed the collusion between the company and the local government. The country prosecuted the individuals and the IFI was able to sanction the company for 12 years.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

## International FIU platforms and intelligence sharing

As outlined earlier,[52] financial intelligence and analysis can play a role in the detection of corruption. However, during the investigation financial information obtained from abroad plays an equally crucial role in establishing links, identify potential evidence and substantiate legal assistance requests to obtain

[52] See section on financial intelligence of these guidelines.

it. Therefore, for the law enforcement authorities the ability to request and receive financial information by utilising FIU channels is essential. Law enforcement authorities typically do not have direct access to FIU information and international exchange, even if the given FIU is organised within such an agency. The proper combination of domestic inter-agency co-operation[53] and the international co-operation of FIUs is required to untap the full potential FIUs have in investigating corruption. During emergencies both spheres of co-operation are challenged and both law enforcement and FIUs have to find solutions to overcome the emerging legal, operational or technical obstacles.

FIU-to-FIU co-operation is primarily done through the Egmont Secure Web (ESW). The Egmont Group is a united body of 167 financial intelligence units (FIUs) that provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and the financing of terrorism (Lefebvre, 2003, 532).

The ESW ensures the communication and exchange of information among FIUs. The purpose of the ESW is to: (i) provide a secure and reliable channel of communication for the members of the Egmont Group; (ii) function in accordance with the mandate of the Heads of FIU; and (iii) adhere to the standards of security, reliability, efficiency and effectiveness specified by the Heads of FIU.

To obtain information, the requesting FIU must provide context, correlating and linking the information sought with the facts under analysis by the relevant authority. The narrative should thus provide a summary connecting the facts under analysis with the underlying suspicion and, where possible, the indication of the predicate offence. To the extent possible the narrative should include the relation of the person(s) under review, the facts of the case and the underlying suspicion, as well as an indication of amounts and accounts connected with the facts under analysis. The narrative should be presented in short, direct, clear and straightforward sentences.

International and regional standards require jurisdictions to establish effective mechanisms for co-operation between the competent national authorities. However, these standards do not provide or refer to any particular mechanism. Some mechanisms to strengthen the co-operation between the FIU and law enforcement authorities may include (Stroligo et al., 2018, 23):

- Staff from either the law enforcement agency or the FIU serving as a liaison officer.
- Designating points of contact in the FIU and competent law enforcement authorities to deal with operational matters and other bilateral issues.
- Signing bilateral or multilateral MoUs among the FIU and relevant law enforcement authorities.
- Establishing inter-agency working groups or task forces to deal with operational or case-based matters or more strategic issues.

During emergencies the traditional co-operation channels and methods may not be sustainable, both between law enforcement authorities and FIUs and the FIU-to-FIU.

The challenges faced by FIUs at the national level during emergencies may impact international FIU platforms, e.g. business continuity and maintaining confidentiality. Notwithstanding, the greater challenges may arise when seeking co-operation with FIUs which are not members of the Egmont Group. Because co-operation in such instances does not operate, among others, through the ESW, an emergency may restrict the ability of an FIU which is not a member to the Egmont Group to share intelligence in a timely manner. In such cases, consideration should be given to ensuring that the involved FIUs have communication channels which enable them to not only share intelligence in a timely manner but do so in a manner which preserves confidentiality and security to the shared intelligence.

[53] See section on inter-agency co-operation of these guidelines.

## Law enforcement and judicial co-operation platforms

### Guidance 23. Law enforcement and judicial co-operation platforms

**For law enforcement authorities:**

- Strengthen the use of law enforcement and judicial co-operation platforms as a mechanism to verify and confirm lines of inquiry in investigations, prior to the submission of requests for MLA.
- Use the secure communication channels provided by law enforcement and co-operation platforms to communicate, and transfer information and evidence.
- Designate points of contacts to the law enforcement and judicial co-operation platforms that they are party to.

Mutual legal assistance (MLA) remains the principal way jurisdictions ensure that evidence collected beyond their borders is admissible in national proceedings. Because of this, international co-operation is often viewed exclusively based on MLA mechanisms.[54] However, international co-operation mechanisms have evolved and have more streamlined methods for communication, co-ordination and sharing of information among authorities from different jurisdictions.

Law enforcement and judicial co-operation platforms[55] complements each other, essentially representing the two parallel running tracks of international co-operation in criminal matters. For the purpose of this section, law enforcement co-operation platforms mean those of investigating authorities, which fulfil the need for exchanging information and intelligence. On the other hand, judicial co-operation platforms for prosecutors and judges support the exchange of evidence through e.g. facilitating MLA requests. The complementarity and synergy of these two fields of co-operation can create an environment all law enforcement authorities can profit from.

Law enforcement and judicial networks usually allow for better information collection, ensure the admissibility of evidence in the affected jurisdictions, and provide more accurate results. Additionally, law enforcement and judicial networks provide a safe space for law enforcement and prosecutorial authorities to foster trust with each other.

These complementary mechanisms take the form of (i) tools and instruments for co-operation found in international treaties; (ii) the promotion and use of dedicated platforms; and (iii) inter-institutional co-operation.

In the light of the above, mechanisms for the exchange of information between competent authorities, serve multiple purposes:

- To obtain information about the existence and whereabouts of potential evidence in another jurisdiction.
- To establish links between parallel running investigations or obtain information on previous cases.
- To decide whether a request for MLA is required and feasible to complete or strengthen the proving in an investigation.
- To prepare or draw up MLA requests.

54 See section Mutual legal assistance and extradition, conflict of jurisdictions of these guidelines.

55 See section Law enforcement and judicial co-operation platforms of these guidelines.

- To resolve questions raised during the execution of MLA requests.

Although the international exchange of information mechanisms is typically quicker, it generally does not produce admissible evidence for criminal proceedings. However, they are critical when seeking to confirm or dispel lines of enquiry in an ongoing investigation.

An important element of international co-operation is building trust and contacts among the requesting and requested authorities. Direct communications support this purpose. Although law enforcement officials generally strive to have face-to-face meetings, such possibilities may already be resource-limited in normal times, while in emergencies, face-to-face meetings may not be possible. New technologies allowing for video communications greatly support these efforts.

As a bilateral form of co-operation between jurisdictions, *liaison officer* is the principal interface between his or her law enforcement agency and the law enforcement authorities of the host jurisdiction. They are a gateway regarding incoming and outgoing international enquiries. A liaison officer is responsible for, among others, processing incoming and outgoing international requests and enquiries (including MLA), assessing threats, risk and harm in line with local, national and international guidance to ensure that enquiries and requests are dealt with appropriately. During emergencies, liaison officers can play a key role in ensuring undisrupted communication between the relevant law enforcement or prosecutorial authorities of the jurisdictions involved and can act as a channel for transmission of information and documents between them.

### *Law enforcement co-operation networks*

Concerning multilateral *law enforcement co-operation platforms*, these include but are not limited to:

- *Interpol* is the world's largest police organisation, composed of 195 member countries. Its core of mission and infrastructure is to provide its member states with databases and digital communication systems between the national law enforcement authorities of its Member States through the National Central Bureau (NCB). Interpol conducts both criminal operational and intelligence analyses. Moreover, it has several databases which support law enforcement activity.
- *Europol* is the EU Agency for Law Enforcement Co-operation. Its mission is to support its member states in preventing and combating all forms of serious international and organised crime. Europol also works with many non-EU partner states and international organisations (EUROPOL, 2022).
- *The Camden Asset Recovery Inter-Agency Network (CARIN) and Asset Recovery Inter-Agency Networks (ARINs)* are an informal network of law enforcement and judicial practitioners in the field of asset tracing, freezing, seizure and confiscation. It is an inter-agency network where each member state is represented by a law enforcement officer and a judicial expert. It seeks to increase the effectiveness of the efforts of its members to deprive criminals of their illicit profits (Secretariat).
- There are currently seven regional ARINs in the following regions: (i) Latin America (*Red the Recuperación de Activos de GAFILAT*); (ii) Asia-Pacific (ARIN-AP); (iii) Caribbean (ARIN-CARIB); (iv) East Africa (ARIN-EA); (v) Southern Africa (ARINSA); (vi) West Arica (ARIN-WA); and (vii) West and Central Asia (ARIN-WCA).
- *The OECD WGB's informal meetings of law enforcement officials (WGB LEOs), the OECD Global Network of Law Enforcement Practitioners against Transnational Bribery (GLEN) and regional Law Enforcement Networks (OECD ACD/LENs)* in the Asia-Pacific region (Asia-Pacific Initiative – ACI LEN), Latin America and Caribbean region (LAC LEN) and Eastern Europe and Central Asia (ACN LEN). These networks promote greater informal co-operation and peer-to-

peer exchange of information among law enforcement practitioners that work on foreign bribery (WGB LEOs), transnational (GLEN) or complex corruption cases (regional LENs).

- *The Global Operational Network of Anti-Corruption Law Enforcement Authorities (GlobE Network)* was established in 2021 under the auspices of UNODC to facilitate informal co-operation and to address the lack of a global network for anti-corruption law enforcement authorities. It provides a platform for peer-to-peer information exchange and informal co-operation to better identify, investigate and prosecute cross-border corruption offences and recover stolen assets (UNODC, 2022).

During emergencies, challenges may arise in sharing information through law enforcement co-operation platforms either because of restrictions law enforcement may have in obtaining information at the national level due to the emergency or because of movement restrictions limiting their ability to communicate with, e.g. liaison officers. The main challenge faced by the OECD/ACD LENs related to restrictions of travel during the COVID-19 pandemic, which limited the ability of in-person meetings. Notwithstanding, the OECD/ACD LENs moved their meetings to a virtual setting, to minimise impact on the ability of law enforcement and prosecutorial authorities to continue meeting and exchange information with each other.

### Box 5.4. The International Anti-Corruption Co-ordination Centre (IACCC)

**Background**

The International Anti-Corruption Co-ordination Centre (IACCC) is a multi-agency law enforcement team. The IACCC is intelligence led and supports law enforcement investigations at no cost. The IACCC does not conduct in-house investigations, however.

The IACCC is designed to simplify international co-operation and provide a comprehensive intelligence snapshot in a rapid manner, with the goal of enhancing the efficiency and speed of international investigations. The IACCC's intelligence-led work helps with the return of assets to affected states. The IACCC members are: Australia, Canada, New Zealand, Singapore, the United States and the United Kingdom. An associate member scheme exists as of July 2020 for smaller offshore jurisdictions to refer cases and pass intelligence.

**Work streams**

The IACCC's work stream focuses on three stages: referral assessment, intelligence development, and investigation support. In the first stage, matters are referred into the centre and the IACCC commences an initial evaluation. Secondly, the IACCC members conduct intelligence development, which involves the extraction of entities and identifiers, development of extensive open-source intelligence searches, checks on home systems of targets, intelligence compiled on LAN, and case officer analyses composite product. The IACCC produces a detailed intelligence report that is disseminated to the relevant authorities. Thirdly, the IACCC provides investigation support, as requested. This involves the deployment of digital forensics (DF) kit and case specific training and mentoring. Further, the IACCC provides MLA/ILOR support.

**Case Achievements**

As of autumn 2021, over 170 cases were referred from across six continents. The IACCC has disseminated approximately 85 intelligence packs and assisted with the submission of 37 MLA requests. From 2017 to 2021, the IACCC has identified over EUR 750 million, resulting in the freezing of over EUR 300 million and returned EUR 70 million to affected states. The IACCC reporting has resulted in the identification of 1 863 financial products and led to t63 subjects charged or arrested.

Despite the successes of the IACCC, the centre faces various challenges to its work, including addressing the amount of information case officers must manage, ensuring case progression beyond intelligence and difficult work and co-operation conditions resulting from COVID-19.

Critical to the IACCC's work will be fostering innovation and employing the latest tools and techniques that will allow IACCC members to identify relevant intelligence most quickly and effectively. Moreover, the IACCC's forward looking focus is increasing investigative support, ensuring identified assets can be returned to affected jurisdictions.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

### *Judicial co-operation networks*

Parallel with law enforcement co-operation platforms, there are a number of judicial co-operation platforms which judicial authorities (prosecutors and judges) may use to facilitate international co-operation with the view of obtaining admissible evidence from abroad:

- *UNODC databases of competent authorities.* The UNODC maintains online directories of competent national authorities under the 1961 and 1971 International Drug Control Treaties, the 1988 Vienna Convention, the UNTOC and the UNCAC. Relevant authorities can request access to an account with the UNODC to obtain relevant information pertaining to, e.g. central authorities, contact persons, relevant corruption prevention authorities, asset recovery focal points).
- *Eurojust.* Eurojust is the EU agency for criminal justice co-operation. It supports co-ordination and co-operation between national authorities in combating serious crime. Each EU Member State has a prosecutor representing their jurisdiction at the seat of Eurojust in The Hague, allowing for every Member State to working in close, direct and personal contact. Co-operation between Eurojust and ten non-EU countries is strengthened by liaison prosecutors, international agreements and single points of contact (SPoCs). Eurojust has contact points with competent authorities in 60 non-EU countries worldwide and signed co-operation agreements with organisations aiming to facilitate co-operation, e.g. IberRed). These connections enable prosecutors from EU Member States to establish quick contact and liaise with their counterparts.
- *European Judicial Network (EJN)*. It is a network of contact points designed to facilitate judicial co-operation in criminal matters. Each EU Member State designates contact points from the central authorities responsible for international judicial co-operation and the judicial authorities or other competent authorities with specific duties in international judicial co-operation. The EJN has several online tools to facilitate judicial co-operation, e.g. the judicial Atlas, judicial library, and the description of the countries' relevant legal system ('*fiches belges')*.
- *Red Iberoamericana de Co-operación Jurídica Internacional (IberRed).* It is a space for co-operation in civil and criminal matters for representatives of Ministries of Justice and prosecutors in 22 countries in Latin America and the Iberian Peninsula (Andorra, Spain and Portugal). IberRed has signed MoUs with Eurojust (2004), EJN (2013) and Interpol (2013). IberRed seeks to optimise international co-operation in criminal and civil matters between Latin American countries by (i) contributing to the effective development of transnational proceedings and optimisation of requests for MLA; and (ii) ensuring effective and practical application of the international co-operation treaties among the Latin American and Iberian countries. The IberRed has five main characteristics: (i) informality (the actions of its members are not designed to be incorporated into proceedings, but to drive them forward. It does not substitute MLA); (ii) Complementarity: the intervention of its members does not substitute the activity of the competent authorities; (iii) horizontality: IberRed works without any hierarchy. SPoCs ("co-ordinators") are assigned for each of the relevant institutions in each country, which co-ordinates the national SPOCs; (iv) Flexibility: to adapt to the characteristics of each judicial organisation; and (v) Mutual trust.

Similar to the law enforcement co-operation platforms,[56] emergency-related challenges may arise in obtaining evidence at the national level for later sharing with international partners, or challenges to meet in person. Additional challenges may arise when having to obtain orders from courts.[57] However, the co-operation networks often maintain secure communication channels which the law enforcement and judicial authorities may use for co-operation and co-ordination purposes, to maintain business continuity during an emergency.

56 See section Law enforcement co-operation networks of these practical guidelines.

57 See section Pre-trial and trial proceedings of these practical guidelines.

## Mutual legal assistance and extradition, conflict of jurisdictions

### Guidance 24. Mutual legal assistance and extradition, conflict of jurisdictions

**For governments:**

- Accept requests for MLA and extradition submitted solely via electronic channels.
- Enable the hearing of persons to be conducted via videoconferencing facilities.
- Identify alternative travel methods, e.g. chartering flights, to secure the surrender of natural persons when the requesting and requested jurisdictions do not share a direct border.

**For law enforcement authorities:**

- Process incoming and outgoing requests for MLA dealing with issues arising from the emergency as a priority.
- Hand over documents or requests to the liaison officer at the embassy of the jurisdiction involved, as a method of delivery of requests for international co-operation.
- Assess the impact that the emergency has on resolving conflicts of jurisdictions and negotiate solutions that ensure the proper administration of justice.

### *Mutual legal assistance*

The purpose of mutual legal assistance (MLA)[58] is to enable States to exercise their criminal jurisdiction by obtaining admissible evidence which can be found abroad for their criminal investigations and prosecutions.

There are three channels of communication for MLA:

- **Diplomatic channels** are used in the absence of an agreement which allows the transmission of the request via the central authorities responsible for international judicial co-operation.
- **Central authorities** are specialised bodies dealing with MLA. They support local authorities by assisting in the elaboration of international investigation strategies and communication with their foreign counterparts to understand the requirements of the legislation of the requested state.
- **Direct transmission.** More recent international conventions[59] allow for the transmission of requests for MLA directly between the competent requesting and requested authorities, without the need of submitting them via diplomatic channels or central authorities. This shortens the time needed for the execution of the requests and facilitates more effective co-operation.

International agreements dealing with MLA (and also extradition) have provisions allowing for the exchange of requests via electronic channels. However, the rule is still the submission of the request in paper format.

In emergencies, as seen during the first year of the COVID-19 pandemic, there was a sharp reduction of MLA requests issued by jurisdictions. The emergency also impacted the ability of the requested jurisdiction to execute requests for MLA. For example, to address this issue, the EU is proposing the full digitalisation of cross-border judicial co-operation. It acknowledges that currently most data

58 These practical guidelines define *mutual legal assistance* as the manner through which a jurisdiction renders assistance to another so that the requesting state may comply with its jurisdictional obligations.

59 (See: CoE, 2001a. Art. 4). Including the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and related regulations.

exchanges in cross-border judicial co-operation takes place on paper, which is slower and less efficient than using electronic means (Commission, 2021).

According to a Eurojust study, during the COVID-19 pandemic, two main problems arise (Eurojust, 2021b, 15):

- *Cases involving the transmission of requests for MLA and the results of their execution.* Requests for MLA normally are submitted via postal services. However, during the COVID-19, the functioning of standard postal services was severely affected or suspended. To mitigate the issue, jurisdictions had the possibility to submit the requests for MLA via their diplomatic representations (via diplomatic courier). However, using the diplomatic channels often takes considerably longer. Another possibility to mitigate the issue is submitting requests for MLA electronically. However, in either case central authorities should assess and reprioritise their work to include the priorities resulting from the emergency.
- *Cases concerning the hearing of persons, including hearing by videoconference.* During the COVID-19 pandemic, obtaining oral evidence was not possible due to lockdowns and movement restrictions. To overcome such challenges, jurisdictions sought to obtain evidence through videoconferencing, where permissible under the legislation of the requested jurisdiction and with a suitable treaty basis.

These issues may impede international co-operation during other emergencies as well. Another factor relevant to the execution of MLA requests relates to in-person co-ordination meetings between requesting and requested jurisdictions. During an emergency, the challenge may be overcome through the use of virtual conference facilities. These enable jurisdiction to reduce costs associated with travel and time needed to participate in meetings. However, virtual conferences remain a mitigating factor when dealing with MLA, which benefit from in-person meetings that allow requesting and requested authorities to better understand the assistance sought and build trust.

### *Extradition*

Extradition is the formal process by which one jurisdiction asks another for the enforced return of a natural person who is in the requested jurisdiction and who is accused or convicted of one or more criminal offences against the law of the requesting jurisdiction. It is one of the oldest forms of international co-operation. However, challenges arise in the surrender of natural persons during emergencies.

The possibility of extraditing a natural person if there is no direct border between the requesting and requested jurisdiction may be limited. This may be due to the impact of the emergency in the requesting or requested jurisdictions, or in a third jurisdiction that the person being surrendered must transit. By way of example, during the COVID-19 pandemic, air traffic came to a standstill, resulting in the postponement of extraditions even in cases where the arrest of the sought person was time-barred. In such cases, and depending on established priorities, consideration should be given to charting special flights to enable the surrender of the natural person to the requesting jurisdiction. However, given the costs involved, the requesting and requested jurisdictions may wish to consider co-ordinating several requests for extradition to allow for several persons to be transported simultaneously on such chartered flights.

### Box 5.5. Case study Nigeria – adjusting operational aspects of the central authority during the COVID-19 pandemic

The central authority of Nigeria was forced to stop its activities during the lockdown phase of the COVID-19 pandemic in Nigeria. However, once the lockdown was relaxed, the central authority continued working virtually. This allowed it to participate in the drafting of a standardised set of guidelines for West Africa in 2021.

At the operational level, the central authority of Nigeria adjusted its procedures in light of the restrictions imposed by the COVID-19 pandemic. Thus, some extradition hearings were carried out through online platforms. In some instances, during confinement, it was easier for the Nigerian authorities to locate fugitives due to their increased use of telephone services that made them easier to track.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

### *Conflicts of jurisdictions, ne bis in idem and transfer of procedures*

*Jurisdiction* is the general power of a State to exercise authority over persons and things within its territory and to decide and impose decisions within its territory. Due process, therefore, enables the legitimate exercise of jurisdiction by the State (Magalhães, 1999, 47; Cintra et al., 2005, 139). National legislation normally includes principles regulating the basis of criminal jurisdiction, e.g. personal, territorial, and universal. Due to the unavoidable overlaps of these principles, multi-jurisdictional cases inherently carry the possibility of conflicts of jurisdictions.

A conflict of jurisdiction can either be *positive*, i.e. when two or more States claim their right to investigate and prosecute the same alleged offence (the same facts and perpetrators), or *negative*, i.e. when two or more States refuse to take on a certain case on the grounds of their lack of authority over it. These practical guidelines focus on *positive conflicts of jurisdiction*, which are the source of several relevant problems in terms of international co-operation.

Circumstances that can trigger positive conflicts of jurisdiction include: (i) different national laws, which include provisions that extend the jurisdiction to crimes committed outside their physical boundaries (e.g. active nationality principle, passive nationality principle), and (ii) transnational criminal organisations and networks that commit crimes that has connections to various jurisdictions.

Positive conflicts of jurisdiction become more frequent with transnational crime and globalisation in general. Multiple prosecutions carried out at the same time can affect the efficiency and duration of the respective proceedings and be detrimental to the rights and interests of the individuals involved. A proper and more efficient administration of justice requires reducing redundancy in investigations and prosecutions, and to avoid situations of duplicated efforts and wasting resources.

As a connected issue, criminal proceedings running parallel in multiple jurisdictions may create *ne bis in idem* situations. The *ne bis in idem* principle prohibits the duplication of proceedings and penalties of a criminal nature for the same acts and against the same person (Eurojust, 2020, 3).

To resolve conflicts of jurisdictions and avoid *ne bis in idem* claims to emerge, the jurisdictions involved should communicate with each other at the earliest possible stage of their investigations. Exchange of information on the existence of the cases, consultation to determine the links between the investigations, co-ordination of investigative steps, establishing close co-operation, and establishing joint investigation teams are the proper way of deconflicting.

Only as the result of proper co-ordination and co-operation can the involved jurisdictions determine the place best suited to prosecute the whole or defined parts of the case. The consultation of the parties can lead to agreements on the transfer of criminal procedures in order to avoid parallel proceedings, overlaps or contradictions in the cases.

During emergencies the possibilities of proper communication and consultation, as well as the carrying out the actual transfer of evidentiary material might be impeded. A solution, which would be feasible during normal times might not result in the proper administration of criminal justice. Thus, jurisdictions should use the available channels of communication and exchange of information[60] to determine the best course of action, taking into account the limitations caused by the emergency.

## Parallel, joint investigations and multi-jurisdictional cases

### Guidance 25. Parallel, joint investigations and multi-jurisdictional cases

**For law enforcement authorities:**

- Evaluate the necessity and scope of international co-operation in cases involving multiple jurisdictions, especially the mutual exchange of information and evidence, co-ordination of investigative steps and measures and considering closer co-operation in the form of parallel or joint investigation.
- Contact their foreign counterparts as soon as possible to clearly explain the urgency of the case, e.g. its priority during an emergency. To promote co-operation consider establishing direct contacts via the different LEA and judicial co-operation platforms.
- Organise co-ordination meetings among the members of parallel or joint investigations through secure online communication channels.

Corruption-related offences have increasingly become transnational. There is, therefore, an increasing need for jurisdictions to rely on international co-operation to effectively investigate and prosecute corruption cases. To enforce their criminal laws, one jurisdiction must rely on other jurisdictions to enforce their laws against perpetrators that operate extraterritorially (Boister, 2015, 11).

In everyday or emergencies, Cross-border corruption and corruption-related offences, e.g. money laundering, are often investigated by the affected jurisdictions in an uncoordinated manner. These investigations usually are factually linked and may run parallel to each other. However, the evidence obtained in one investigation likely is relevant to another to establish the relevant facts for each of them. The absence of proper communication among law enforcement authorities of the affected jurisdictions, therefore, risks negatively impacting each other, leading to, among others, the loss of evidence, incomplete outcomes and contradicting results.

Successfully investigating cross-border offences requires communication, co-operation and co-ordination among the affected jurisdictions. Law enforcement and judicial networks[61] are crucial in identifying the links between existing and prospective investigations. The correlation between facts, persons of interest in an investigation, or the instrumentalities or proceeds of crime used in, generated by or resulting from the commission of corruption or its ancillary offences among the affected jurisdictions allows them to co-ordinate their investigative steps better. Moreover, it allows them to

60 See section Law enforcement and judicial co-operation platforms of these practical guidelines.

61 See section Law enforcement and judicial co-operation platforms of these practical guidelines.

streamline their needs to exchange information, collect evidence or take action to prevent the dissipation of the proceeds of crime.

The nature of cross-border investigations and the level of trust among law enforcement authorities also help inform whether the affected jurisdictions will co-ordinate parallel investigations or pursue joint investigations, where closer co-operation is required.

*Parallel investigations* mean investigating facts that constitute a criminal offence in the involved jurisdictions simultaneously. Initiating parallel investigations allows for combining the investigative expertise from the involved jurisdictions to complement the efforts of each other. Under Recommendation XIX(C)(i) of the 2021 Anti-Bribery Recommendation (OECD, 2022b), in multi-jurisdictional cases, the OECD encourages the Member countries to the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (OECD, 2011b) (OECD Anti-Bribery Convention) to engage in direct co-ordination in parallel investigations and prosecutions, including through the sharing of information and evidence.[62]

*Joint investigations* blend law enforcement and judicial co-operation. They are an effective and enhanced form of international co-operation in criminal matters. They have the unique possibility of allowing the affected jurisdictions forming joint investigation teams (JITs) to co-ordinate investigative strategy and measures, share the workload and the costs of the investigation. Additionally, since the parties to the joint investigation are not tied to requests for mutual legal assistance (MLA),[63] they can act in their full investigative capacity, thereby reducing the attached bureaucracy considerably. Recommendation XIX(C)(v) of the 2021 Anti-Bribery Recommendations requires the Member countries of the OECD Anti-Bribery Convention to consider setting up joint or parallel investigative teams when conducting investigations and prosecutions that may necessitate co-ordinated and concerted action with one or several other member countries (OECD, 2022b).

International treaties dealing with international co-operation generally have provisions for setting up JITs, e.g. art. 9 of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988 Vienna Convention) (UNODC, 1988), art. 19 of the United Nations Convention against Transnational Organised Crime (UNTOC) (UNODC, 2001), art. 49 of the United Nations Convention Against Corruption (UNCAC) (UNODC, 2003), art. 20 of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS 182) (CoE, 2001b) and art. 13 of the EU Convention on Mutual Assistance in Criminal Matters Between the Member States of the European Union (Union, 2000).

During emergencies, the activities of JITs can be impacted by, e.g. lack of personnel and other resources or travel limitations. It includes having to postpone joint investigative actions and the overall progress of the investigations or delaying the setting up of JITs (Eurojust, 2021b, 4 and 17). To mitigate these challenges, a secure communication platform can be established to enable JIT members to continue co-ordinating their activities and the next steps of their investigations without face-to-face meetings (Eurojust, 2021b, 17). Despite the limitations imposed by the COVID-19 pandemic, there are examples that law enforcement authorities were able to accommodate their practices and continue co-operating in JIT framework.

62 See section Parallel, joint investigations and multi-jurisdictional cases of these practical guidelines.

63 See section Mutual Legal Assistance of these practical guidelines.

### Box 5.6. Poland/Ukraine case study – foreign bribery related to the State Road Agency of Ukraine (Ukravtodor)

Between October 2016 and October 2019, companies from Poland, Turkey and Ukraine allegedly bribed the head of the State Road Agency of Ukraine (Ukravtodor), who is a Polish and Ukrainian national. The bribes totalled approx. EUR 1 million in exchange for road construction contracts. The proceeds of the bribery and their laundering were handled by a multilevel criminal organisation lead by the corrupt official.

The law enforcement and prosecutorial authorities of Poland detected the case via special investigative techniques[64] in 2018, the investigation started in January 2019. In Ukraine the investigation started in mid-2019 based on discrepancies discovered between the official's income and spendings.

After initial contact and exchanges of information, the law enforcement agencies realised that they are working on closely linked cases, and after personal consultation they decided to establish a Joint Investigation Team (JIT) involving the prosecutors and investigators on both sides.

The JIT agreement enabled the partners to share the workload, communicate on designated channels, co-ordinate their investigations and exchange information and admissible evidence directly and real-time, also in electronic form. The JIT agreement also alleviated the bureaucratic process of MLA exchange. Due to the COVID-related restrictions, in-person contacts of the JIT were limited, with only several offline meetings held. Nevertheless, the investigative steps were synchronised, and in July 2020 the Polish and Ukrainian law enforcement authorities executed a simultaneous operation of searches, arrests and seizure of assets.

As the result, both the active and passive side of bribery has been identified and the criminal organisation collecting bribes and laundering its proceeds was dismantled.

In July 2020, 16 individuals were charged in Poland for several crimes, including active foreign bribery. One individual was convicted for money laundering and complicity in passive foreign bribery. The individual, after entering into a negotiated settlement with the Polish authorities, was sentenced to three years' imprisonment – suspended for five years – and a fine of approx. EUR 12 564. Another individual also negotiated a settlement with authorities and was sentenced also for three years imprisonment – suspended for five years – and a fine of approx. EUR 26 700 and forfeiture of property worth EUR 330 000.

The remaining proceedings for foreign bribery and other charges are ongoing at the time of publication.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project and {OECD, 2022, #192 296@67-68}

64 See section Special investigative techniques of these practical guidelines.

### Box 5.7. Denmark/Mauritius case study – foreign bribery related to a power plant project

The case concerns a power plant project in Mauritius and involves a Danish contractor and a Mauritian State-Owned Entity SOE. The Danish contractor allegedly bribed public officials of Mauritius regarding the redevelopment of a power plant in Mauritius. An IFI financed the project.

In Denmark, a whistleblower[65] first reported the allegations to the Danish contractor in April 2018. The Danish contractor ordered an external investigation, dismissed the involved employees, reported two persons to the Danish Police and self-reported[66] the matter to the IFI and other relevant stakeholders.

In 2020, the IFI's investigation found that the Danish contractor engaged in fraudulent and corrupt practices in the context of the project.

In Mauritius, the Independent Commission Against Corruption (ICAC) initiated its investigation following press articles and a referral by the IFI to Mauritian authorities. Informal knowledge sharing between ICAC and the State Prosecutor for Serious Economic and International Crime (SOIK) of Denmark followed. Mauritius then sent a request for MLA to Denmark. The ICAC and SOIK established a joint investigation team. The collaboration included an exercise by both agencies where evidence was extracted forensically from technological devices which provided important leads for the progress of the investigations. In September 2021, Mauritian law enforcement agencies arrested several natural persons associated with the Danish company, a local subcontractor, a former energy minister, engineers in SOEs and managers of the Central Procurement Board. The ICAC investigation has identified illicit flows of funds to two countries in the Indian Ocean and Asia and has accordingly engaged in informal co-operation with these two jurisdictions. The investigation is presently examining the role played by the international consultant in favouring the Danish contractor.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project and OECD, 2023, 86.

## Asset recovery

### Guidance 26. Asset recovery

**For law enforcement authorities:**

- Discuss the most effective manner of implementing requests seeking to seize or confiscate assets, particularly concerning their management during emergencies.

In cross-border corruption cases, asset tracking and asset recovery also require intensive international co-operation. The secured criminal assets might be linked to conducts in multiple jurisdictions and subject to overlapping claims. Asset sharing, repatriation of stolen goods and potential damage claims justify intense communication and co-operation of the involved countries' law enforcement agencies.

One of the issues during the COVID-19 pandemic related to the ability of jurisdiction to manage seized assets pending a final decision on their confiscation, restitution to the previous owner or to potential victims.

65 See section Information from whisleblowers/reporting persons of these practical guidelines.

66 See section Self-reporting of these practical guidelines.

In turn, the return of corruption-related proceeds of crime requires a partnership between the jurisdictions involved. During the return phase, the jurisdictions must discuss the best way to return the assets and how to implement control measures that foster transparency and accountability. However, an emergency situation such as the COVID-19 pandemic may restrict the ability of authorities of the jurisdictions involved to meet and initiate discussions on the return of the confiscated assets.

Moreover, during an emergency, the return of corruption-related proceeds of crime faces additional challenges. Implementing control measures may be limited due to the restrictions imposed by the emergency. Thus, jurisdictions should find innovative solutions, e.g. the returned assets put to alleviate the impact of the emergency (Marsh, 2020).

### Box 5.8. South Africa case study – *Tenderpreneurs*

The case was detected via a social media post whereby an individual had boasted about buying luxury vehicles with cash, which raised alerts with car dealers and banks, given the limited businesses that were open and the difficult economic conditions.

Consistent with the Fusion Centre (see Box 3.6. South Africa case study – the ) operational pillars, members of SAMLIT, FIC and law enforcement authorities initiated an analysis into possible misconduct. This analysis confirmed that the individual was linked to several entities that had been awarded tenders valued at millions of ZAR from a National Health entity of the government.

Subsequently, law enforcement opened a full investigation and found that 34 bank accounts were used. The individual and entities controlled by the individual had received funds from public tenders. Immediately after the award of a tender, money was quickly forwarded into accounts controlled by the individual, related entities or associates. The investigation later established that these other entities that received funds had received kickbacks from the individual as part of this *tenderpreneur* scheme. Moreover, the investigation showed that the individual used other persons and businesses to conceal the source and nature of funds and evade the national debarment list, as one of the entities used by the individual was debarred. The law enforcement authorities also found that a senior government official from the National Health entity played a role in the scheme and was responsible for allocating the contract.

As a result of the support and information provided by SAMLIT, the Fusion Centre, and financial institutions, the Revenue Service was able to obtain preservation orders and recovered assets consisting of properties, vehicles and ZAR 60 million (based on the taxes outstanding). In parallel, it was possible to determine that the individual had not been tax compliant for several years, which led to the opening of a separate tax investigation. In addition to the main subject, the senior public official and the subject's fiancée were arrested for fraud and theft in contravention of the Public Finance Management Act.

Source: Peer learning activities, Law Enforcement Response to Corruption in Emergencies Project

# Annex A. Guidance on law enforcement response to corruption in emergencies

***Changes to operational practices***

## Guidance 1. Changes to operational practices

For governments:

- Elaborate a risk assessment specific to corruption during the emergency, to map out risks and the respective mitigating measures.
- Evaluate the law enforcement system and allocate resources to prioritise investigative and prosecutorial work based on the risk assessment.

For law enforcement authorities:

- Review case prioritisation to ensure it is aligned with the emergency-related risks.
- Develop guidelines on the use of new technological solutions, such as remote interviewing, to execute procedural steps during emergencies.
- Modify working regimes to ensure the continuity of the operation and introducing necessary protection measures for staff members if required by the nature of the emergency.

**Source*s of detection***

## Guidance 2. Criminal intelligence

For law enforcement authorities:

- Review their processes for gathering human intelligence to minimise the risks arising from the emergency while ensuring the safety of their officers and human intelligence assets.
- Use technological solutions to obtain human intelligence while minimising face-to-face interaction and ensure the safety of their informants and co-operating witnesses.

## Guidance 3. Financial intelligence

For law enforcement authorities:

- Request FIUs to prepare strategic analyses that guide the emerging patterns of criminality resulting from the emergency and use it for adapting detection practices.
- Routinely utilise operational analyses prepared by FIUs as a source of information to better detect the commission of corruption and its ancillary offences during an emergency.

### Guidance 4. Information received through other inter-agency co-operation

For governments:

- Identify and resolve legal, regulatory or operational challenges that institutions may encounter when collaborating.

For law enforcement authorities:

- Identify the public institutions that may possess and share emergency-related information potentially useful for detection purposes.
- Verify whether existing inter-agency platforms may be used or repurposed to deal with the emergency or establish a specific inter-agency platform to deal with the emergency.

### Guidance 5. Co-operation with Information from tax authorities

For governments:

- Include tax authorities in any inter-agency co-operation mechanism to detect, investigate and prosecute corruption-related offences arising from emergencies.
- Discuss, identify and agree on the detection and investigation objectives of tax authorities and law enforcement to fully explore synergies between them.

### Guidance 6. Co-operation with Information from supreme audit institutions

For law enforcement authorities:

- Examine the results of audits of emergency-related funds without delays.
- Hold consultations with SAIs with respect to the features of the allocation and disbursement of emergency funds and respective risks, and the possibilities to initiate audits of certain programmes/projects.

### Guidance 7. Public procurement information

For governments:

- Ensure that law enforcement agencies have access to continuous, timely, accurate and verifiable information regarding government expenditures arising from the emergency.

For law enforcement authorities:

- Focus their analytical efforts on the examination of emergency-related public procurement procedures.

### Guidance 8. Asset disclosure

For governments:

- Prioritise the verification of asset declarations of public officials who work in the risk areas dealing with mitigating the consequences of the emergency.
- Seek technological solutions to receive and process asset disclosures from public officials to limit face-to-face interactions.

### Guidance 9. Information from investigative journalists, media and social media platforms

For law enforcement authorities:

- Take steps to proactively monitor the media and use it as a source of detecting corruption.
- Take steps to enhance co-operation with the media for the purposes of receiving timely information on alleged corruption and proper follow-up.

### Guidance 10. Information from whistleblowers/reporting persons

For governments:

- Raise awareness about the existing whistleblowing and reporting mechanisms afforded by law enforcement authorities and other relevant agencies to help detect corruption-related offences.
- Update legislation to ensure it envisages adequate protection to public and private sector whistleblowers/reporting persons.
- Develop technologies that allow the public to submit complaints in anonymised, electronic channels that can be collected and analysed by law enforcement.

For law enforcement authorities:

- Establish reporting channels enabling the public to make complaints or report suspected corruption- allegations related to the emergency.

For private sector actors:

- Raise awareness among private sector employees the complaint, reporting and whistleblowing mechanisms available to them to report suspicions of corruption.

### Guidance 11. Information from the private sector actions

For private sector actors:

- Update their internal controls regarding the direction and supervision of auditing teams.
- Conduct self-assessment and anti-corruption compliance audits to minimise corruption-related risks in their supply chain and day-to-day business.

### Guidance 12. Integrity testing

For governments:

- Consider implementing targeted integrity testing for public officials who work in the risk areas dealing with mitigating the consequences of the emergency.

***Investigation and prosecution***

### Guidance 13. Open-source intelligence and data collection

For law enforcement authorities:

- Establish specific methods and guidelines applied to OSINT and data collection by defining their purpose for the investigation and establishing the sources, identifiers and datasets that will be used during an emergency.

- Validate and verify the information obtained through OSINT and data collection by collecting them from different sources, where possible.
- Avoid selection bias of the information collected through OSINT and data collection by having it verified by more than one person.
- Take steps to ensure that the information collected through OSINT and data collection is retraceable.
- Minimise the digital footprint of law enforcement personnel, especially those tasked with OSINT investigations.

### Guidance 14. Electronic evidence

For law enforcement authorities:

- Enter into or reviewing existing MOUs with OSPs to address the challenges and identified risks during an emergency to ensure the retention of electronic evidence.

### Guidance 15. Special investigative techniques (SITs)

For law enforcement authorities:

- Conduct assessment pertaining to their SITs, to ensure their relevance regarding priority investigations while balancing it with the safety of law enforcement staff during emergencies, and adjusting the SIT practice accordingly.
- Establish access to and receive information from newly created emergency-related databases for proper SIT planning.

### Guidance 16. Forensic expertise

For law enforcement authorities:

- Identify the forensic expertise required during the investigation planning stage, e.g. forensic auditing, preserving, collecting and reviewing electronic evidence, while taking into account the nature of the emergency and related corruption offences.
- Hire *ad hoc* forensic experts related to the specific risks and typologies generated by the emergency situation, in particular when such expertise is neither available in-house nor at a partner agency.
- Share expertise with domestic and foreign partners regarding emergency-related investigations and prosecutions and learn about any forensic expertise programmes that foreign partners may have to support ongoing investigative and prosecutorial action during an emergency.

### Guidance 17. Identifying subjects – natural and legal persons

For governments:

- Establish and make available, at a minimum to law enforcement authorities, access to databases indicating beneficial ownership information of registered legal persons and legal entities.
- Take steps to provide and maintain an up-to-date lists of politically exposed persons (PEPs) accessible, at a minimum, to law enforcement authorities.

### Guidance 18. Pre-trial and trial proceedings

For governments:

- Assess the impact of the emergency on pre-trial and trial proceedings and identify mitigating measures while preserving the rule of law and the right to a fair trial.
- Enable courts to conduct proceedings virtually during an emergency, to ensure business continuity.
- Take steps to digitalise cases and upgrade court management systems to enable court filings, the storage and transfer of information and evidence in digital format.
- Suspend or extend procedural timelines and even statutes of limitation to allow for proper investigation and prosecution of alleged corruption cases.

### Guidance 19. Co-operating witnesses, plea agreements and non-trial resolutions. Witness protection

For governments:

- Establish a comprehensive legal framework to enable witness co-operation, plea agreements and non-trial resolutions in corruption cases.
- Provide dedicated resources for law enforcement to ensure the continuity of ongoing co-operation agreement-based procedures.
- Ensure that witness protection programs have suitable funding to continue operating during emergencies.

For law enforcement authorities:

- Issue guidelines for investigators and prosecutors about identifying suitable cases and apply the co-operation agreements effectively.
- Encourage meetings with co-operating witnesses, co-operating perpetrators and defence counsels through secure telecommunication or videoconferencing facilities.

### Guidance 20. Freezing, seizure and confiscation

For governments:

- Ensure that the seizure and confiscation regime is effective to deal with the specific corruption-related risks identified during the emergency, and is applied in practice.

### Guidance 21. High-profile corruption

For governments:

- Establish or strengthen existing specialised anti-corruption law enforcement and judicial authorities.
- Strengthen the external independence of law enforcement and judicial authorities dealing with high-profile corruption cases and the internal independence of investigators and prosecutors working on such cases.
- Provide adequate resources to law enforcement and judicial authorities dealing with high-profile corruption cases to enable them to conduct their procedure independently from other agencies.

- Review the legal framework of public immunities with the view of ensuring that immunities do not pose an obstacle to effective investigation and prosecution of high-profile corruption cases.

For law enforcement authorities:

- Review their communication and public relations strategies to be able to counter illicit pressure and influencing attempts.
- Strengthen internal guidelines and procedures to safeguard investigators and prosecutors from potential pressure via disciplinary or labour law related decisions of the management.

### Guidance 22. International financial institutions' integrity and investigation units

For law enforcement authorities:

- Enter into MoUs with IFIs in cases involving IFI-funded projects to help expedite investigations and facilitate information sharing.

### Guidance 23. Law enforcement and judicial co-operation platforms

For law enforcement authorities:

- Strengthen the use of law enforcement and judicial co-operation platforms as a mechanism to verify and confirm lines of inquiry in investigations, prior to the submission of requests for MLA.
- Use the secure communication channels provided by law enforcement and co-operation platforms to communicate, and transfer information and evidence.
- Designate points of contacts to the law enforcement and judicial co-operation platforms that they are party to.

### Guidance 24. Mutual legal assistance and extradition, conflict of jurisdictions

For governments:

- Accept requests for MLA and extradition submitted solely via electronic channels.
- Enable the hearing of persons to be conducted via videoconferencing facilities.
- Identify alternative travel methods, e.g. chartering flights, to secure the surrender of natural persons when the requesting and requested jurisdictions do not share a direct border.

For law enforcement authorities:

- Process incoming and outgoing requests for MLA dealing with issues arising from the emergency as a priority.
- Hand over documents or requests to the liaison officer at the embassy of the jurisdiction involved, as a method of delivery of requests for international co-operation.
- Assess the impact that the emergency has on resolving conflicts of jurisdictions and negotiate solutions that ensure the proper administration of justice.

### Guidance 25. Parallel, joint investigations and multi-jurisdictional cases

For law enforcement authorities:

- Evaluate the necessity and scope of international co-operation in cases involving multiple jurisdictions, especially the mutual exchange of information and evidence, co-ordination of

investigative steps and measures and considering closer co-operation in the form of parallel or joint investigation.

- Contact their foreign counterparts as soon as possible to clearly explain the urgency of the case, e.g. its priority during an emergency. To promote co-operation consider establishing direct contacts via the different LEA and judicial co-operation platforms.
- Organise co-ordination meetings among the members of parallel or joint investigations through secure online communication channels.

### Guidance 26: Asset recovery

For law enforcement authorities:

- Discuss the most effective manner of implementing requests seeking to seize or confiscate assets, particularly concerning their management during emergencies.

# Annex B. Training curriculum for law enforcement practitioners on combatting corruption in emergencies

This annex provides training curricula for the different components of the guidelines for law enforcement responses to corruption in emergency situations. It understands the term *training curriculum* as a set of guidelines to help training centres and initiatives decide on the content of a respective training course for law enforcement officials and develop its syllabi and study plans.

The training curriculum below is recommendatory. It suggests the course content, objectives and methodologies. It also indicates the subordination of areas for a more effective training. This annex provides four training curricula: curricula for the three main topics of the guideline, i.e. sources of detection, investigation and prosecution, and international co-operation and a curriculum for a simulated case-based training.

The proposed division ensures flexibility on the training needs of the target audience. It enables the relevant stakeholders either to consider individual, targeted training on one or more topics comprised in the guidelines, or to immerse different topics into a practical, case-based scenario to simulate an investigation during emergency situations.

## Training on sources of detection of corruption-related offences in emergency situations

## Description

Detecting the crime is the first step and challenge to any effective law enforcement and prosecutorial action against corruption-related offences.[67] Detection relies on a systematic method of collecting, assessing and prioritising information into practical intelligence and turning them into admissible evidence through investigation. While information available from traditional sources is still valid and relevant for detection purposes, new sources of information can be identified based on how the flow of information is evaluated, analysed and disseminated. The analytic work establishes connections and transforms pieces of information into valuable intelligence.

The Practical Guidelines took into consideration additional sources of detection, e.g. integrity testing, accounting and audit, but since during the research phase no relevant cases were encountered, those are not covered in the training curriculum in details.

## Purpose, objective(s) and expected result(s)

The training on sources of detection aims at presenting the participants with the different sources of information available to assist them in detecting corruption-related offences. It discusses the challenges brought to the detection of corruption-related cases during emergency situations and provides good practices to overcome those challenges.

The **general objectives** of the training in sources of detection:

1. To present to the participants the different sources of information available to them to detect corruption-related cases more effectively.
2. To demonstrate the importance of inter-agency co-operation, and co-operation with the private sector, to detect corruption-related cases more effectively.
3. To present the importance of whistleblowers (or reporting persons) and investigative journalism as a reliable source of information for the detection of corruption-related cases.
4. To learn and discuss the challenges presented by emergency situation in the detection of corruption-related cases and learn good practices to overcome those challenges.

67 The training curriculum understands *corruption-related offences* to include those defined in the OECD Anti-Bribery Convention and mandatory and non-mandatory offences defined in other international standards, e.g. the United Nations Convention Against Corruption (UNCAC).

The expected results are:

1. Training 25-35 participants per training session and per area (cluster)[68] on the sources of detection of corruption-related offences.
2. Understanding the different sources of information available to law enforcement and prosecutor to detect corruption-related offences.

## Target audience

Primary audience (recommended):

- Law enforcement officials
- Prosecutors
- Financial analysts
- Criminal analysts
- Intelligence officers

Secondary audience (optional):

- Tax authorities
- FIU officers
- Public officials responsible for review and verification of asset disclosures, public procurement processes
- Auditors in supreme audit institutions
- Investigative journalists
- Private sector (accountants, external auditors and compliance officers)

## Duration

- Up to 1 day for each of the areas indicated in the training curriculum, based on the level of knowledge and proficiency of the participants, established through pre-testing.

68 Depending on the duration of the training session.

- 4-5 days when combining all the areas indicated in this part of the training curriculum, based on the level of knowledge and proficiency of the participants, established through pre-testing.

## Delivery

On-site (preferable) or online.

## Assessment

- **Pre-testing:** whereby the selected participants apply to an online multiple-choice test to assess the groups general knowledge on the subject matter of the specific course. This will help the trainer to establish the depth and breadth of the training provided for each of the areas described in of the areas outlined in the training curriculum (Section 2.7 below).
- **Post-testing:** whereby the selected participants apply to the same multiple-choice test provided as the pre-test to establish whether knowledge has been enhanced in the specific area.
- **Reporting:** Whereby the trainer provides an end-of-training report, describing the results, challenges and next steps.

## Training curriculum

| No. | Area | Contents | Methodology | Pre-requisite |
|---|---|---|---|---|
| 1.1. | Risk assessment | Understanding the importance of conducting risk assessments deriving from the emergency.<br>Implementing the risk assessment to map out the most corruption-prone areas and activities.<br>Evaluation and prioritisation of detection sources based on the risk assessment.<br>Identification and mitigation of risks to investigations and prosecutions in emergency situations. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention. | None |
| 1.2. | Criminal intelligence | Evaluation of source and data.<br>Basic analysis techniques, e.g. link analysis and flow analysis, inference development.<br>Limits to collection of criminal intelligence in emergency situations.<br>Adapting processes for gathering intelligence in the emergency situation.<br>Technology solutions to obtain human intelligence in the emergency | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention. | None |

| No. | Area | Contents | Methodology | Pre-requisite |
|---|---|---|---|---|
| | | situation. | | |
| 1.3. | Financial intelligence | FIU's risk-based assessment and analysis of the patterns of criminality arising from the emergency situation.<br>Forensic accounting and financial analysis techniques.<br>The confidential nature of financial intelligence and possible limits regarding its further use as evidence.<br>Electronic case organisation.<br>Limits to collection of financial intelligence in emergency situations. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention. | None |
| 1.4. | Inter-agency co-operation | Relevant agencies for the detection of corruption-related offences, their mandate, and the kinds of information they possess depending on the type of the emergency situation.<br>Legal, institutional, and technical conditions for efficient inter-agency co-operation.<br>Overcoming challenges in inter-agency sharing of information.<br>Features of access by law enforcement to the information in the possession of other institutions, technical solutions for providing remote access.<br>Challenges to inter-agency co-operation during emergency situations, and good practices for overcoming them. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice. | Areas 1.1 and 1.2. |
| 1.5. | Public procurement information | Understanding public procurement: importance, types and exceptions.<br>Risks to public procurement management and special/simplified procurement procedures during emergency situations.<br>Good practices to mitigate risks associated with procuring during emergency situations.<br>Access of law enforcement to public procurement data. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention. | Area 1.4. |
| 1.6. | Tax authorities information | Understanding the role of tax authorities in the detection of corruption-related offences.<br>Enhancing the detection of corruption-related offences through co-operation with tax authorities.<br>Limits of co-operation with tax authorities.<br>Challenges and risks associated with tax collection and tax investigations during emergency situations.<br>Good practices of co-operation with tax authorities during emergency situations to detect corruption-related offences. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice. | Area 1.4. |
| 1.7. | Supreme audit institutions (SAIs) information | Understanding the role and importance of SAIs in the detection of corruption-related offences.<br>Types of audits conducted by SAIs and their relevant to detecting | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in | Area 1.4. |

| No. | Area | Contents | Methodology | Pre-requisite |
|---|---|---|---|---|
| | | corruption-related investigations.<br>The impact on auditing during emergency situations, the change of the scope, priorities and approaches.<br>Good practices of co-operation between law enforcement and SAIs during emergency situations. | practice. | |
| 1.8. | Investigative journalism, media reporting and social media | Introduction to the principles and techniques of investigative journalism.<br>Oversight and co-operation of detection and investigation authorities by/with investigative journalism.<br>Examples of detecting corruption by journalists during emergency situations.<br>Considerations on obtaining and using information in social media.<br>Monitoring media by law enforcement for detection purposes. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention.<br>Interactive session featuring an open exchange with an investigative journalist(s) on the methods of collecting information and approaches to co-operating with law enforcement. | None |
| 1.9. | Whistleblowers | Defining a whistleblower.<br>Organisation of channels for reporting, including anonymously, special channels for reporting corruption in the emergency.<br>Understanding the importance of whistleblower protection in the private and public sectors.<br>Challenges to whistleblowing and whistleblower protection and reporting during emergency situations. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice. | Area 1.1. |

## Training on investigation and prosecution of corruption-related offences in emergency situations

## Description

Emergency situations pose additional challenges and obstacles to law enforcement and judicial authorities in conducting investigation and prosecution of corruption cases, on the legal, operational and technical level. To counter these and maintain control over the investigation and prosecution, law enforcement and prosecutorial authorities should design a well-made and proactive investigation strategy that establishes a clear methodology and investigative plan that builds upon initial allegations leading to the successful conduct of investigations.

## Purpose, objective(s) and expected result(s)

The training on investigation and prosecution aims at providing the participants with an understanding of the mechanisms available to them to investigate and prosecute corruption-related offences, including high-level corruption. It discusses the challenges brought to investigations and prosecutions during emergency situations and provides good practices to overcoming those challenges.

The **general objectives** of the training on investigation and prosecution are:

1. To provide the participants with understanding and knowledge on the challenges brought by emergency situations and how to adapt their investigation and prosecution procedures.
2. To learn the different mechanisms available when investigating and prosecuting corruption-related cases, their impact on investigations and prosecutions, and the limitations they may have during emergency situations.

The expected results are:

1. Training 25-35 participants per training session and per area (cluster)[69] on investigation and prosecution of corruption-related offences, including high-profile corruption.
2. Understanding the tools and procedures available to investigators and prosecutors and how an emergency situation may impact them.

## Target audience

Primary audience (recommended):

- Law enforcement officials
- Prosecutors

Secondary audience (optional):

- Intelligence officers
- Criminal analysts
- Financial analysts

69 Depending on the duration of the training session.

## Duration

- Up to 1 day for each of the areas indicated in the training curriculum below, based on the level of knowledge and proficiency of the participants, established through pre-testing (see sub-section under assessment below).
- 3-4 days when combining all the areas indicated in this part of the training curriculum below, based on the level of knowledge and proficiency of the participants, established through pre-testing (assessment section, below)

## Delivery

On-site (preferable) or online.

## Assessment

- **Pre-testing:** whereby the selected participants apply to an online multiple-choice test to assess the groups general knowledge on the subject matter of the specific course. This will help the trainer to establish the depth and breadth of the training provided for each of the areas described in of the areas outlined in the training curriculum (Section on training curriculum, below).
- **Post-testing:** whereby the selected participants apply to the same multiple-choice test provided as the pre-test to establish whether knowledge has been enhanced in the specific area.
- **Reporting:** Whereby the trainer provides an end-of-training report, describing the results, challenges and next steps.

## Training curriculum

| No. | Area | Contents | Methodology | Pre-requisite |
|---|---|---|---|---|
| 2.1. | Development of an investigative strategy | Identifying potential targets (natural persons, legal persons, assets).<br>Developing investigative theory.<br>Choosing investigative methods, prioritisation of investigative actions.<br>Circumstantial evidence.<br>Ensuring adequate resources for the case.<br>Impact of emergency situations on the investigation process and respective adjustments to investigative | Presentations introducing topic, presenting content and formulating the problem.<br>Practical exercise based on a hypothetical case example(s) tasking the participants to develop their initial plans of investigations according to their theory of the case with considering an emergency situation. | |

| No. | Area | Contents | Methodology | Pre-requisite |
|---|---|---|---|---|
| | | strategies. | | |
| 2.2. | Open-source intelligence (OSINT) and data collection | Specific methods and guidelines applied to OSINT and data gathering. Assessing the reliability of data sources. Managing, collecting, storing, validating and disseminating OSINT.<br>OSINT databases/sources.<br>Technologies, software, and platforms used by law enforcement for OSINT and data collection.<br>Risks associated with OSINT. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention. | None |
| 2.3. | Electronic evidence | Understanding electronic evidence.<br>Collecting and storing electronic evidence.<br>Preservation of electronic evidence.<br>The impact and risk of digital footprint in the collection of electronic evidence. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice. | None |
| 2.4. | Special investigative techniques (SITs) | Defining SITs.<br>Understanding common types of SITs (controlled delivery, surveillance, telecommunications interception, undercover operations, etc.)<br>Impact of emergency situations in the deployment of SITs.<br>Ensuring the safety of law enforcement applying SITs in emergency situations.<br>Prioritisation of SITs that can be carried out in emergency situations. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice. | None |
| 2.5. | Forensic expertise | Defining forensic expertise.<br>Understanding the value of forensic expertise in corruption-related investigations.<br>Adding value to indirect methods of proof through forensic expertise.<br>Types of forensic expertise required for emergency-related investigations (e.g. forensic auditing to investigate financial losses, forensic analysis of medical devices etc. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice. | None |
| 2.6. | Identifying subjects: natural and legal persons | Differentiating legal ownership from beneficial ownership.<br>Understanding the main types of legal persons used to | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of | Area 2.2. |

| No. | Area | Contents | Methodology | Pre-requisite |
|---|---|---|---|---|
| | | conceal identity in corruption-related investigations.<br>Using beneficial ownership databases.<br>Accessing beneficial ownership.<br>Identification of natural persons.<br>Challenges to the identification of subjects during emergency situations. | knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention. | |
| 2.7. | Pre-trial and trial proceedings | Impact of emergency situations in pre-trial and trial proceedings.<br>Using technology solutions to overcome challenges brought by emergency situations (digitisation of investigation files and court proceedings, oral evidence by remote link, etc.).<br>Maintaining the relevance and reliability of evidence, storing and preserving it, and archiving electronic files. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice. | Areas 2.1., 2.4.-2.6. |
| 2.8. | Cooperating witnesses, plea agreements and non-trial resolutions. Witness protection | Understanding the categories of co-operating witnesses.<br>The impact of emergency situations in the collection of interrogating witnesses and collecting testimonies.<br>Methods of work with co-operating witnesses.<br>Plea bargaining, non-trial resolutions and other agreements with the prosecution. witness protection programmes. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention. | Areas 2.6. and 2.7. |
| 2.9. | Freezing, seizure and confiscation | Types of provisional measures available (freezing, seizure).<br>Types of confiscation measures available (asset-based confiscation, value-based confiscation, third-party confiscation, extended confiscation, non-conviction-based confiscation).<br>Considerations on when and how to apply provisional measures in a corruption-related investigation.<br>Impact of emergency situations on applying provisional measures and confiscation. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention. | Areas 2.2. and 2.7. |
| 2.10. | High-profile corruption | Defining politically exposed persons (PEPs).<br>High-profile corruption and independence of investigations.<br>High-profile corruption and political immunity (absolute and functional immunity). Impact of emergency | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising | Areas 2.6. and 2.7. |

| No. | Area | Contents | Methodology | Pre-requisite |
|---|---|---|---|---|
| | | situations leading to high-profile corruption.<br>Sensitivity of emergency-related cases and respective strategies (e.g. specialisation, public relations etc.). | it and enabling knowledge retention. | |

## Training on international co-operation of corruption-related offences in emergency situations

## Description

Corruption-related offences during an emergency situation and their investigations rarely are purely domestic. Law enforcement and prosecutors will need to obtain information and evidence from other jurisdictions routinely, e.g. communication from ISPs, financial data, beneficial ownership, or evidence substantiating self-reports by foreign companies. Most of these corruption-related cases and investigations cannot be solved without international co-operation due to the requirement of admissibility of evidence obtained from abroad, considering multinational legal entities, ancillary offences like money laundering, and asset recovery efforts. However, during an emergency situation, law enforcement and judicial co-operation faces considerable obstacles, as it was experienced e.g. during the COVID-19 pandemic.

## Purpose, objective(s) and expected result(s)

The training on international co-operation aims at providing the participants with an understanding on the different mechanisms available for exchanging information and collecting evidence with foreign counterparts. It further addresses the limitations in international co-operation during emergency situations and provides good practices to overcoming those limitations.

The **general objectives** of the training in international co-operation are:

1. To provide the participants with understanding and knowledge on international co-operation and exchange of information, including its tools and channels of communication.
2. To show the participants the limitations of international co-operation and exchange of information.
3. To learn the different mechanisms available in international co-operation and exchange of information, their purpose and their value to enquiries, investigations and prosecutions.

4. To understand the challenges faced in international co-operation and exchange of information during emergency situations.

The expected results are:

1. Training 25-35 participants per training session and per area (cluster)[70] on international co-operation of corruption-related offences in emergency situations.
2. Understanding when and how to use mechanisms for the international exchange of information and international co-operation, and their added value to national investigations.
3. Raising awareness and building capacities on the methods and channels for international co-operation, and the limits imposed by emergency situations.

## Target audience

- Law enforcement (operational and liaison officers)
- Prosecutorial authorities (operational and liaison magistrates)
- Focal points from regional and international networks.
- Staff from central authorities working on international co-operation.

## Duration

- Up to 1 day for each of the areas indicated in the training curriculum below, based on the level of knowledge and proficiency of the participants, established through pre-testing (see sub-section under Assessment, below).
- 3-4 days when combining all the areas indicated in this part of the training curriculum below, based on the level of knowledge and proficiency of the participants, established through pre-testing (see sub-section under Assessment, below).

## Delivery

On-site (preferable) or online.

70 Depending on the duration of the training session.

## Assessment

- **Pre-testing:** whereby the selected participants apply to an online multiple-choice test to assess the groups general knowledge on the subject matter of the specific course. This will help the trainer to establish the depth and breadth of the training provided for each of the areas described in of the areas outlined in the training curriculum below.
- **Post-testing:** whereby the selected participants apply to the same multiple-choice test provided as the pre-test to establish whether knowledge has been enhanced in the specific area.
- **Reporting:** Whereby the trainer provides an end-of-training report, describing the results, challenges and next steps.

## Training curriculum

| No. | Area | Contents | Methodology | Pre-requisite |
|---|---|---|---|---|
| 3.1. | International financial institution integrity and investigative units (IFI). | Understanding the role and function of IFIs.<br>Extent and limit of the investigations conducted by IFIs.<br>Co-operation between IFIs and national law enforcement and prosecutorial authorities.<br>Challenges faced by IFIs in their investigations during emergency situations.<br>Good practices to overcome the challenges faced by IFIs.<br>Collection by and evidence sharing between IFIs and law enforcement and prosecutorial authorities. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice. | None |
| 3.2. | Law enforcement and judicial co-operation platforms | Information sharing vs. collection of evidence.<br>Sharing information through law enforcement platforms.<br>Facilitating MLA through judicial co-operation platforms.<br>Existing law enforcement platforms at the regional and international levels (OECD LEO, GLEN and LENs, Interpol, ARINs, GlobE Network, etc.)<br>Existing judicial co-operation platforms at the regional and international levels (Eurojust, EJN, IberRed, etc.)<br>The role and function of the liaison officer. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention. | None |
| 3.3. | Mutual legal assistance and extradition | Understanding MLA and extradition.<br>Electronic vs. paper-based transmission of MLA request.<br>Channels of transmission of MLA requests (diplomatic, central authority, direct). | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice. | Area 3.2. |

| No. | Area | Contents | Methodology | Pre-requisite |
|---|---|---|---|---|
| | | The role and limits of the central authority.<br>Contents of MLA and extradition request.<br>Purpose, nature and object of MLA.<br>Limits of MLA (international treaty, national legislation of requested jurisdiction, etc.).<br>Drafting MLA requests.<br>Features of MLA in times of emergencies. | Practical exercises on drafting an MLA request. | |
| 3.4. | Parallel, joint investigations and multi-jurisdictional cases | Spontaneous transmission of information as a catalyst to parallel, joint and multi-jurisdictional cases.<br>Initiating parallel and multi-jurisdictional cases.<br>Establishing the objectives of parallel and multi-jurisdictional cases.<br>Determining the points of contact.<br>Sharing information and evidence in parallel and multi-jurisdictional cases.<br>Initiating and co-ordinating joint investigations.<br>Setting up joint investigation teams (JITs).<br>Powers and limitations of JITs.<br>Exchanging information and evidence through JITs.<br>Planning and co-ordinating operational activities.<br>Work of JITs in the circumstances of emergency. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention. | Area 3.2. |
| 3.5. | Asset recovery | Defining asset recovery and understanding the phases asset recovery process.<br>Understanding the difference between direct and indirect proceeds, and instrumentalities of crime.<br>Conducting financial investigations parallel to criminal ones.<br>Understanding the importance of inter-agency co-operation.<br>Determining beneficial ownership.<br>Conducting pre-seizure planning.<br>Seizing and confiscating proceeds and instrumentalities of crime.<br>Managing seized and confiscated assets. | Presentations introducing topic, presenting content and formulating the problem.<br>Case study presentation(s) showing the application of knowledge in practice.<br>Practical exercises for processing knowledge, generalising it and enabling knowledge retention. | Areas 2.9. and 3.2. |

## Simulated case-based training on detecting, investigating and prosecuting corruption-related offences in emergency situations

### Description

The training clusters described under points 2-4 may be complemented by an additional practical part that will simulate the investigation of a realistic large scale corruption case related to an emergency situation. Alternatively, this part may be integrated in the previous clusters and broken down into smaller components that will replace practical exercises under the respective areas.

Methodologically, it is based on a hypothetical case scenario whereby the participants, in 4-5 multi-agency groups, must investigate initial information provided to them. The practical case-based training has approx. 70-120 documents, shared with the participants as they progress with their simulated investigations. At certain milestones, the trainers provide thematic interventions targeting the core elements needed for an effective investigation and prosecution of corruption-related offences. At the conclusion of each stage of the investigation each group may be asked to present the results of their work on the case.

This cluster may also be followed by a 1.5 day's workshop on drafting an indictment. The final part of the case-based training may also include a moot court exercise with the involvement of judges who will hear the cases prepared by the groups.

### Purpose, objective(s) and expected result(s)

The simulated case-based training seeks to enhance the capacities of the participants in detecting, investigating and prosecuting corruption-related offences, including money laundering and high-profile corruption, related to emergency situations. While this simulated investigation will be conducted as a part of a regular criminal investigation, it may pay additional attention to conducting a parallel financial investigation aimed at identification, tracing and successful recovery of criminal assets.

The training through a simulated case-based scenario enables the participants to (i) raise their awareness in the entire detection, investigation and prosecution chain; (ii) enhance their capacities in detecting and investigating corruption-related offences, and (iii) apply the law effectively, strengthen their teamwork skills, and advance inter-agency co-operation. Moreover, because of the nature of the training, the case-based scenario can be created to address any type of emergency situation, thereby enhancing awareness and reaction from investigators and prosecutors.

The **general objectives** of the simulated case-based training are:

1. To provide the participants with the understanding and knowledge, and tools required to identify and investigate corruption-related offences during emergency situations.

2. To highlight the importance and added value of inter-agency co-operation to detect, investigate and prosecute corruption-related offences during emergency situations.
3. To link financial and criminal investigations, thereby cutting the illicit financial flows generated directly or indirectly from corruption-related offences.
4. To build capacities through a learning-by-doing methodology, by simulating a real-life case of corruption during an emergency situation.

The expected results are:

1. Training 25-35 participants per training session and per area (cluster)[71] on international co-operation of corruption-related offences in emergency situations.
2. Raising awareness and building capacities on the asset recovery process and its integration with other elements of detection, investigation and international co-operation.

## Target audience

The same as under points 2-4 depending on the areas covered.

## Duration

4-5 days.

## Delivery

On-site.

## Assessment

- **Pre-testing:** whereby the selected participants apply to an online multiple-choice test to assess the groups general knowledge on the subject matter of the specific course. This will help the trainer to establish the depth and breadth of the training provided for each of the areas described in of the areas outlined in the training curriculum.

71 Depending on the duration of the training session.

- **Post-testing:** whereby the selected participants apply to the same multiple-choice test provided as the pre-test to establish whether knowledge has been enhanced in the specific area.
- **Reporting:** Whereby the trainer provides an end-of-training report, describing the results, challenges and next steps.

## Training curriculum

The contents of a training are variable, depending on the modules added onto the training, with taking as a basis the selected topics of clues.

# References


Böhm, I. & Lolagar, S. (2021) Open source intelligence. *International Cybersecurity Law Review*, **2**, 317-337. http://dx.doi.org/10.1365/s43439-021-00042-7

Boister, N. (2012) *An Introduction to Transnational Criminal Law*. Oxford University Press,

Boister, N. (2015) The Concept and Nature of Transnational Criminal Law. In *Routledge Handbook of Transnational Criminal Law,* (Eds, Boister, N. & Currie, R.J.) Routledge, pp. 11-26.

Brown, S.D. (2007) The Meaning of Criminal Intelligence. *International Journal of Police Science & Management*, **9**, 336-340. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=22b7483e22e2d6bf992e23c35d0defa16b13cc45

Brun, J.-P. et al. (2022) *Taxing Crime: A Whole-of-Government Approach to Fighting Corruption, Money Laundering, and Tax Crimes*. World Bank, Washington, DC. https://doi.org/10.1596/978-1-4648-1873-8

CARIN Secretariat Camden Asset Recovery Inter-Agency Network. https://www.carin.network

Carter, D.L. (2009) *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. USDOJ Office of Community Oriented Policing Services, Washington, DC. https://irp.fas.org/agency/doj/lei.pdf

Cintra, A.C.D.A., Grinover, A.P. & Dinamarco, C.R. (2005) *Teoria Geral do Processo*. Malheiros, São Paulo.

CoE (2001a) European Convention on Cybercrime. **ETS 185 of 23 November 2001,** https://rm.coe.int/1680081 561

CoE (2001b) Explanatory Report to the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce57

CoE (2005) Recommendation Rec(2005)10 of the Committee of Ministers to Member States on “Special Investigative Techniques” in Relation to Serious Crimes Including Acts of Terrorism. https://www.coe.int/t/dg1/legalco-operation/economiccrime/organisedcrime/Rec_2 005_10.pdf

CoE (2019) Electronic Evidence in Civil and Administrative Proceedings: Guidelines and Explanatory Memorandum. https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

CoE (2001c) Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters. **ETS No. 182 of 8 November 2001, in force 1 February 2004.**, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008155e

Council of the European Union (2000) Council Act 2000/C 197/01 of 29 May 2000 Establishing in Accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters Between the Member States of the European Union. **OJ C 197/1, 12.7.2000**, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ: C:2000:197:0001:0023: EN: PDF

CPNI (2016) My Digital Footprint: A Guide to Digital Footprint Discovery and Management. https://www.cpni.gov.uk/system/files/documents/d3/e8/28-February-2017-Edited-In-house-My-Digital-Footprint-booklet.pdf

CRS (2022) Law Enforcement and Technology: Using Social Media. **R47008**, https://sgp.fas.org/crs/misc/R47008.pdf

Currie, R.J. (2010) *International and Transnational Criminal Law*. Irwin Law,

DCAF (2020) Thematic Brief: Police Integrity Testing. https://dcaf.ch/sites/default/files/publications/documents/DCAF_Brief_Police_Integrity_Testing_Jan2021_final_ENG_0.pdf

ECtHR (1998) Teixeira de Castro v. Portugal. **44/1997/828/1034**, https://hudoc.echr.coe.int/fre?i=001-58193

ECtHR (2008) Ramanauskas v. Lithuania. **Application no. 74420/01**, https://hudoc.echr.coe.int/fre?i=001-84935

Egmont Group About. https://egmontgroup.org/en/content/about

ECtHR (2022) Financial Intelligence Units' Role in the Fight Against Money Laundering of Corruption Proceeds Within the Context of the COVID-19 Pandemic. Public Report. https://egmontgroup.org/wp-content/uploads/2022/05/FIU-Role-in-Fight-Against-ML-of-Corruption-Proceeds_COVIDContext_Public_Final.pdf

Eurojust (2020) Case Law by the Court of Justice of the European Union on the principle of Ne Bis in Idem in Criminal Matters. https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2020-04_Case-law-by-CJEU-on-NeBisInIdem_EN.pdf

Eurojust (2021) The Impact of COVID-19 on Judicial Co-operation in Criminal Matters – Analysis of Eurojust's Casework. https://www.eurojust.europa.eu/sites/default/files/assets/2021-05-12-COVID-19-report.pdf

European Commission (2021a) Digitalisation of Cross-Border Judicial Co-operation. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/digitalisation-justice/digitalisation-cross-border-judicial-co-operation_en

European Commission (2021b) Special Investigation Service (STT). https://antifraud-knowledge-centre.ec.europa.eu/library-good-practices-and-case-studies/good-practices/special-investigation-service-stt_en

EUROPOL. (2003) *Intelligence Handling*. Office for Official Publications of the European Communities, Luxembourg. https://op.europa.eu/en/publication-detail/-/publication/45961f30-b84b-4079-b60d-1dd778a07c3c

EUROPOL. (2021) SIRIUS EU Digital Evidence Situation Report – 3 Annual Report, 2021. https://www.eurojust.europa.eu/sites/default/files/assets/sirius_eu_digital_evidence_situation_report_2021.pdf

EUROPOL (2022) About Europol: Helping Make Europe Safer. https://www.europol.europa.eu/about-europol

Europol & Eurojust (2019) Common Challenges in Combating Cybercrime as Identified by Eurojust and Europol. Fhttps://www.eurojust.europa.eu/sites/default/files/publications/reports/2019-06_joint-eurojust-europol-report_common-challenges-in-combating-cybercrime_en.pdf

Evans, A. (2008) The Role of Supreme Audit Institutions in Combating Corruption. *U4 Helpdesk Answer*, https://www.u4.no/publications/the-role-of-supreme-audit-institutions-in-combating-corruption.pdf

FATF (2006) Trade Based Money Laundering.

FATF (2018a) *Methodology for Assessing Technical Compliance with the FATF Recommendations and*

*the Effectiveness of AML/CFT Systems*. FATF, Paris. https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2 022%20Feb%202013.pdf

FATF (2018b) Professional Money Laundering. www.fatf-gafi.org/publications/methodandtrends/documents/professional-money-laundering.html

FATF (2019) International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. The FATF Recommendations. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

FATF (2020) COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses. www.fatf-gafi.org/publications/methodandtrends/documents/COVID-19-ML-TF.html

Findley, M., Nielson, D. & Sharman, J.C. (2012) *Global Shell Games: Testing Money Launderers' and Terrorist Financiers' Access to Shell Companies*. Griffith University Centre for Governance and Public Policy,

Fratto, T., Gust, J. & Ward, S. (2020) Leveraging Trusted Methods to Mitigate FCPA Risk during COVID-19. *Business Law Today*, https://www.americanbar.org/groups/business_law/publications/blt/2020/11/fcpa-risk/

GAC & CICC (2016) Understanding Digital Footprints: Steps to Protect Personal Information. A Guide for Law Enforcement. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/Understanding_Digital_Footprints-09-2016.pdf

Hoppe, T. (2016) Legislative Toolkit on Integrity Testing.

IESBA, IAASB & IRBA (2020) Navigating the Heightened Risks of Fraud and Other Illicit Activities During the COVID-19 Pandemic Including Considerations for Auditing Financial Statements. https://www.ethicsboard.org/publications/navigating-heightened-risks-fraud-and-other-illicit-activities-during-COVID-19-pandemic

INTOSAI (2019) INTOSAI-P 1: The Lima Declaration. https://www.intosai.org/fileadmin/downloads/documents/open_access/INT_P_1_u_P_10/INTOSAI_P_1_en_2019.pdf

INTOSAI (2020) Accountability in a Time of Crisis: How Supreme Audit Institutions and Development Partners Can Learn From Previous Crises and Ensure Effective Responses to COVID-19 in Developing Countries. https://idi.no/elibrary/COVID-19/986-accountability-in-a-time-of-crisis/file

ISO. (2018) *ISO 31000:2018 Risk Management – Guidelines*. International Organisation for Standardisation, Geneva.

Kotlyar, D. & Pop, L. (2019) *E-filing Asset Declarations: Benefits and Challenges*. World Bank, Washington, DC. http://hdl.handle.net/10986/32066

Lefebvre, S. (2003) The Difficulties and Dilemmas of International Intelligence Co-operation. *International Journal of Intelligence and CounterIntelligence*, **16**, 527-542. http://dx.doi.org/10.1080/716100 467

Machado, M.R. (2004) *Internacionalização do direito penal: a gestão de problemas internacionais por meio do crime e da pena*. Editora 34, São Paulo.

Magalhães, J.C.D. (1999) Fatores de Limitação da Jurisdição do Estado. *Revista dos Tribunais*, **88**, 46-58.

(2018) *Structured Settlements for Corruption Offences Towards Global Standards?* International Bar Association, London. https://www.oecd.org/corruption/anti-bribery/IBA-Structured-Settlements-Report-2018.pdf

Marsh, S. (2020) Putting Money Recovered From Graft to Good Use against COVID-19. *The StAR*, **Columnists**, https://www.the-star.co.ke/opinion/columnists/2020-04-13-putting-money-recovered-from-graft-to-good-use-against-COVID-19/

Interior, M.D.J.E., Hacienda, M.D.E.Y. & Tributaria, A.E.D.A. (1995) Convenio de Colaboracion suscrito entre el Ministerio de Justicia e Interior, el Ministerio de Economia y Hacienda y la Agencia Estatal de Administración Tributaria, en materiia de apoyo al Ministerio Fiscal en La Lucha contra los Delitos Economicos relacionados con la Corrupciion. https://www.fiscal.es/documents/20142/119628/Convenio+de+colaboración+suscrito+entre+el+Ministerio+de+Justicia+e+Interior%2C+el+Ministerio+de+Economia+y+Hacienda+y+la+Agencia+Estatal+de+Administración+Tributaria%2C+en+materia+de+apoyo+al+Ministerio+Fiscal+en+la+lucha+contra+los+delitos+económicos.pdf/d4bae740-115d-bc55-a0f6-d5ba21a2841e?version=1.1&t=1531480207 157

Ministerio Fiscal del Reino de España (2022) Memoria 2022 – Fiscalía contra la Corrupción y la Criminalidad Organizada. https://www.fiscal.es/documents/20142/183863/Memoria+2 022+-+Fiscalía+contra+la+Corrupción+y+la+Criminalidad+Organizada.pdf/2cf70ddd-4dfe-a29f-f64aee1c375bc552?t=1663584122 022

Monteith, C. & Gomes Pereira, P. (2015) Asset Recovery. In *Routledge Handbook of Transnational Crime,* (Eds, Boister, N. & Currie, R.J.) Routledge, New York, pp. 137-152. https://doi.org/10.4324/9780203380 277

NCA (2020) SARs Analysis on COVID-19. *SARs in Action*, **5**, https://nationalcrimeagency.gov.uk/who-we-are/publications/452-sars-in-action-may-2020/file

Nilsson, H.G. (2005) Special Investigation Techniques and Developments in Mutual Legal Assistance: The Crossroads Between Police Co-operation and Judicial Co-operation. *Resource Material Series*, **65**, 39-45. https://www.unafei.or.jp/publications/pdf/RS_No65/No65_07VE_Nilsson2.pdf

OCCRP (2020) Crime, Corruption and Coronavirus. https://www.occrp.org/en/coronavirus/

OECD. (2011a) *Asset Declarations for Public Officials a Tool to Prevent Corruption*. OECD, Paris. http://dx.doi.org/10.1787/9789264095281-en

OECD. (2011b) Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents. https://www.oecd.org/daf/anti-bribery/ConvCombatBribery$_{ENG.pdf}$

OECD. (2013) *Effective Inter-Agency Co-operation in Fighting Tax Crimes and Other Financial Crimes*.

OECD. (2016) *Committing to Effective Whistleblower Protection*. OECD Publishing, Paris. http://www.oecd-ilibrary.org/docserver/download/4216061e.pdf?expires=1458837257&id=id&accname=ocid195445&checksum=0B627928A51DBC4C33197D3AB7C2D4A6

OECD. (2017) *The Detection of Foreign Bribery*. OECD Publishing, Paris. www.oecd.org/corruption/the-detection-of-foreign-bribery.htm

OECD. (2019) Resolving Foreign Bribery Cases with Non-Trial Resolutions: Settlements and Non-Trial Agreements by Parties to the Anti-Bribery Convention. OECD Publishing, Paris. www.oecd.org/corruption/Resolving-Foreign-Bribery-Cases-with-Non-Trial-Resolutions.htm

OECD. (2020) Tax Administration Responses to COVID-19: Assisting Wider Government. OECD Publishing, Paris. https://read.oecd-ilibrary.org/view/?ref=135_135352-d2rqlqlfmw&title=Tax-Administration-Responses-to-COVID-19-Assisting-Wider-Government

OECD. (2021) Managing Emergency Procurement and Risks. https://www.oecd-ilibrary.org/sites/cb67f940-en/index.html?itemId=/content/component/cb67f940-en

OECD. (2022a) Implementing the OECD Anti-Bribery Convention. Phase 4 Report: Poland. https://www.oecd.org/daf/anti-bribery/poland-phase-4-report.pdf

OECD. (2022b) Public Procurement. https://www.oecd.org/gov/public-procurement/

OECD. (2022c) Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions. **OECD/LEGAL/0378**,

https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0378

OECD. (2022d) Recommendation of the Council on Public Procurement. **OECD/LEGAL/0411**, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0411

OECD. (2023) Implementing the OECD Anti-Bribery Convention. Phase 4 Report: Denmark. https://www.oecd.org/daf/anti-bribery/denmark-phase-4-report.pdf

OECD & IADB (2019) A Beneficial Ownership Implementation Toolkit. http://www.oecd.org/tax/transparency/beneficial-ownership-toolkit.pdf

Office of the Director of National Intelligence (2011) U.S. National Intelligence: an Overview 2011. https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf

Pieth, M., Low, L.A. & Bonucci, N. (2014) *The OECD Convention on Bribery. A Commentary*. Cambridge University Press,

Resimić, M. (2021) Institutional arrangements for whistleblowing: Challenges and best practices. *Transparency International Anti-Corruption Helpdesk Answer*, https://knowledgehub.transparency.org/assets/uploads/helpdesk/Overview-of-whistleblowing-institutional-arrangements$_{2021}$PR.pdf

Seddon, J. & Ivanovs, A. (2022) Self-Reporting Obligations to the Authorities and Other Disclosure Obligations: The UK Perspective. In *The Practitioner's Guide to Global Investigations. Volume I: Global Investigations in the United Kingdom and the United States,* (Eds, Seddon, J. et al.) Global Investigations Review, London, pp. 44-75.

Jason Sharman et al. (2011) The Puppet Masters How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It. http://public.eblib.com/choice/publicfullrecord.aspx?p=799 756

Stroligo, K., Hsu, C.-L. & Kouts, T. (2018) *Financial Intelligence Units Working With Law Enforcement Authorities and Prosecutors*. World Bank, Washington, DC. https://openknowledge.worldbank.org/handle/10986/31254

Transparency International (2020) Public Procurement During States of Emergency: Minimum Requirements to Ensure the Integrity of Contracts Awarded During Crises. https://images.transparencycdn.org/images/EN_Latin-America_emergency_procurement_COVID-19.pdf

UNODC (1988) United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. **United Nations, Treaty Series, vol. 1582, p. 95 (20 December 1988)**, https://treaties.un.org/doc/Treaties/1990 November 19901 111%2008-29%20AM/Ch_VI_19p.pdf

UNODC. (2000) United Nations Convention Against Transnational Organised Crime and the Protocols Thereto. *UNTS*, **2225**, 209 (28 September 2003). https://treaties.un.org/doc/Treaties/2000 November 20001 115%2011-11%20AM/Ch_XVIII_12p.pdf

UNODC. (2003) United Nations Convention against Corruption. *UNTS*, **2349**, 41 (14 December 2005). https://treaties.un.org/doc/Treaties/2003 December 20031 209%2002-50%20PM/Ch_XVIII_14p.pdf

UNODC. (2011) *Criminal Intelligence: Manual for Analysts*. UNODC, Vienna. https://www.unodc.org/documents/organised-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf

UNODC. (2020) G20 Good Practices Compendium on Combating Corruption in the Response to COVID-19. https://www.unodc.org/pdf/corruption/G20_Compendium_COVID-19_FINAL.pdf

UNODC. (2022) About the GlobE Network: Cross-Border Co-operation to End Corruption. https://globenetwork.unodc.org/globenetwork/en/about.html

World Bank (2020) Sanctions System: Annyal Report FY20. https://documents1.worldbank.org/curated/en/861191602141633639/pdf/World-Bank-Group-Sanctions-System-Annual-Report-FY20.pdf