Asset and Interest Disclosure (AID) Systems in EU Member and Candidate States

Report on the standardised EU risk analysis framework and roadmap for implementing automated and digital AID systems

Di Nicola Andrea, Baratto Gabriele, Donati Bianca, Rigon Beatrice
Centre for Security and Crime Sciences (CSSC)
University of Trento and University of Verona (Italy)

Co-funded by the European Union

Asset and Interest Disclosure Systems in EU Member and Candidate States
Report on the standardised EU risk analysis framework and roadmap for implementing automated and digital AID systems

Authors:

Andrea Di Nicola

Gabriele Baratto

Bianca Donati

Beatrice Rigon

With the collaboration of:

Beatrice Pattaro

The CSSC research team included (in alphabetical order) Gabriele Baratto, Caterina Bergomi, Andrea Di Nicola, Bianca Donati, Giuseppe Espa, Elena Ioriatti, Beatrice Pattaro, Beatrice Rigon.

Project: qAID - Towards contemporary knowledge and innovative tools for assessing and enhancing effectiveness of Asset and Interest Disclosure (AID) systems in EU Member and Candidate States

Deliverable 3.1

Partners (beneficiaries)

Associate partner

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission (Directorate General for Migration and Home Affairs). Neither the European Union nor the granting authority can be held responsible for them.

Centre for Security and Crime Sciences (CSSC) of the University of Trento and the University of Verona

www.cssc.unitn.it

Trento, June 2025

Table of Contents

1. Introduction 3
   1.1 Background 3
   1.2 Aim and contents of the report 4
   1.3 Scope and methodology 5
   1.4 Synthesis of the results (executive summary) 6
2. Country profiles 9
   2.1 General overview 9
      2.1.1 Bulgaria 9
      2.1.2 Georgia 11
      2.1.3 Germany 14
      2.1.4 Italy 17
      2.1.5 Latvia 18
      2.1.6 Moldova 23
      2.1.7 Montenegro 26
      2.1.8 Romania 28
      2.1.9 Serbia 30
      2.1.10 Ukraine 32
   2.2 Comparative analysis 34
      2.2.1 Risk analysis and verification 35
      2.2.2 Risk indicators or “red flags” 35
      2.2.3 Consequences 36
      2.2.4 Digitalisation 37
3. Best practices for implementing a standardised EU risk analysis framework and roadmap for automated and digital AID systems 38
4. Annex A - Interview protocol 40
5. Bibliography 42

1. Introduction

1.1 Background

Asset and Interest Disclosure (AID) systems are increasingly becoming one of the most important multipurpose tools used worldwide to prevent and combat corruption in the public sector (Rossi et al., 2017). AID systems aim to build a culture of integrity, foster public officials' accountability and promote the public's trust (Jenkins, 2015; StAR Initiative, 2012), by collecting information about public officials' assets, incomes, revenue streams, expenditures and activities, to inform on existing or potential conflicts of interest. Based on each country's specific needs, disclosure systems may be aimed at identifying conflicts of interest, detecting illicit enrichment, or at both. Such objectives are reflected in the structure and contents of the declaration forms and disclosure obligations (Pop et al., 2023).

The implementation of effective measures requiring public officials to disclose information related to their financial interests and activities—commonly through Asset and Interest Disclosure (AID) systems—is strongly encouraged at both the international and European Union levels[1]. Across Europe, AID systems are widely established, with each country tailoring their design and operational model to their own legal, institutional, and administrative frameworks. While these systems serve as critical tools for accountability, they also present significant challenges in terms of volume and complexity of the declarations. The number of declarations filed annually can be overwhelming, making manual review for inconsistencies or signs of misconduct highly resource-intensive and, in many cases, impractical.

In response to this challenge, the integration of risk analysis has become an essential component of modern AID systems. Risk analysis involves the systematic identification, assessment, and prioritization of risks inherent in the information disclosed by public officials. By leveraging this approach, oversight bodies can more effectively allocate resources to the most high-risk cases, thus increasing the efficiency and impact of verification processes[2]. Through the use of data analytics and advanced review techniques, anomalies or patterns that suggest potential irregularities can be identified and flagged for further scrutiny. These processes are strongly supported by the use of digital tools, which have also been identified as a general best practice for the implementation of AID systems: for this reason, an increasing number of countries is working towards progressively adopting them.

At the core of this methodology are "red flags"—defined indicators that signal a heightened probability of wrongdoing (Kotlyar & Pop, 2021). While not conclusive evidence of misconduct, red flags serve as early warnings that warrant closer examination. For example, a sharp increase in reported assets without a corresponding legitimate income source may indicate an unjustified enrichment. The application of red flag criteria allows agencies to prioritize the most relevant and potentially problematic disclosures, streamlining their investigative efforts and strengthening accountability.

[1] This recommendation is enshrined by articles 8(5) and 52(5) of the UN Convention Against Corruption (UNCAC), since AID systems may lead to the identification of potential conflicts of interest or reveal instances of corrupt behaviour by public officials. Within the European Union, article 3(3) of the recent proposal for a "Directive on combating corruption" establishes the need for Member States to "ensure that key preventive tools such as […] effective rules for the disclosure and management of conflicts of interests in the public sector, effective rules for the disclosure and verification of assets of public officials […] are in place. European Commission, Proposal for a Directive of the European Parliament and of the Council on combating corruption, replacing Council Framework Decision 2003/568/JHA and the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union and amending Directive (EU) 2017/1371 of the European Parliament and of the Council, COM(2023) 234 final, 2023/0135 (COD), Brussels, 03.05.2023. Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A234%3AFIN.

[2] Organisation for Economic Co-operation and Development. (2023). Integrity of asset declarations and conflict of interest disclosures: Towards better frameworks and implementation (GOV/PGC/INT (2023)12/FINAL). OECD Publishing, p.23.

The research and analysis presented in this report aim to support the development of a standardized risk analysis framework for AID systems across Europe and a roadmap for implementing automated and digital AID systems. This proposed framework seeks to harmonize key methodological principles while maintaining sufficient flexibility to adapt to the distinct legal, economic, and cultural contexts of each EU Member and Candidate State.

1.2 Aim and contents of the report

The main objective of this report is to map and to provide a systematic analysis of the current state of national AID systems in EU Member and Candidate States with specific regard to risk analysis methods, to identify best practices and recommendations for the development of a standardised EU risk analysis framework and of a roadmap for implementing automated and digital AID systems. To achieve this aim, the report will present the results of in-depth interviews carried out with anti-corruption agencies and transparency bodies in EU Member and Candidate States.

The activity was carried out in WP3 "*Development of a standardized EU risk analysis framework to help filter declarations and prioritize verification and of a roadmap for implementing automated and digital risk analysis of declarations of asset and interest*", in the context of EU-funded project "*qAID – Towards contemporary knowledge and innovative tools for assessing and enhancing effectiveness of Asset and Interest Disclosure (AID) systems in EU Member and Candidate States*". The project is coordinated by the Centre for Security and Crime Sciences ("CSSC") of the University of Trento and the University of Verona and carried out in partnership with the Romanian National Agency for Integrity (ANI), the Centre for the Study of Democracy (CSD – based in Bulgaria), the Regional Anti-Corruption Initiative (RAI) Secretariat and the Italian Anticorruption Authority (ANAC). For more information about the project's consortium and objectives, please see the box below.

Following the Introduction (Section 1), the report is divided into two sections, covering the main features of the risk analysis mechanisms (Section 2), and providing an overview of best practices and recommendations identified based on the interview results and secondary research (Section 3).

Project qAID – Towards contemporary knowledge and innovative tools for assessing and enhancing effectiveness of Asset and Interest Disclosure (AID) systems in EU Member and Candidate States

General objective

The general objective of project qAID is to provide EU Member States (MSs) and Candidate States (CSs) with contemporary knowledge and innovative tools to assess and improve the impact of national asset and interest disclosure (AID) systems. The project aims to be the first comprehensive EU project to address the systems of AID in EU MSs and CSs and identify avenues to make them more effective and efficient. The general objective will be reached by:

i. Identifying **best practices** and effective (including automated and digital) systems and processes through structured evaluation process;

ii. Developing a **standardised EU risk analysis framework** to strengthen filters for declarations and prioritise verification, along with a roadmap for implementing automated and digital risk analysis of declarations of assets and interests of relevant public officials in EU MSs and CSs;

iii. Developing a **comprehensive toolkit to measure the impact** of asset and interest disclosure systems in EU MSs and CSs;

iv. **Disseminating the new knowledge** and developed tools among national stakeholders in EU MSs and CSs.

Specific objectives

To achieve its aim, the project sets itself the following specific objectives:

i. Develop and promote an integrated approach to measuring progress and assessing the impact of AID systems in EU Member and Candidate States;

ii. Promote the implementation of best practices and data exchange on AID systems in EU Member and Candidate States (with a particular focus on risk analysis, including automated and digital, to filter declarations and prioritize verification);

iii. Enhance the capacity of anti-corruption institutions in dealing with asset and conflict of interest disclosure in EU Member and Candidate States.

Project partners

Beneficiaries

Centre for Security and Crime Sciences (CSSC) | ITALY [Coordinator]

Regional Anti-Corruption Initiative (RAI) Secretariat | BOSNIA-HERZEGOVINA

Centre for the Study of Democracy (CSD) | BULGARIA

Agenția Națională de Integritate (ANI) | ROMANIA

Associated partner

Autorità Nazionale Anticorruzione (ANAC) | ITALY

Funding

European Commission (Directorate General for Migration and Home Affairs) – ISF Programme 21-27

Website

https://rai-see.org/qaid/

1.3 Scope and methodology

Based on the results of extensive desk research and literature review, analysis of secondary sources and consultations with the project's partners, the CSSC research team developed an interview protocol aimed at collecting information about existing risk analysis mechanisms in national AID systems and providing a better understanding of their characteristics and inner processes. The interview was structured into six sections, focusing on the following aspects:

i. **Background information** about the existing AID system;
ii. The **risk analysis method** of existing AID systems. Whether and to what extent (automated or not) they are used in EU MSs and CSs and what rules they provide;
iii. The **risk indicators ("red flags")** used to qualify a declaration as "at risk". How these indicators are identified, updated and combined to determine the risk level of a declaration;
iv. The **consequences** that follow once a declaration is qualified as "at risk";
v. The **digitalisation** process and how it could support or improve the risk analysis;
vi. The **best practices** that outline the desirable features that risk analysis methods should employ.

The interview protocol underwent a pilot phase in Italy, where the interview was conducted by CSSC with ANAC. The finalised version of the interview protocol was distributed via e-mail to anticorruption and transparency institutions and bodies in 11 EU Member and Candidate States. Based on the results of WP2, the interview invitation (and related protocol) was addressed to those countries which had reported

implementing risk analysis mechanisms. The interviews protocols were transmitted at the end of February 2025 (see Annex A). The interviews were conducted between March and April 2025.

More in detail, it was possible to reach and conduct the in-depth interviews with anti-corruption and transparency bodies in 10 countries out of the 11 which had stated to have a risk analysis mechanism when surveyed in WP2. Specifically, interviews were conducted with the following:

EU Member States

- BG | Bulgaria
- DE | Germany
- IT | Italy
- LV | Latvia
- RO | Romania

EU Candidate States

- GE | Georgia
- MD | Moldova
- ME | Montenegro
- RS | Serbia
- UA | Ukraine

1.4 Synthesis of the results (executive summary)

This paragraph presents a synthesis of the results of the qAID in-depth interviews, which will be analysed in detail in the following sections of this report.

Country profiles

The analysis of the risk analysis methods at the national level, based on the results of the interviews, reveals similarities and differences across the countries.

- **Risk analysis and verification.** Risk analysis and verification often overlap in practice, although they are conceptually distinct. Indeed, risk analysis estimates the likelihood of irregularities in asset and interest declarations and thus precedes—and triggers—verification. Conversely, verification ensures the accuracy of the declaration and legal enforceability by enabling sanctions when warranted. Three primary models of risk analysis currently exist: fully electronic, fully manual, and hybrid. The latter appears to be the most common, since it supports the gradual transition towards digital models, it best adapts to legal frameworks which could pose constraints to full IT integration and is able to process various alerts.
- **Risk indicators ("red flags").** Risk indicators allow the early detection of potential irregularities or violations (e.g. false information, illicit enrichment, conflicts of interest, incompatibilities). Although most countries implement red flags to support the risk analysis, only Ukraine and Latvia maintain formalized and regularly updated red flag lists, while the others rely on more limited and standardised risk indicators. Ukraine's system uses a weighted scoring model to trigger verification above a risk threshold.
- **Consequences.** The declarations are predominantly verified by centralised anti-corruption bodies (e.g., Georgia, Montenegro, Romania, Serbia, Ukraine), although decentralized models of verification are in place in several countries (e.g., Latvia, Italy, Germany). The effective management of "at risk" declarations requires strong inter-agency cooperation and

communication extending to information exchange and to referrals to law enforcement when criminal offenses are detected.

- **Digitalisation.** Digitalisation has contributed to the significant advancement of risk analysis mechanisms and their efficiency; nevertheless, challenges still remain. Indeed, in several countries a full digital integration is hindered by technical, organisational, legislative difficulties, as well as challenges related to user adaptation.

Best practices for implementing a standardised EU risk analysis framework and roadmap for automated and digital AID systems

By combining the interview responses with recommendations resulting from the desk research, general principles and suggestions were identified to support the development of a standardised EU risk analysis framework and of a roadmap for implementing automated and digital AID systems, integrating long term experiences and innovative approaches.

Standardised EU risk analysis framework

- **Risk-based approach.** AID systems must be risk-based, prioritizing proactive control of declarations from top executives (PTEFs) by identifying red flags in real time and enabling thorough verification beyond formalistic or reactive checks.
- **Public database interoperability**. An effective risk analysis mechanism requires integrating multiple databases also at international level to identify risk indicators—such as individuals holding multiple roles, significant asset or income changes, discrepancies in financial and property records—triggering in-depth reviews.
- **Efficient system architecture**. The design of national risk analysis systems should either enable collaboration and comparison among administrations via centralized information access or simplify processes by assigning clear responsibility to individual administrations, ensuring flexibility and prompt adaptation to specific national needs.
- **Strong internal oversight and resources.** Adequate human and financial resources, along with strong internal oversight mechanisms, are crucial for fairness and consistency, especially within key bodies like National Anticorruption or Integrity Agencies.
- **Continuous learning and international cooperation.** The development and strengthening of national risk criteria and systems benefit from guidance and sharing best practices with international partners, making international benchmarking and studying advanced models strongly recommended.
- **Transparency.** An advanced AID system should be transparent enough to allow citizens to scrutinize public officials' declarations, fostering accountability and public trust. Greater public access to aggregated control statistics is also advocated.
- **Digitally supported mechanisms.** Digitalisation is pivotal for modern AID systems, combining electronic submission and checking of declarations, IT verification and reporting tools, and machine-readable data human analysis, which remains of critical importance. A mixed method model could thus ensure accuracy and comprehensive coverage.

Roadmap for automated and digital AID systems

- **Electronic submission and verification**. Systems should enable electronic submission—preferably via pre-compiled forms—and automated checking of all declarations to streamline submission, improve compliance, enhance data management and swifter reviews, and facilitate publication.
- **IT tools for verification and reporting**. Leveraging IT tools for in-depth verification and systematic reporting is an essential component of a digital risk analysis system.

- **Machine-readable data.** Data should be machine-readable to facilitate continuous system training and analysis.
- **Automated data checking and prioritization.** Automated tools are vital for checking all declaration items, automatically grouping and prioritizing declarations that present higher risk or multiple "red flags".
- **Red-Flags and cross-checks.** Automated red-flag detection algorithms, cross-checks with public registers, and mechanisms for prioritization greatly improve the efficiency of verification and increase the identification of irregularities.
- **Interoperable systems and integration with external data.** Implementing electronic submission platforms and interoperable systems allows integration of financial, property, and employment databases to identify high-risk declarations. International cooperation can enable national and cross-border communication. Integration with external data ensures a clearer, more comprehensive picture, and should be done gradually to allow familiarisation.

2. Country profiles

This section will present and discuss the results of the interviews conducted in WP3 in relation to the national AID systems, with particular attention to the structure and functioning of the current state of risk analysis mechanisms. Each section references the questions **(Qn)** asked during the interview (see Annex A): the corresponding text therefore refers to the respondent's answer to that specific question.

2.1 General overview

2.1.1 Bulgaria

Background information

The AID system was introduced back in 2006, and the Bulgarian National Audit Office was in charge of collecting and analysing the declarations. In 2018 the *Counter-Corruption and Unlawfully Acquired Asset Forfeiture Act* was adopted, wherein the collection and analysis of AID declarations was transferred to the newly established Commission for Countering Corruption and Confiscation of Unlawfully Acquired Property. In 2023 the Commission was restructured, and the anti-corruption activities were transferred into the Commission for Combating Corruption, while the forfeiture of assets was tasked to a Commission for confiscation of unlawfully acquired property.

The collection and check of law and mid-level public officials is conducted by the inspectorates attached to each ministry, the municipalities and some State agencies. The inspectorates use a methodology similar to that of the Commission: that's why many inspectorates that collect declarations from their employees in ministries and agencies periodically seek the opinion of the Commission for Combating Corruption on how to handle various issues related to the collected declarations. At the same time, they do not have established procedures for cooperation with the Chief Inspectorate under the Council of Ministers, which is responsible for coordinating the work of the individual inspectorates within ministries and agencies **(Q1).**

In addition to the changes of the responsible authority, the legal framework for the AID declarations was also updated. For example, both in 2018 and in 2023 the introduced new laws extended the range of public officials that are obliged to submit annual AID declarations. Moreover, the list of assets and income sources was also expanded to address certain gaps in the existing legal framework **(Q2).**

Risk analysis method

The Commission for Combating Corruption checks and verifies all submitted AID declarations without trying to select or prioritize "high-risk declarations" **(Q12a)**. All declarations are cross-checked **(Q6)** with a number of official public registries (e.g. property registry, vehicle registry, bank registry etc.) to verify the information in the AID declaration.

Since the Commission also has investigative powers, their operational unit can additionally analyse the information of specific declarations and conduct a comprehensive lifestyle assessment of the declarant, including by application of regular police investigation methods, exchange of operational information with other police authorities abroad or in some cases by special investigative techniques. However, the work of the investigative unit is mainly triggered by notifications from institutions, citizens, media, whistle-blower signals or intelligence information collected through informants. In this case the information from the AID declaration is cross-checked with the lifestyle of the declarant using information from media,

online sources, testimonies from witnesses, additionally collected information (e.g. information from travel agencies, video surveillance, etc.).

In fact, when the Commission for Combating Corruption receives a report—for example, if someone alerts them about issues related to asset declarations or conflicts of interest involving public officials—they initiate an investigation. To exemplify, a GDBOP investigation into a VAT fraud crime revealed a connection to a member of parliament, prompting the Commission to launch its own investigation. Similarly, if media reports expose potential issues, the Commission can act on them independently.

The risk analysis is semi-automated; they use a mixed method[3] **(Q3)**. Data from AID declarations and data provided from the public registries are uploaded on the servers of the Commission and a specialised software allows to cross-check declarations' data with data from the registries. The uploading is done manually (using discs and/or memory sticks).

The verification is also a semi-automated process, as the software allows only one AID declaration to be cross-checked and verified at a time. The Public Registry Directorate within the Anti-Corruption Commission is tasked with verifying the accuracy and timeliness of declarations submitted by high-level officials (GRECO, 2023) **(Q12b)**.

AID declarations are submitted by declarants both on paper (because of the requirement for hand signature) and in electronic version. The electronic version is uploaded manually by an expert from the Commission, who also does a basic check (whether the electronic version of the declaration is available, the file is completed and not corrupted or in wrong format). Once the declarations are uploaded along with the data from the public registers, each declaration is cross-checked and verified using the specialised software **(Q5)**.

All declarations are checked because of the increased number of declarants due to the political crisis in Bulgaria. Over the past four years, frequent parliamentary elections and numerous regular and caretaker governments have led to a continuous influx of new declarants who need to be reviewed. In previous years, the anti-corruption authority usually conducted only one review per year. However, in recent years, with two or even three elections annually, they now must verify MPs, ministers, deputy ministers, and many more up to three times per year **(Q6).**

One of the issues with the AID system was related to the requirement for all high public officials to submit an AID declaration one year after leaving office. Most people did not comply, and many sanctions were imposed. However, the subsequent review of these cases revealed that in most cases people did not do that intentionally, but rather because of the long period many of them simply forgot. As a result, the requirement for such declaration was removed as an obligation **(Q7).**

In the previous survey's result are indicated as "red flags" that are used to qualify a declaration as "at risk" the following: late submission of the declaration, missing data, data inconsistencies or discrepancies (e.g. within the form, with past declarations, with external databases), behaviour inconsistent with the content of the declaration (e.g. assets acquired above annual salary or set percentage of annual salary), business or companies abroad, missing information about or suspiciously large amounts related to family members[4] **(Q8).**

The processing of declarations involves too much manual work involved both in entering the data of the declarants and in the subsequent verification process. First, employees of the CPC enter data declaration by declaration from thousands of disks and flash drives. Instead of creating an online form through which declarants can submit their data, like the National Revenue Agency does, they manually input 17 to 18

[3] Answer to question 3.2 "*The risk analysis of the declarations is conducted:"* of the qAID online survey (WP2). Possible answers: Automatically – Manually – Mixed method.
[4] Answer to question 3.4 "*Which elements are identified as risk indicators ("red flags")?"* of the qAID online survey (WP2).

thousand declarations one by one. Additionally, they apparently check the names of public officials individually: employees divide the work by regions, and different groups start verifying each person by searching for them in the registers. This process should also be automatable with a relatively simple script that could check all declarants across all registers and generate lists of discrepancies. These cases could then be reviewed by employees **(Q15** and **Q16).**

2.1.2 Georgia

Background information

The journey toward transparency and accountability in the asset and interest declaration system in Georgia began in 1997. Specifically, the foundations were laid in November of that year with the introduction of the declaration system. Initially, it was a paper-based system. Around 47,000 public officials were required to declare their assets and incomes. However, these declarations were not publicly available and could only be assessed upon request **(Q1).**

In 2010, the system transitioned to an electronic platform, making all declarations accessible online. At the same time, the range of officials required to declare their assets expanded to include senior-level officials as well as middle managers, thereby broadening the scope of who was obligated to declare their public income and interests.

In 2017, a specific department was created within the Civil Service Bureau to oversee the process. This department, known as the Declarations Monitoring Department, was responsible for checking the completeness of the data, managing the increase in declarations and auditing the submitted declarations.

In 2021, the Georgian AID system introduced electronic ID cards, allowing public officials to electronically sign and submit their declarations. This innovation also enabled officials living abroad to file their declarations from anywhere in the world (public officials who are residing outside of Georgia are still required to submit their declarations) **(Q2).**

Since September 2023, the Anti-Corruption Bureau has taken on a range of functions and is actively working to refine these processes by researching best practices and ensuring full compliance to GRECO international recommendations.

Risk analysis method

The development of a risk analysis method is still ongoing, with both international and local experts contributing to the process. This effort has been part of the broader development of the asset declaration system that has been in place in the country.

The process of risk assessment for public officials considers several factors, such as positions of state-political officials, the vulnerability to the risk factors, the high level of the position held, and any potential conflicts of interest identified during their tenure. Additionally, information from previous declarations is examined, including any omissions or inconsistencies, as well as allegations made against the official by the media or civil society. Moreover, a special Commission is being established each year, to review the asset declarations of selected public officials each year.

Currently, Georgia is working actively on developing a more robust risk analysis method for selecting which declarations should be monitored **(Q3)**. The system used for asset declarations is designed to simplify the process for public officials by automatically extracting data from public registries. For example, declarants can easily click a button to transfer details such as the type of property they hold in

Georgia, as the system is connected to national registries. This feature ensures that information is not omitted, as it is pre-filled, including data related to contracts, notary services, and other relevant details. The declarant is then responsible for reviewing and verifying the information to ensure completeness and accuracy. If any omissions or errors are found, the declarant is given an additional month to correct the information (Q5).

As a part of its mandate, the grounds for initiating the monitoring of an official's asset declaration are:

a) a random selection by the Unified Electronic Declaration System;
b) a reasoned written application;
c) declarations selected by a standing Commission on the basis of specific risk factors (positions of state-political officials, particular risk of corruption, high public interest and violations revealed as a result of the monitoring).

The Bureau has a prerogative to monitor public officials either based on its own decision or upon a written request. Media organizations also play a vital role in this process, as they can alert the Anti-Corruption Bureau and request specific declarations to be reviewed. The Bureau has a structured plan to ensure that all declarations are checked annually. At the beginning of each year the Bureau establishes its monitoring schedule, outlining which officials' declarations will be reviewed that year. If a declaration has not been selected for monitoring but a public interest alert arises, the Bureau will always consider the public interest, and the specific declaration may be prioritized for monitoring. The total number of declarations monitored could vary from year to year, depending on the number of reasoned written applications to be considered.

In terms of monitoring, about 20% of the declarations are subject to double-checking. Financial auditing is conducted to verify the accuracy of the information provided, particularly to identify any potential cases of illicit enrichment or inconsistencies between the declared income and other financial details. Since the Bureau does not have direct access to bank account data, officials are required to provide specific bank transaction information when necessary. This information is handled with strict confidentiality, and only the relevant department within the Bureau has access to such sensitive data, including information related to the declarant's family members, as they are also subject to declaration requirements.

The data is cross-checked against previous declarations to identify inconsistencies, such as unexplained changes in income, illicit enrichment, conflicts of interest, or undeclared gifts or sponsorships. Additionally, if assets declared in previous years are not listed in the current year's declaration without an explanation, this triggers further investigation. If the declarant has sold or transferred property or entered into contracts that should be disclosed, they must provide an explanation. This process ensures that all declarations are thoroughly reviewed for accuracy and compliance (Q5).

Each year, the number of public officials and the legal framework undergo changes, along with the definition of who qualifies as a public official. Currently, all declarations are subject to factual correctness and completeness. However, the thorough monitoring will be assured to 10-20% of declarations, and this number is expected to increase by the end of 2025 due to recent changes in the legal framework. Over the past decade, the scope of the law has been amended multiple times, redefining who is considered a senior-level public official or a manager. Additionally, the classification of specialist levels has evolved and some positions or institutions, which were created for specific purposes, no longer exist, whereas some of new have been created (Q6).

Since its establishment in September 2023 and throughout 2024, the Bureau has been working diligently on implementing a risk-based approach for monitoring asset declarations. Given the limitations on the number of declarations the Bureau can review annually, it is possible that some of the selected declarations may not pose any significant risk and could be entirely accurate. To address this, the Bureau aims to develop a program with specific rules and algorithms that will automatically detect

inconsistencies in the data submitted. This software would help identify declarations that contain discrepancies, making it easier to prioritize and target those with a higher risk of corruption. In addition to the automated system, the Bureau will also follow a manual approach, where individuals can submit requests for specific declarations to be monitored. This is in line with the law, which allows people to bring attention to particular declarations for review. Furthermore, an official shall, within two months after dismissal, if he/she failed to submit the declaration within the calendar year of his/her dismissal, and within the same, respective month of completing the previous declaration in the year following the dismissal, unless he/she is appointed to another position, complete and submit an official's asset declaration.

The Bureau also considers public input, including reports from colleges or monitoring entities, as another avenue to identify declarations that should be targeted. By combining both automated and manual methods, the Bureau will be better equipped to allocate its resources efficiently, ensuring that the highest-risk declarations are prioritized for closer scrutiny, while maintaining a comprehensive and legally compliant monitoring process **(Q7).**

Risk indicators ("red flags")

Georgia is currently working on a list of red flags (so **Q10-11** cannot find a proper answer yet but fall into the best practices Georgia is currently working on implementing). High public interest shall be a key factor in determining which declarations are monitored. Violations revealed in previous declarations, the official's high-level role, or involvement in high-risk areas such as procurement processes will also be important considerations. If a person is holding a position that carries a higher risk of corruption, such as being involved in procurement or in a conflict of interest is identified, their declaration will be considered "at-risk" **(Q8).**

These at-risk declarations are thoroughly checked. This process may include reviewing any omissions, comparing the current declaration with previous filings, and cross-referencing the official's declaration with those of their family members or other public officials they may be connected with. For example, when monitoring judges, the Bureau will look for outliers in their declarations. If a particular public official reports receiving significantly higher amounts compared to others – such as three times the amount – this will raise a flag, and those declarations will also be categorized as at-risk, as they exhibit a pattern that deviates from the norm **(Q9).**

Consequences

Establishing a threshold for identifying at-risk declarations is crucial. GRECO recommends using targeted statistical data to identify a pool of declarations that meet a certain risk threshold. According to GRECO, these thresholds should be re-evaluated periodically, to be sure that all levels of public officials are properly checked. This includes not only ministers and their deputies, but also advisors, who will be selected either through the automated program or via manual checks **(Q12a).**

The Bureau is a preventive institution, meaning that its primary function is preventative, rather than prosecutorial. It does not have the authority to file motions towards the prosecution. If a declaration is identified with intentional violations, it is sent to the appropriate bodies for further investigation to determine if there are any criminal violations of the law. If such violations are found, the case is transferred to the relevant authorities, such as the prosecution. Based on the results of the monitoring of official's asset declarations, the Bureau has three main types of responses:

a) In case of the non-existence of a violation in the official's asset declaration – the Bureau will not issue an administrative fine;

b) The second response occurs in case of the existence of a violation in the official's asset declaration: - If incomplete or incorrect data are entered into the official's asset declaration wilfully, and if there are essential elements of an offence, the Bureau shall forward the respective declaration and materials of the proceedings to the relevant law enforcement body for further response; Plus, the official's asset declaration shall be assessed negatively.
c) In the case of the existence of a minor violation in the official's asset declaration- the Bureau will issue an administrative fine, which gives the declarant the opportunity to rectify the information **Q12b)**.

Since its establishment in 2023, the ACB is the only central institution responsible for collecting and monitoring asset declarations in Georgia, in line with the regulations and recommendations of the European Commission. Previously, these responsibilities were handled by the Civil Service Bureau, but its staff, along with two key departments, was transferred to the ACB. One department was tasked with ensuring the accuracy and completeness of the data, while the other focused on auditing the financial aspects and verifying the factual correctness of the declarations. The staff from both departments now works under the ACB. The ACB inherited numerous responsibilities from various institutions in Georgia. These include tasks such as monitoring ethics and integration policies, advising on the creation of an anti-corruption political climate, and developing national strategies and integrity plans. The Bureau is also responsible for reviewing the financial declarations of political parties. The Bureau publishes on its website the statistical data indicating how many declarations have been submitted and their outcomes **(Q13).**

Digitalisation

Digitalisation in Georgia is still an ongoing process. The Bureau's website is also going to be re-evaluated, re-checked and restructured for declarations **(Q14).** So far, not relevant issues have been encountered while developing the new website **(Q15).** Also, Georgia received positive feedback by GRECO's evaluation team.

2.1.3 Germany

General overview

To compensate for the lack of a disclosure requirement for investments and assets, various agencies involved in preventing, uncovering and prosecuting corruption are required to cooperate to ensure the success of the fight against corruption. This cooperation is based on the need for the law enforcement authorities to be informed early if there is a suspicion of criminal activity related to corruption. Agencies are expected to discuss and analyse these suspicions together so that the appropriate response can be made swiftly, flexibly and effectively.

Tax authorities are obliged to report any facts that raise suspicion of a criminal offense, in line with tax laws such as section 4 (5), first sentence, no. 10 of the Income Tax Act, section 10 of the Ordinance on Tax Audits, and section 31b, second sentence of the Fiscal Code. These rules require revenue authorities to report such suspicions to law enforcement authorities. Similarly, courts, public prosecution offices, and administrative authorities are also obligated to report relevant information to the tax authorities. The notification requirements are further supported by general legal provisions, such as those in civil service law (regarding compensation claims), the Fiscal Code (section 116 on tax crimes), the Criminal Code (sections 73 et seq. on asset confiscation), and the Code of Criminal Procedure (sections 111nb et seq. on provisional asset securing) (UNODC, n.d.).

Out of Germany's 16 Länder, 15 have implemented their own rules to ensure that tax authorities, audit institutions, and other relevant authorities fulfil the notification requirements, effectively compensating for the lack of an asset and investment disclosure obligation.

On the basis of the Anti-Corruption Directive, all staff assignments in the Federal Criminal Police Office (in 2018) and in the Federal Police (in 2013) have been assessed for their respective vulnerability for corruption. The assessment identified 660 positions in the Federal Criminal Police Office and 1979 positions in the Federal Police to be especially vulnerable to corruption[5]. The results of this assessment were communicated to the different departments, managerial staff and employees concerned and registered in the personnel management system. In addition to the compulsory measures already in place (i.e. intensified administrative and operational supervision, the principle of greater scrutiny/"multiple eyes", transparency, further training and regular briefings by supervisors), further protective measures were imposed or proposed by the Internal Audit in both agencies where needed. These for example include inspections and random checks by supervisors, staff or task rotation and/or other organisational measures (GRECO, 2024).

The GRECO Evaluation Team learned that apart from this risk assessment procedure, there are more general risk analyses carried out by the Internal Audit of the Federal Police, looking at a wider variety of risk categories (i.e. the risk of deviating from standards). One of risk categories examined in this context is also corruption. As the occasion demands (e.g. in case of a transfer of tasks, creation of new posts or organisational units), targeted risk assessments are carried out, involving the responsible Internal Audit Division.

Members of the Bundestag[6]

Background information

In Germany, the Bundestag Code of Conduct has been in place since 1972, initially serving as an administrative regulation for Parliament. In the 1980s, the first actual laws regarding the Code came into force and have constantly been updated since then. The original focus of the Code was on MPs declaring remunerated side activities, but in 1987 the scope of the declaration was expanded to include shareholdings as well. As for now, the law requires MPs to disclose any income they receive during their mandate, including income from side activities, donations and shareholdings. However, it should be noted that German MPs are not actually required to declare their wealth, such as movable assets, upon entering office, although certain non-paid voluntary activities must be disclosed (Q1).

The Code has undergone significant updates, with the last comprehensive reform taking place in October 2021. One of the key updates was the reduction of the threshold for declaring shareholdings down to 5%, meaning the MPs must now declare any shareholding or public partnership exceeding 5%. This change was motivated by increased media scrutiny during COVID-19 pandemic, particularly concerning MPs involved in crucial sectors, such as companies selling face masks. The reduction in the threshold aims to increase public trust in the political system and ensure greater transparency among MPs (Q2).

[5] This assessment is repeated every five years in the Federal Criminal Police Office and will be carried out in full for all offices in the Federal Police in 2021 (due to major organizational and staff changes).
[6] Due to the interviewee's background, the interview focused exclusively on members of the Bundestag.

Risk analysis method

Germany employs a manual risk analysis method for assessing MPs' declarations **(Q3).** There is currently no electronic or automated system to assist the verification process; all checks are carried out manually by the Division responsible for monitoring compliance **(Q4).**

The process begins when an MP submits a declaration, either in hard copy or via email. Once the declaration is received, the Division performs a plausibility check to ensure the data is accurate. If any inconsistencies or potential breaches are identified, the Division will request clarification from the MP. Once data is confirmed, it is entered into a database and made publicly available. If discrepancies are discovered through further investigation, including cross-checking with external information, the MP is asked to provide clarification again. If the MP fails to comply with these requests, a formal sanctioning procedure is initiated **(Q5).**

Every declaration submitted by an MP is assessed **(Q6)**, and the Division has not encountered any major issues in implementing the risk analysis mechanism. While staff was previously limited, the verification process has become easier as it now involves nine individuals. Moreover, MPs typically take their compliance obligations seriously, and many of them proactively seek clarification before submitting their declarations, in order to minimize errors and ensure accuracy **(Q7)**.

Risk indicators ("red flags")

Risk indicators, or red flags, are used to identify declarations that might be "at risk". For instance, late submission of a declaration is considered a red flag, and if an MP fails to submit their declaration on time, a sanctioning procedure is triggered. Additionally, in case of indications (e.g. information by third parties or the media) that a Member of the Bundestag has failed to meet his or her obligations under section 45 of the Members of the Bundestag Act, the Division will request clarification. If the MP does not clarify the situation, a sanctioning procedure follows **(Q8)**. The Division identifies red flags through the submission process and cross-checks with third-party information **(Q9)**. Risk levels are determined based on the severity of the issue identified **(Q10)**.

Consequences

All "at-risk" declarations are subject to verification **(Q12a)**. The verification process is carried out by the Division **(Q12b)**. consequences of a declaration being flagged as "at risk" involve the initiation of a formal procedure in which the MP is asked to clarify the discrepancies. MPs are usually given one month to provide clarification to the President of the Bundestag.

If the MP fails to address the issues or fails to clarify potential breaches, the Division conducts further steps of the legal sanctioning procedure regulated in section 51 of the Members of the Bundestag Act on behalf of the President. The sanctions are proportioned to the severity of the breach. In case of minor negligence (e.g. exceeding the time limit for declaring information by no more than three months), the Member concerned shall receive an admonishment by the President. Where this is not the case, the Presidium of the Bundestag, which is composed by the President herself and her Deputies (usually one member for each political party represented in the Bundestag), shall then state whether a breach of obligations has taken place. A statement by the Presidium that a Members of the Bundestag has failed to meet his or her obligations shall be published as a Bundestag printed paper. A statement that no breach of obligations has been committed shall be published at the request of the Member of the Bundestag. Beyond that the Presidium may impose a fine, the amount of which shall depend on the gravity of the case in question and the degree of fault. The fine may amount to up to half of the annual Members' remuneration.

While minor breaches are handled confidentially, more serious violations, such as unreported paid side activities, are made public. In cases of severe breaches, fines may be imposed, and these fines are collected by the President of the Bundestag. The information circulates within the Division and the President and/or the Presidium **(Q13)**.

Digitalisation

Currently, Germany is working on implementing an e-filing system to support the risk analysis process. While the digitalization of data submission could make the process more efficient, the plausibility check would still need to be performed manually to ensure the accuracy and relevance of the data published. The introduction of an electronic system could also help raise awareness among MPs about the importance of timely submission of their declarations **(Q14)**. However, legal and technical challenges remain, and for now, the verification process continues to rely on manual methods **(Q15)**.

2.1.4 Italy

Background information

The AID system for Politically Exposed Persons (PEPs) in Italy was first introduced by Article 9 of Law No. 441 of July 5, 1982, which regulates asset and income declarations, as well as those related to electoral propaganda expenses by members of Parliament. These declarations are published annually in a printed bulletin by the Office of the Presidency of the Chamber (Ufficio di Presidenza della Camera) and made available to voters. In 2013, with Decree-Law No. 149, further provisions were introduced, including the mandatory publication of asset and income data for Parliament members on the official website of the Italian Parliament. This was in accordance with Legislative Decree No. 33 of March 14, 2013, and Law No. 441 of 1982, requiring the publication of donations exceeding €3,000 annually and any individual donations exceeding €500. Each member's personal page on the Chamber's website publishes the corresponding asset and income documentation, along with any additional documentation voluntarily made public by some deputies at the start of the legislature.

For directors and governing bodies of public administrations, each administration is responsible for publishing the declarations of its employees, with oversight of non-publication delegated to the RPCT (Responsible for Preventing Corruption) and ANAC **(Q1).**

Over time, the obligations for asset and income declarations have gradually extended, especially with the introduction of best practices for Politically Exposed Persons (PEPs) in 2018 by the Bank of Italy, which aimed to enhance the due diligence procedures for managing relationships in anti-money laundering contexts **(Q2).**

Risk analysis method – Risk indicators ("red flags")

Legislative Decree No. 149 of December 2013 establishes the specific procedures governing asset declarations, interest disclosures, and incompatibility statements. Each declaration is reviewed internally by the relevant institution through its designated anti-corruption office, without the support of a standardized or automated risk analysis framework. The Italian AID system is characterized by a pronounced decentralization, wherein each public administration independently establishes its own methodological criteria to comply with statutory declaratory obligations. This decentralized approach results in a tailored mechanism for each administration, adjusted to its organizational and managerial needs, as well as to the number of employees. For instance, in certain independent administrative authorities with a relatively small workforce, it is feasible for every single declaration to be collected and

subjected to comprehensive audits. Conversely, in large public administrations with thousands of employees, such a medium/large-sized municipal administration, declarations with may undergo sampling-based verification. In such cases, the system is so decentralized that the criteria for selecting declarations for in-depth verification can be determined by the advisers at the helm of individual services within a municipal administration.

Consequences

Each administration is the competent authority for carrying out verification. Once an "at-risk" declaration is identified, the relevant administration must verify it **(Q12a).** According to the general obligation for public officials, they must report serious crimes they become aware of during the performance of their public duties **(Q12b).**

If an individual administration fails to publish declarations or does not carry out verification procedures for "at-risk" declarations, this behaviour is considered a risk for the administration itself. In such cases, citizens or stakeholders can report the situation to ANAC, which will initiate its own verification process. The individual administration keeps information regarding the verification procedures it initiates, and in some cases, ANAC also holds this information **(Q13).**

Digitalisation

Digitalisation plays a key role in enhancing the transparency of information and facilitating its publication in the transparent administration section, as well as enabling automatic verification **(Q14).**

However, the main challenges related to the implementation of digital risk analysis mechanisms are primarily organizational. The responsibility for risk analysis has been delegated to individual administrations, leading to a distributed and fragmented structure. This can make it difficult to develop and apply a unified risk analysis. A potential solution to this challenge would be to establish a consistent legal framework and implement a transparency platform by ANAC, which would provide unified access to all sections of the transparent administration **(Q15).**

In terms of financial transaction risk analysis, digital tools have already been widely implemented to support the process. In the context of anti-money laundering, the UIF (Financial Intelligence Unit) has introduced specific anomaly indicators to assist obligated entities in identifying suspicious transactions, in line with its responsibilities under Article 6, paragraph 4(e) of Legislative Decree No. 231/2007.

2.1.5 Latvia

Background information

The Public Officials Declarations Information System (PODIS) has been operational since 01.01.1997: data from public officials' declaration started to be entered and stored as well as lists of public officials submitted by the institutions and their verification materials. From 2010 became mandatory the electronic submission of declarations for public officials and, one year later, also the submission of all lists of organizations was required to be electronic **(Q1)**.

A new information system, the Payment Administration Information System (MAIS), was developed in 2020. All information on declarations by public officials since 2014 has been transferred from PODIS to MAIS. Only lists of officials submitted since 2020 are available in MAIS. Since the development of MAIS in 2020, the functionality of the information system and the automation of the declaration checks have been improved. Also from 2020, declarations and lists of public officials are accepted and processed in

the Payment Administration Information System (PAIS). Submitted declarations are cross-checked with 19 evaluation criteria, previously defined in the MAIS classifier. The introduction of MAIS provides a broader approach to the verification declarations by public officials. It allows for a comparison of the submitted declarations with information provided in declarations submitted in previous reporting periods (if there is any), as well as a broader classification of the evaluation criteria of the submitted declarations in MAIS. Thus, the declarations of public officials are checked also against the non-validated assessment criteria of the MAIS classifier **(Q2 and Q3)**.

Risk analysis method

Latvia has implemented an automatic risk analysis mechanism thanks to the Payment Administration Information System (MAIS) **(Q3)**.

In order to improve risk analysis, minimise manual work, develop efficiency and save resources for the verification process, in the MAIS was implemented a new risk functionality for public officials' declarations in 2024 (the "Public Officials' Declarations Risk Assessment Report"). This new functionality provides for a more extensive comparison of the data furnished in the public official's declaration with the data held by the SRS and the data available in the information system of other institutions. Moreover, it introduces automated notification of officials about the risks identified. As can be observed by this implementation, the risk analysis system is constantly being improved **(Q7)**.

In the process of verifying the declarations of public officials, the information provided in the declarations is compared with the information provided in previous reporting periods (if any existing), and the information provided in the declaration is compared with the information available to the State Revenue Service (SRS). If necessary, an in-depth examination of the procedure for submitting and completing the declaration is carried out through the request and assessment of additional documents not available to the SRS (e.g. certificates, contracts, explanations, account statements).

Concerning risk analysis, two case-scenario can be pictured:

(1) Declarations are received automatically in the Electronic Declaration System (EDS), the MAIS confirms all the established criteria for the evaluation of the declarations at the moment of the data entry, and the system itself automatically validates the declarations and if no compliance with the above criteria is found, it makes data public in the SRS database.
The return is, then, manually checked by a member of the Data Administration Unit of the Public Information System against the assessment criteria not validated by the MAIS classifier.

(2) Declarations submitted to ESD for which the MAIS has not validated one of the assessment criteria set out in the classifier, are checked manually through an in-depth verification comparing declarations with additional documentation.

In this case, the check is not automatically validated by the MAIS during the initial check of the declaration and further examination is requested.

After this manual checking of the declarations, an official of the Public Officials' Data Administration Unit manually approves or rejects the declarations in the MAIS **(Q5)**.

Considering the recommendations of GRECO, internal regulation of the SRS identifies the public officials whose declarations submitted are subjected to mandatory manual verification. Special attention is paid to senior public officials: by law, their declarations are always manually checked. These senior public officials are: the President, Members of Parliament, the Prime Minister, the Prime Minister's Deputies, Ministers, Ministers with special responsibilities, Parliamentary Secretaries, Advisers to Ministers, Heads of Ministerial Offices, Assistant Ministers, Advisers to the Prime Minister, Advisers to the President,

Sectoral Advisers, Head of Protocol to the President, Adviser (foreign affairs), declarations submitted by the Deputy Chief of Protocol to the President of the Republic of Latvia, Economic Policy Adviser to the President of the Republic of Latvia, external consultative advisers to ministers, municipal council chairpersons, municipal council executive directors, municipal council deputies, university rectors, university councils, university senators and members of the boards of state and municipal capital companies, and civil servants and employees working for the State Revenue Service **(Q6)**.

Precisely, the KNAB (Corruption Prevention and Combating Bureau) checks declarations of some 1000 officials and, of these, some 150 undergo in-depth inspections, in accordance with KNAB's guidelines and internal thematic priorities. These set the criteria for in-depth inspections such as the public official's position in the hierarchy of public governance, functions, high exposure to conflicts of interest, prior sanction for LPCOI (Law on the Prevention of Conflicts of Interest in the Activities of Public Officials) violations, and media alerts.

Risk analysis method – Risk indicators ("red flags")

The criteria developed by MAIS and employed during the risk analysis **(Q8)** are listed below (*Tab. 1*).

Tab. 1. Criteria developed by MAIS and employed during the risk analysis of asset and interest declarations in Latvia. Year: 2025.

Criterion	Rationale
"Beneficiary" section not completed	If there is at least one entry in the "Beneficiary" section of the declaration, a manual check must be carried out.
Declaration does not have a job category that requires manual acceptance	If the declaration includes a post with category 1, 2, 3, 14 or 15, the declaration must be manually accepted
For income with the type "Salary", the corresponding posts are indicated	In the "Income" section of the return, all income with the type "Salary" must indicate the occupation as the main occupation, or in the "Additional occupations" section
The main job is shown in income as "Salary"	The person's main place of work must be shown on the declaration under "Income" with "Type of income" = "Salary"
Marked as an attorney-at-law and indicating the position	If one of the sections of the return - "2. Positions", "7. Income", "8. Transactions", "11. Benefits received" - is marked "No subs. Adv. Prof. activity", then the declaration must be manually checked.
Cash holdings up to a certain amount (per line)	If one line in the "Cash provisions" section shows an amount greater than the amount in the configuration, the declaration must be manually checked.
Declaration submitted by the deadline	If the date of submission of the return in EDS is higher than the due date for submission of the return, the return must be manually checked.
Total income up to a certain amount	If the amount of income in EUR in the "Income" section exceeds the configured value, the declaration must be manually checked.
No material change in declared cash savings	If the sum of the cash and non-cash accumulations declared in the previous declaration and in this declaration exceeds the defined parameters, a manual check of the declaration must be carried out.
No material change in the total amount of debt in the declaration	If the sum of the debts declared in the previous declaration and in this declaration exceeds the defined parameters, a manual check of the declaration must be carried out.
No material change in the total amount of loans in the declaration	If the sum of the loans declared in the previous declaration and in this declaration exceeds the defined parameters, a manual check of the declaration must be carried out.

Criterion	Rationale
3 months have not elapsed since the date of publication of the declaration	3 months have passed since the declaration was published in the PDB
The declaration has a corresponding list of officials	If the declaration does not have a list of officials, the declaration must be manually checked
The declaration must include all the positions held	If the declaration does not include all the positions held by the official, a manual check is required
For a declaration submitted for the first time, a declaration already exists for the selected period	The person already has a first-time return in the selected tax period and return type that is not in Rejected, Planned status.
No material increase or decrease in income	If there is a significant difference between the total income declared in the previous year's current return and the total income declared in this year's current return, the return must be manually checked.
All details of relatives are given	The criterion checks the relationship data in the MAIS and whether it matches the data provided in the declaration. If not, all relatives are listed in the declaration, a manual check must be carried out.
Types of income not exceeding the aggregate amount	If certain categories of income in the "Income" section exceed the configured amount value in EUR, then the return must be manually checked.

Source: table provided by the State Revenue Service (SRS) of Latvia.

The most significant risks are selected and assessed to detect large-scale inaccuracies in the SAP Business Objects DNA report **(Q9)**. This model contains its own "Risk criteria for declarations by public officials" **(Q8)**:

- No material change in declared cash savings.
- The shareholding data in the declaration corresponds to the data held by the Companies Registration Office.
- Cash savings reported in the declaration are not significantly different from those reported to the SRS.
- Total income is not significantly different from the bank's data.
- Total income does not differ significantly from the data available to the SRS.
- The data of the immovable property indicated in the declaration corresponds to the Land Register data.
- The total amount of transactions does not differ significantly from the data available to the SRS.
- Total indebtedness does not differ significantly from the data available to the SRS.
- The total amount of loans does not differ significantly from the data available to the SRS.
- The data on the tractor as provided in the declaration do not differ significantly from the data held by the SRS.

The level of risk of the declaration is determined by assessing the effectiveness thresholds **(Q10)**:

- Comparison of income with information provided by banks from €15.000.
- Increase/decrease in cash provisions from €15.000.
- Increase/decrease in indebtedness from €15.000.
- Increase/decrease in loans from €15.000.
- Transactions of €80.000 and above.

The Public Officials Data Administration Unit evaluates and, if necessary, updates the settings of the 12 criteria of the procedure of acceptance and processing of the public officials' declarations of the MAIS on

an annual basis, which are configured according to the tolerance level, the national minimum salary and other conditions (Q11).

Consequences

As was highlighted before, there is a risk threshold and 25% of risk declarations with higher, more significant risks are checked (Q12a). The competent authority for the following verification is the State Revenue Service (Q12b).

Supervision of abidance by PTEFs (Preventing corruption and promoting integrity in central governments) with the LPCOI (Law on the Prevention on Conflicts of Interest in the Activities of Public Officials) requirements is split between the KNAB (Corruption Prevention Bureau) and the SRS (State Revenue Service), pursuant to an agreement concluded between the two bodies in 2012. Both check public officials' asset declarations albeit from different perspectives. The KNAB uses the declarations as a tool to identify conflicts of interest and examines the legality of officials' activities from the point of view of their compliance with the LOCI-prescribed restrictions and incompatibilities. The SRS implements national tax policies and screens officials' assets to check the legality of their income and establish compliance with the tax legislation.

A public official may update the declaration no later than three months after the declaration has been published in the SRS Public Disclosure Database.

It is mandatory to update the declaration within one month after:

- A ruling in administrative offence proceedings has entered into force.
- A ruling has entered into force in criminal proceedings.
- A minor offence has been established.
- In other cases where the person has been notified of discrepancies found in the declaration of a public official.

Supervision is exercised ex officio, following complaints, whether submitted directly to the KNAB or reported anonymously via hotlines, as well as media reports. An in-depth inspection entails a detailed assessment of the public official's duties, his/her asset declaration and comparing it with the one submitted in the previous year and with information available from public registries. Where an illegal combination of offices and incompatibilities are identified, an administrative case is to be opened and charges for breaches filed.

The SRS imposes sanctions under Article 166 of the Administrative Violations Code for failure to submit a declaration or to submit it on time, non-observance of procedural requirements, and submitting a false declaration. If false information on large amounts of illegal income is detected, the case is to be forwarded to the Finance Police for criminal investigation. Compared to the KNAB, no internal criteria for in-depth verifications in respect of those public officials who may be susceptible to higher corruption risks and no internal procedure on how to conduct such assessments have been elaborated, including for the purpose of manual checks of declarations submitted by the Prime Minister and ministers. More in-depth verifications could only be carried out in response to external requests, although the meaning of an "in-depth" verification has not been defined.

Digitalisation

According to the interviewee's opinion, digitalization could improve/support the risk analysis mechanism, considering their well-functioning, fully automatic risk analysis system (Q14). However, there were technical and financial difficulties in implementing the system (Q15).

2.1.6 Moldova

Background information

In Moldova, the AID system was first developed and implemented in 2011. At first, it was a rather rudimentary paper-based system which involved two declarations: one about assets and one about personal interest. Questionnaires were delivered to declarants of each institution, and the answers were collected by the *collector*[7]. However, the system appeared to be quite ineffective so, after a short period of time, Moldova started to negotiate with the World Bank to fund the development of an automatic system for submitting, analysing and delivering results **(Q1).**

The E-integrity[8] system was implemented in 2018 and became operational on January 1st, according to the new Law of Asset Declarations (Law 133/2016[9]). The new law obliged all declarants[10] to submit their declarations only electronically. At first, it was a difficult and revolutionary change in Moldova because many people had no familiarity with electronic devices nor online submission **(Q2).**

Now, when declarants enter ANI website, they simply must click on "*submit declaration*". Once they click this button, they enter in the E-integrity system. The following step is authentication, which can be done either through electronic signature, mobile signature or electronic ID. After authentication, they must insert their primary password.

[7] The previous *collectors*' mission is to provide declarants with electronic signatures, which are devices, like an electronic stick. They provide these devices and input primary information such as the declarant's name, the number of orders they give and the name of the institution they work for. Then, the subject of the declaration and the system access are set. They have no further influence or intervention in the system, as they are only responsible for providing the signature, while each declarant is now responsible for entering and submitting their declaration.

[8] In 2018, the National Integrity Authority (ANI) launched the e-Integrity system, regulated by Government Decision No. 228 on April 10, 2020. The main scope of the system includes: submission and signing of asset declarations, automated verification of declarations against state register data, management of control files based on notifications or *ex officio* investigations, updating information in the electronic register of declarants, managing prohibitions on holding public office. The system goes beyond the basic legal requirements by making declarations publicly available immediately after electronic signing, instead of waiting for the 30-day period of time required by law. Declarants access the system through the ANI website using a username and password or a digital certificate. After completing the online form, they must sign it electronically; once signed, the declaration is automatically published on the website, and the official receives email confirmation. Personal data, other than names and surnames, are blurred. The system allows searches of asset declarations by parameters such as name, declaration type, reporting period, organization, department, region/city, and function. Transparency International, media and CSOs in Moldova have requested that declarations be made available in machine-readable formats to facilitate analysis. For a while, investigative journalists manually analysed PDF documents, with inefficiencies in the blurring of personal data. On 27.03.2025, the Law 133/2016 was amended, and art. 9. states that ANI publishes the submitted declarations on its official website "*in a format that allows automated data processing (open data)*". Currently, ANI is working with external donors to implement the publication of the declarations in open data format.

[9] Two main laws of Moldova regulate the requirements for submission and verification of asset and interest declarations – the Law on the Asset and Interest Declarations (Law n. 133 of June 2016) and the Law on the National Integrity Agency (Law n. 132 of June 2016). Law n. 132 regulates two types of "control" that concern declarations:

1) "Control of declarations" ("*controlul declarațiilor de avere și interese*"; Article 27) which means control of the timely submission and control of compliance with the declaration form;

2) "Control of assets and interests" ("*controlul averii și al intereselor personale*"; Article 28) which means an in-depth verification of information on assets and variations of wealth.

Law n. 132 (Art. 27.3) requires that out of all declarations that ANI controls during a calendar year at least 40% should be those of the declarants holding responsible positions and ANI should randomly select such declarations for the verification ex officio ("40% rule"). It appears that this requirement concerns only "control of declarations", that is the control of timely submission and formal compliance with the form, and that it does not extend to the in-depth verification ("control of assets and interests"). In World Bank, *Risked-based verification of asset and interest declarations in Moldova*, February 2020.

[10] The only exception is regulated by Article) of Law 133/2016, which establishes that those subjects whose identity constitute a secret of State (e.g. Intelligence Service) should submit a paper-based declarations to their designated collectors.

Risk analysis method

In general, it is not possible to verify all submitted declarations because, before the recent amendment of the law, there were about 58,000 declarants. Now, the number has increased to 65,000 declarants. The inspectorate verifies roughly 1,800 to 2,000 per year **(Q6).**

At the end of the declaration period, by March 31st, the president of the authority issues an executive order. In this order, they define the "red zone" or risk criteria. For example, every year, for the past seven years, judges, prosecutors, and members of Parliament are subject to verification, 100% of them. This also includes high-ranking officials such as the President, Prime Minister, Ministers, Secretary General, Secretary of State, and heads of agencies. This constitutes a significant portion of the verification process, and it is mandatory. Another part of the verification process is based on risk analysis **(Q5).**

The verification process is quite challenging and lengthy. Currently, the process is manual: an integrity inspector analyses the submitted declarations and cross-checks them with other available data sources. However, once the automated system is implemented in the future, the risk assessment will involve a combination of both automatic and manual checks.

Regarding the current legal framework, the verification of asset and interest declarations involves several steps. First, it checks whether the declaration was submitted on time, whether the subject of the declaration complies with formal requirements, and whether the subject of the declaration complies with formal requirements, and whether there is any apparent relation between the legal regime of the declarant and the assets or personal interests they declare. The verification process begins after the submission deadline has passed.

Declarations subject to annual verification are selected randomly, based on risk factors such as corruption risk and the vulnerability of the declarants. The criteria for selection are approved annually by the Integrity Council, which functions similarly to a supervisor board, like the Board of ANI. As a part of the verification process, at least 30% of the submitted interest declarations verified in a calendar year must come from high-ranking officials such as the President, Members of Parliament, Ministers of State, judges, prosecutors and heads of certain autonomous public institutions and authorities.

Due to the limited number of integrity inspectors and the time-consuming nature of the process, only a mandatory sample of subjects is verified each year. Additionally, certain institutions are randomly selected for verification. For example, this year, the heads of departments in the Ministry of Internal Affairs were verified, while last year, only the heads of departments in the Custom Service were verified, not all employees.

The assignment of declarations and verification is done randomly by the electronic distribution system, which is part of the E-integrity system. The distribution of cases is mandatory and tied to the case file. Each verification must be completed within two months from the date of their distribution. Once completed, it is finalised in a brief protocol published on the ANI website.

Risk indicators ("red flags")

The Supervising Committee establishes the criteria, based on ANI specific proposals (e.g. corruption risk and vulnerabilities). However, ANI does not participate in the decision-making process that ends with a set of criteria. However, the final decision matches the proposal.

ANI, on the other hand, proposes the criteria based on the analysis of possible areas of trespassing or breaching the law from the representative of some agencies, and then they narrow down the focus. The risk level is determined by a combination of around ten criteria. If a declaration matches the ten criteria, then it is selected for in depth verification **(Q8)**.

Consequences

If, upon verification, it is found that a declarant has not submitted or has submitted the asset and interest declaration late, the integrity inspector imposes the corresponding administrative sanction. If the declarant fails to submit the declaration, the inspector issues a request for submission within 30 days. Failure to submit the declaration within 30 days of receiving the request constitutes grounds for termination of the subject's mandate, employment, or service relationship.

If, during the verification of a specific interest declaration, there is a reasonable suspicion of a criminal offense or violation of tax legislation, the integrity inspector notifies the law enforcement authorities[11]. Alternatively, the state tax service informs the President of ANI. In such cases, the integrity inspector continues the verification procedure, while the law enforcement authorities and the state tax service are required to inform the inspector of the decision taken. The authority also has the right to challenge the decision of these institutions.

If, following verification, the integrity inspector identifies an apparent violation of the legal regime regarding asset and interest disclosure – such as failing to declare all assets and interests, providing erroneous or incomplete declaration, or finding a substantial discrepancy between the subject's income, expenses, and acquired assets – the inspector initiates a referral for a full review of the subject's assets and interests.

Additionally, if the integrity inspector finds an apparent violation concerning conflict of interest, incompatibilities, or restrictions during the verification of assets and interest declarations, they initiate a referral for verification of compliance with these legal provisions.

Basically, if during the control of a declarant's legal assets, the inspectors gather more material than necessary for their findings (meaning they find documents or evidence beyond what is needed for their report), these additional documents are also sent to the tax service. However, in recent years, such cases have not occurred, probably because the situation has changed in some way. The tax service has a threshold for discrepancies (meaning a significant difference between the declared assets and financial data) of 500,000 lei, while the inspectors have a lower threshold, which is 20 average salaries per economy for the current year (16,100 lei), which in 2025 amounts to 322,000 lei. Therefore, if the discrepancies found by the inspectors do not exceed 500,000 lei, the tax service is usually not interested in their findings, as it considers these discrepancies too small to intervene, according to their own standards.

Digitalisation

Moldova is currently working with development partners to create a new automated system to carry out verification of declarations through cross-checking with databases. The M-Connect[12] system is expected to be implemented within two years. The system would allow to automatically verify all declarations, but also to select throughout verification those declarations where the system identifies a higher risk level, and this will trigger manual in depth verification **(Q14).**

[11] In 2024, only 2-3 out of 46 referrals made by integrity inspectors were sent to the Prosecutor's Office.

[12] MConnect currently verifies data from the following national registers: Citizen Register (ID cards, passports, residence), Civil Status Register (birth, marriage, death), Motor Vehicle Register, Real Estate Register, Tax Administration Registers, Business Entities Registers, Social Welfare Register. MConnect is a government-to-government (G2G) and government-to-business (G2B) data exchange (interoperability) platform, integrating over 53 public institutions and increasingly the private sector (banks, utilities) in real time. Public authorities exchange data in real time, through this platform, without requesting it from citizens and the business environment in the form of certificates, reports, etc. In Regional Anticorruption Initiative (RAI), *Assessment of the legal framework and technical capacities to conduct asset declaration collection, verification, and exchange of data with other jurisdictions in the Southeast Europe - REPORT*, January 2024.

The biggest challenge with digitalisation does not regard financial or technical obstacles. The biggest challenge was to push this draft law through the Parliament, thanks to the specialized Commission. Nonetheless, the most recent amendments to Law 133/2016, which implements the digitalization of the declaration verification process, were operated on 27.03.2025 **(Q15)**.

2.1.7 Montenegro

Background information

The Asset and Interest Disclosure system in Montenegro was first implemented in 2012 under the Commission for Prevention of Conflicts of Interest. Initially, the verification of asset and interest declarations was conducted entirely manually. However, in 2016, the Agency for Prevention of Corruption (APAC) took over as the legal successor of the Commission. The APAC began implementing electronic networking and cross-checking of databases from relevant Montenegrin institutions, such as the Police Administration, Tax Administration, the Central Bank, and others **(Q1)**. Information system currently verifies information from the following national registers by calling respective web services established via direct (peer-to-peer) connection with competent institutions (RAI, 2024).

The information system currently verifies data from the following national registries via web services established through direct (peer-to-peer) connections with competent institutions:

- Motor Vehicle Register – APAC has access;
- Real Estate Register – APAC has access;
- Register of Securities – APAC has access;
- Tax Administration Registers – APAC has access;
- Business Entities Registers – APAC has access;
- Credit Registers of the Central Bank – APAC has access;
- Criminal Register – APAC has access;
- Citizen Personal Status Register (birth, marriage, death) – APAC has access;
- Register of Ships/Vessels – APAC does not have access;
- Citizen Register (personal IDs, IDs for foreigners, passports, personal ID number, residence) - The Agency has access **only** to the Citizen Registry for residence and personal ID number. As for searching data related to personal IDs, foreigners' ID cards, and passports – APAC does not have access.

In 2024, the system for controlling asset declarations was upgraded and became fully operational in the second half of 2024 **(Q2)**.

Risk analysis method

Montenegro uses a mixed approach for risk analysis when assessing IA declarations **(Q3)**. This method combines both manual and automated processes. The system's risk analysis framework is based on the recommendations of expert Quentin Reed, who provided guidelines to the APAC in cooperation with the Council of Europe. These guidelines mainly focus on identifying most significant discrepancies, often referred to as "red flags", rather than attempting to detect every minor irregularity. The goal is to prioritize and focus on potential issues that could lead to corruption or other legal violations **(Q4)**.

In the period from 2016 to 2023, the Agency's Information System was developed and maintained by the Serbian software development and system integrator company. Since 2023, this role has been taken

over by the software company "B-ONE" LLC, Podgorica, specialized in the development and implementation of software solutions (RAI, 2024).

The risk analysis process has evolved during time:

- 2012-2016: during this period, risk analysis was conducted manually, with no electronic verification.
- 2016-2024: the process became a mixed system, where both manual and electronic verifications were employed. This allowed the APAC to cross-check asset and interest declarations with various institutional databases. However, the process still faced challenges, particularly with regard to irregularities such as ownership histories or transaction record of properties. In some cases, institutions had to be conducted for additional documentation or data.
- Post-2024: with the implementation of a more advanced system in 2024, the risk analysis process was expected to improve. However, the system still faces challenges in accurately identifying red flags automatically, therefore requiring manual verification in certain cases.

The verification of interest and asset declarations involves several steps (Q5):

1. Administrative verification: the first step focuses on checking the basic accuracy and completeness of the data submitted in the reports/declarations. Reports are compared to official registries, and the consistency is verified. In this phase, all received declarations are checked (Q6).
2. Further verification: for a specific number of officials who have submitted reports/declarations, a more detailed methodology is applied. This phase is performed according to the CAO plan. This ensures that a particular group of public officials is verified, while another group is selected randomly (or through sampling) to undergo verification. This step ensures that both specific and random samples of officials are reviewed.
3. In-depth verification: this step involves a more comprehensive verification method, and it is conducted according to the CAO plan. It focuses on a small number of officials, selected according to specific criteria such as their role, ability, level or exposure to potential corruption. This type of verification is carried out when a procedure has already been initiated earlier based on reports from legal entities, *ex officio* reports, or other sources. In this phase, the process involves cross-referencing the data across all network databases or relevant institutions. It also includes obtaining data from competent state and local authorities, public enterprises, companies, institutions, and other legal entities.

Risk indicators ("red flags")

Several indicators are used to qualify a declaration as "at-risk". The most common red flags include: discrepancies between the declared assets and the actual financial status, reports of previous violations by the same individual or organization, information obtained from external sources such as media, NGOs, or whistleblowers, failure to report ownership of asset or failure to update information on time, refusal to provide access to bank account data, multiple or repeated violations of the law, conflict of interest (Q8).

Through practice, the efficiency of the systems progressively improves, as red flags are periodically updated with new data (Q10).

The identification of red flags involves comparing current reports with previous declarations and verifying the data across institutional databases. The recurrence of violations, such as failing to report changes in assets or misreporting financial information, plays a crucial role in determining the level of risk. The more significant the irregularity, the higher the risk (Q9).

The risk level is primarily determined by the severity and recurrence of irregularities. For example, the combination of unreported wealth, discrepancies in property ownership, and multiple violations may trigger further investigation. A high-risk declaration can be subject to deeper scrutiny to identify potential violations and consequently impose sanctions **(Q10)**.

Consequences

In Montenegro, a "risk threshold" exists to trigger verification of declarations. If a declaration contains multiple risk indicators, it is automatically flagged for further verification **(Q12a).** Special attention is given to individuals holding positions in State authorities with significant decision-making power, such as in sectors like healthcare or education, which also have a larger impact on the population.

The Agency for the Prevention of Corruption is the main competent authority for verification **(Q12b).**

Once a declaration is identified as "at-risk", additional information is gathered to confirm or dismiss the suspicions. Requests for further data are sent to relevant institutions, and the verification process continues until a conclusive decision is reached **(Q13)**.

Digitalisation

Digitalisation has played a crucial role in enhancing the risk analysis process in Montenegro. The implementation of electronic networking of databases in 2016 marked the beginning of a more integrated system. Despite this, the new system introduced in 2024 still faces technical challenges. As a matter of fact, it is not yet fully capable of automatically detecting red flags or irregularities, and there are issues with outdated or incomplete data **(Q14)**.

The primary limitations of digitalisation in Montenegro's risk analysis system are technical and legal. The new database, while an improvement, does not seamlessly integrate with previous systems, sometimes leading to inefficiencies. Additionally, the inability to track ownership histories or transaction records in real-time remains a significant barrier to effective risk analysis **(Q15)**.

2.1.8 Romania

Background information

The AID system was first implemented in Romania in 2007. Prior there were some normative acts that regulated the asset declarations and the conflict-of-interest disclosure, but a proper AID system became operational in 2007, when ANI was established. The operationalisation of the AID system occurred also because of the recommendations of the European Commission through the Mechanism for Cooperation and Verification (CVM).

After just one year, the law that originally established ANI was declared unconstitutional. However, the situation was resolved in 2011 when a new law, deemed constitutional, made ANI fully operational. In June 2017, ANI developed the PREVENT system, a tool to detect and eliminate potential conflict of interests in public procurement procedures (World Bank, 2021) **(Q1).**

Currently, there are some issues with a legislative reform that is a milestone under the Recovery Found, and that should also contain some adjustments suggested by the European Commission and GRECO. These are adjustments concerning regulations on incompatibilities and conflicts of interest that are currently very fragmented (about 200 acts). The focus of this reform is to align the provisions related to incompatibilities and conflicts of interest **(Q2).**

Risk analysis method

ANI is the authority responsible for managing the AID system and within the authority there are people called "focal points" that are responsible for the process: they have to properly apply the normative provisions on asset declarations. Such "focal points" can be found in every institution, and they are the ones that actually manage the process. The declarations are electronically submitted and sent to the responsible person within the institution the public official works for. This person, the designated focal point for the institution, first checks the submitted declarations for compliance and then sends them to ANI, the central institution responsible for the verification process **(Q4).**

The number of deponents every year is around 500,000 public officials coming from 40 different categories (in elective years this number rises to one million). Compared to ANI's personnel, the number of deponents is huge: that is why ANI's verification process can both be triggered by third parties reporting an integrity incident, but can also conduct the *ex officio* verification. So, verification is triggered mainly by notifications, which means that less than 1% of the submitted declarations are actually verified **(Q6)**.

Anyone—private citizens, media reports, whistleblowers—can send an alert that obliges ANI to verify the "at risk" declaration. It has also been developed a system (PREVENT System) that verifies a sample of declarations (based on the public position one wants to analyse), which are selected on several criteria: these criteria are previously chosen and, as a result, red flags are identified to trigger the verification by the inspectors. That is why Romania appears to have a proper operational electronic risk analysis system **(Q3)**. The implementation of an electronic system for risk analysis was recommended by GRECO, as it could help to highlight "at risk" declarations with red flags and prioritize them in the verification process, provided that there is a high number of deponents **(Q7).**

Risk indicators ("red flags")

Red flags are tailor-made, and each year can be updated **(Q11)**. According to the Survey results (WP2), some elements considered as "red flags" are: missing data, data inconsistencies or discrepancies (e.g. within the form, with past declarations, with external databases), behaviour inconsistent with the declaration (e.g. assets acquired above annual salary or set percentage of annual salary)[13] **(Q8) (Q9).**

Consequences

Verification is conducted by ANI through cross-checks between the declarations data and public registers: ANI has direct access to some registers ANI, while to some others it has to ask for the access (e.g. banks). The system analyses data from integrity forms and performs cross-checks with databases from the National Trade Register and the National Register of Personal Records. It can automatically identify potential links between public decision-makers in the contracting institution and bidders[14] (World Bank, 2021) **(Q12b)**. When potential conflicts of interests are detected, the PREVENT System sends an "Integrity warning" to both ANI and the contracting authority. The contracting authority has the obligation to take measures to address the integrity risk (e.g. replacing a member in an evaluation committee, excluding a bidder), and the National Agency for Public Procurement verifies that the necessary measures have been implemented (World Bank, 2021).

[13] Answer to question 3.4 "*Which elements are identified as risk indicators ("red flags")?"* of the qAID online survey (WP2).

Digitalisation

Concerning digitalization, a great step forward was made between 2021 and 2022, with the implementation of a fully electronic submission system. However, the implementation of the electronic submission was not easy because of the requirement of the electronic certified signature: not everybody has that type of signature and, for this reason, the transition to an electronic system took two/three years (Q15). Now, there is a digital platform where every public official has an account and has to fill the form based on Romanian law. Thanks to the digitalization of the submission system, in Romania there is now a clearer image of the effective number of declarants and some loopholes concerning the fulfilling and completeness of the declarations have been solved (Q14).

Regarding the scope of the declaration, all assets, incomes, shares in abroad companies (there is the need to disclose the value of the shares and the market value of the shares) and conflicts of interest must be declared. The obligation is also applied to the spouse and children of the declarant.

2.1.9 Serbia

Background information

Serbia's AID system was first implemented in 2010. At first, it consisted of a completely manual mechanism in which declarations were written, and the hard copy was submitted manually. In 2012, a new e-filing system was introduced that allowed electronic submission (Q1).

Few years later, in 2016, the Information system was implemented. It is a custom-built application based on the eDocumentus platform for managing electronic documents and automating business processes. It was created by a Serbian software development and system integration company. It is intended to facilitate business operations for organizations that need to create, organize, distribute, and have insight into many business documents daily. Some key functionalities of the eDocumentus application include document identification and classification, recording, reviewing, change tracking, versioning and managing business processes. One of the main features of the eDocumentus is a modular enterprise system that provides advanced functions to users through additional software tools (RAI, 2024).

In 2020 there was an improvement of the electronic submission system. During the same year they started the application of a new law on prevention of corruption with the aim of helping public officials meet their declaration obligation. As a result, new web forms with the electronic signatures capabilities were introduced, making it easier for public officials to complete the declaration. Additionally, the scope of the declarations was extended to add new types of income (Q2).

Risk analysis method

Serbia reported to have a mixed risk analysis method (Q3) with electronic submission of declarations and manual verification (Q4).

Concerning the submission of the declarations, once public officials enter a public office they have 30 days to submit the declaration. Also, if/when there are some changes regarding the income or asset during the mandate, public officials are obliged to declare such modification. At the end of their mandate, or if they move office, public officials have 2 years to submit the asset declaration.

All declarations are presented to the Anti-Corruption Authority and a restricted number of them are selected to be verified based on risk elements identified annually through the adoption of the Annual Verification Plan by the director of the Agency for Prevention of Corruption (ACAS: www.acas.rs). This Plan is drafted in collaboration with other agencies such as the Conflict-of-Interest Department, the Control of

Political Activity Department, the Compliance Department, etc. The risk indicators that are generally considered in the Annual Verification Plan are income type, type and number of public servants that are working in certain public authorities, budget of institutions, specific areas prone to corruption, responsibilities and competencies of public authorities.

Once selected the categories, the Annual verification Plan is published on the ACAS website, so that public officials will know, at the beginning of the year, if they will go through verification that year. The number of declarations verified annually is approximately 200-300 **(Q6)**. Besides this, if during the year a report is filed, extraordinary verification will be conducted for a set number of public officials.

However, two years ago Serbia changed the guidelines for drafting the Annual Verification Plan and included new categories of high-position public officials (from executive and judiciary branch) in accordance with GRECO recommendations **(Q5).** Also, the Annual Verification Plan is drafted thanks to the collaboration between the Agency for Prevention of Corruption and other agencies[15].

There were no major difficulties in drafting the Annual Verification Plan even if the Law on Prevention of Corruption did not specify enough the categories that shall be selected **(Q7).**

Risk indicators (“red flags”)

The main indicator is the position of the public official but there are some other indicators such as his incomes, the number of employees in public bodies, the budget of public bodies and their competence **(Q8).** Indicators are identified using both internal (e.g., data regarding the number of complaints submitted against public officials) and external sources (e.g., report and research from civil society organizations) **(Q9)** and are periodically updated **(Q11).**

As categories of public officials whose declarations are verified during the whole year are predetermined in the Annual Verification Plan, there is no risk level that must be defined **(Q10)** nor a risk threshold that triggers verification **(Q12a).**

The main indicator is the position of the public official but there are some other indicators such as his incomes, the number of employees in public bodies, the budget of public bodies and their competence **(Q8).** Indicators are identified using both internal (e.g., data regarding the number of complaints submitted against public officials) and external sources (e.g., report and research from civil society organizations) **(Q9)** and are periodically updated **(Q11).**

[15] To ensure more efficient data control, the APC signed the Protocols on Business and Technical Cooperation with a number of institutions (e.g. Ministry of Interior, Republic Public Prosecutor Office, Commission for Protection of Rights in the Public Procurement Procedures, Commission for Protection of Competition, Public Procurement Office, Central securities depository and clearing house, Ministry of Finance - Treasury, Tax Administration, Customs Administration, Administration for the Prevention of Money Laundering, as well as with Business Registers Agency and Republic Geodetic Authority). There is also a Memorandum on Cooperation signed among the Supreme Court of Cassation, Anticorruption Council and Privatization Agency. On 13 July 2023, Serbian Business Registers Agency (SBRA) and Agency for the Prevention of Corruption signed a new agreement on data retrieval, which will enable the regular access and retrieval of data from the SBRA’s databases on business entities, beneficial owners, and related parties in the upcoming period. APC's Information system currently retrieves and verifies information by integrating with national GSB or NKOS platform from the following national registers: Citizen Register (personal IDs, IDs for foreigners, passports, personal ID number, residence), Motor Vehicle Register, Arms register, Business Entities Registers, Central Register of Compulsory Social Insurance. Authorized officers of the APC have created user accounts and have access via respective web sites to the following registers: Real Estate Register (metadata and ortho-photo records), Register of Securities. As per APC's request, National Bank of Serbia is sending data from the Central Bank Register of Commercial Bank Accounts in the form of a machine-readable file, which is imported into the Information System. APC sends a written request for data verification from Tax Administration records and receives data exported into PDF file via secure email system. Similar procedure is followed for bank account data verification from Commercial banks in the Republic of Serbia. In Regional Anticorruption Initiative (RAI), *Assessment of the legal framework and technical capacities to conduct asset declaration collection, verification, and exchange of data with other jurisdictions in Southeast Europe - REPORT*, January 2024, pp. 144-145.

As categories of public officials whose declarations are verified during the whole year are predetermined in the Annual Verification Plan, there is no risk level that must be defined **(Q10)** nor a risk threshold that triggers verification **(Q12a).**

Consequences

The Agency for Prevention of Corruption is the competent authority for asset declarations. Within the structure of the Agency, there is a specific sector for asset declaration control dedicated to registers and asset declaration (Asset Declaration Control Sector) and they often conduct a preliminary check (e.g. if declarations are submitted on time), while another sector conducts an in-depth analysis by checking the data of the declarations **(Q12b).** If any procedure is initiated following the identification of a red flag, follow-up information about the procedure is shared within the Agency **(Q13).**

Digitalisation

The electronic submission of the declarations helps public officials with the submission process and assists the agency in detecting technical errors (e.g. fields not fulfilled, fields filled with something not coherent) that are now fewer than 2010 **(Q14).**

The implementation of the e-filing did not encounter any limitation because if public officials find any difficulties in fulfilling the forms they can contact the Department of the Register to receive help in completing their legal obligation **(Q15).**

2.1.10 Ukraine

Background information

In Ukraine, the 2014 Revolution of Dignity (*Euromaidan*) led to the establishment of a new electronic asset disclosure system (World Bank, 2021). The Logical and Arithmetic control system (LAC) was first introduced in 2016 **(Q1).** The design of the system included an enhanced asset declaration form, secure data storage, and a public-access website separated from the main database to protect against data tampering. Submitted documents could not be altered or removed, and each one displayed the date and time of submission. Additionally, the system ensured free, read-only public access to the e-declarations and allowed for data reuse (World Bank, 2021). By 2021, the system of selection of declarations for full control through risk assessment became operational. In 2024, it was further enhanced and improved, and the scope of data evaluated was broadened from 31% in 2015 to 75% by 2024 **(Q2)**. This expansion is essential for improving the system's effectiveness in flagging potential risks and discrepancies in financial disclosures by public servants.

Risk analysis method

Ukraine employs a fully automated risk analysis system - Logical and Arithmetic Control system (LAC) **(Q3).** The risk analysis is fully automated, ensuring consistency and eliminating the need for human input in this initial phase of the process **(Q4).** Logical and Arithmetic control (LAC) is a tool that allows the Registry's software tools to identify inconsistencies between the information reflected in the declaration and the data in the registers and evaluate them. LAC is used to assess the risk of the declaration, which results in a calculated risk rating. The declarations with the highest risk rating are selected for full verification.

Each declarant must submit his declaration through his personal cabinet. After the submission, there is an automatic exchange of information/automatic verification between the information contained in the submitted declaration and the information contained in all the national registers, to which the National Agency for Corruption Prevention (NACP) has automated access. These registers (around 20) include information that is crucial for cross-checking the accuracy of the data provided in the declarations **(Q6)**.

The process involves two steps. It begins with the declarant submitting their declaration containing financial information through their personal account. Once the declaration is submitted, the system automatically cross-checks the information with external data in the national registers. If discrepancies are identified as a result of the data comparison, those are labelled as risks in the declaration and each risk is assigned a score.

The second phase involves the application of mathematical formulas and rules that identify risk in a declaration **(Q5).** Based on these evaluations, the system flags declarations as either "at-risk" or not. The triggering of at least one of the formulas is considered an identified risk. Each risk identified in the declaration has a weighting factor. The sum of the weighting factors of all identified risks is the calculated risk rating of the declaration. This is how the declaration's risk is assessed. All declarations to which the LAC is applied are ranked by the value of the risk rating indicator (from highest to lowest), which is taken into account when selecting declarations for full verification.

As a result of these two stages, all discrepancies detected by the machine are given a specific score (coefficient). Each discrepancy is considered to be an identified risk. Then, all scores are added, and the risk rating indicator of the declaration is deduced, and a number is appointed.

"Non-risky" declarations may be subject to and pass an automated verification if such a declaration contains information that can be verified with the data of the registers.

Risk indicators ("red flags")

The primary indicators used to flag a declaration as "at-risk" are inconsistencies between the data submitted in the declaration and the information in the external registers **(Q8)**. These discrepancies might include inconsistencies in reported asset, income, or other financial information that can be cross-checked against the data held in national registers **(Q9).**

The system also uses a set of predefined rules and mathematical formulas to identify these inconsistencies and assign a risk score to each declaration. For example, the formula for signs of illicit enrichment, when income, expenses and savings are calculated. If the expenses exceed the savings, the illicit enrichment formula is triggered. Such a declaration has the highest risk rating **(Q10).**

If discrepancies are detected, the system flags the declaration for further review. The NACP, responsible for overseeing the system, periodically updates the set of rules and the indicators used to determine risk. This ensures that the system remains adaptable to new forms of potential corruption or financial misconduct, such as emerging issues with cryptocurrencies or digital assets. Over time, the criteria and thresholds for what is considered an "at-risk" declaration are refined to maintain the system's effectiveness **(Q11).**

Consequences

When a declaration is flagged as "at-risk", the NACP initiates a process of full verification **(Q12a).** This verification is conducted based on the risk score assigned by the system, and, if necessary, the NACP will collaborate with other state authorities, such as the National Anti-Corruption Bureau, the National Police, the State Bureau of Investigation and prosecution authorities to conduct further investigation. Information from whistleblowers, the media, law enforcement agencies, as well as individuals and legal entities may

also serve as grounds for a full verification. If the verification uncovers that the declaration contains false or misleading information, further legal procedures may follow, including the initiation of administrative or criminal liability proceedings **(Q12b).**

Moreover, if a discrepancy is detected in a declaration, the NACP prepares a motivated conclusion and sends the relevant documentation to the pre-trial prosecution authorities, which may then conduct their own investigations. It's worth noting that cooperation between the NACP and other state authorities can vary depending on the nature of the violation. For example, in cases of administrative violations, criminal prosecution authorities may not be involved, but the NACP still works closely with other government bodies to address the issue **(Q13).**

Digitalisation

While the Ukrainian AID system is highly regarded for its digitalization and efficiency, it faces certain legal and technical challenges.

The most evident legal limitation is related to the cross-referencing of data between the submitted declarations and the external registers. Many of these external registers were established at different times and work with different systems, which means that there is not always a perfect alignment between the information provided in the declarations and the data stored in the registers. Therefore, a mismatch can happen between the scope of the information available in the registers and the data which should be reflected in the declarations.

For instance, some information concerning real assets to which rights were acquired before 2013 was not included in the registers, as the latter were developed from earlier systems. This information was collected by the Bureau of Technical Information, which did not fully exchange data with the newer registers.

On the other hand, technical problems can affect the different methodology that each register employs for recording relevant data. In particular, the fact that the information in the declaration is indicated in one text field, while in the register there are six text fields, makes it technically problematic to combine them.

Another technical difficulty concerns, for example, the so-called *tax identification number* (which is an equivalent to the Italian fiscal code). This number is not always indicated in the registers. So, especially for people with very common surnames, if the tax identification number is not reported, it can be extremely difficult to identify the subject to which the assets refer to **(Q7/15).**

Despite these challenges, digitalization has played a critical role in improving the overall risk analysis and verification processes. The AID system enables Ukraine to process over 1 million declarations annually, significantly enhancing the transparency, efficiency, and effectiveness of the verification of public servants' declarations **(Q14).**

2.2 Comparative analysis

The previously presented overview of risk analysis mechanism models has revealed both similarities and differences between them. In order to summarize these findings and offer a broader perspective in line with the report's objectives, it is useful to conduct a comparative analysis of the results. This analysis aims to highlight the outcomes of the interviews and identify best practices (see paragraph 3) by drawing attention to key features.

2.2.1 Risk analysis and verification

The interviews revealed that the distinction between risk analysis and the verification phase is often ambiguous in practice. While the two processes are conceptually distinct, operational overlaps are frequently observed. Risk analysis generally precedes verification, as it aims to estimate the probability that a declaration contains irregularities or signals possible violations. Verification, on the other hand, is a fundamental component in ensuring the effectiveness of asset and interest disclosure (AID) systems, as well as the enforceability of relevant legal frameworks, by enabling the imposition of sanctions when warranted. Without a robust verification process, AID mechanisms would be reduced to mere information collection tools, with limited utility in detecting or deterring corruption.

Verification enables competent authorities to confirm whether declarations have been duly and timely submitted and whether the disclosed data is accurate, complete, and truthful. As such, a minimum level of scrutiny is required to "establish a credible threat of detection" (StAR Initiative, 2012: 60). Risk analysis often functions as a triggering mechanism for verification or serves complementary functions to enhance its effectiveness (Kotlyar & Pop, 2021).

The findings from the research indicate the existence of three primary models of risk analysis: fully electronic, fully manual, and hybrid. The hybrid model appears to be the most widespread, due to several factors. First, the transition from manual to electronic systems typically necessitates a gradual, mixed-method approach. Second, domestic regulatory frameworks may pose structural or legal constraints to full IT integration. Third, hybrid systems are better equipped to process a variety of alerts, including those derived from cross-checking with external databases and from media or public reports.

The implementation of the hybrid model varies across jurisdictions, depending on the national legal and institutional frameworks. In addition to automated cross-checks, verification may also be triggered by public reports (e.g., whistleblower submissions, media coverage), investigative findings (e.g., related to public procurement), or random selection. The random selection process may follow predefined criteria, as in the case of Moldova, or be entirely casual, as observed in Georgia.

A fully electronic risk analysis system has so far been implemented only in Ukraine and Latvia. Ukraine has developed a risk-scoring algorithm that assigns a calculated risk rating to each declaration, whereas Latvia's system (ESD) performs automated checks by applying predefined rules and matching declarations with other registers. In contrast, a fully manual approach remains in use in Serbia and Germany: Serbian legislation specifies categories of politically exposed persons (PEPs) subject to annual verification, while in Germany, all declarations submitted by members of the Bundestag are subject to verification.

2.2.2 Risk indicators or "red flags"

Risk indicators, also referred to as "red flags," are tools designed to identify exposure to potential risks or early signs of irregularities within asset and interest declarations (AIDs) (Kotlyar & Pop, 2021). The risk assessment process typically highlights possible violations, such as the submission of false or incomplete information; illicit enrichment (i.e., unjustified variations in personal wealth); conflicts of interest; incompatibility between public office and other professional activities or positions; acceptance of prohibited gifts or sponsorships; the holding of unauthorized financial interests; and breaches of anti-corruption regulations, such as post-employment restrictions.

The majority of the States interviewed report employing risk indicators as part of their risk analysis frameworks. However, only two countries—Ukraine and Latvia—have adopted a formalized and continuously updated list of red flags. Given the evolving nature of public officials' conduct and the rapid

development of digital technologies, it is essential for red flag systems to be periodically revised in order to remain effective and relevant (Hoppe & Kalniņš, 2020).

Of particular note is Ukraine's advanced risk assessment mechanism, which incorporates a weighted scoring model: each red flag is assigned a specific weight, and an algebraic formula is applied to compute a composite risk score for each declaration. A verification procedure is initiated only when the calculated risk exceeds a predetermined threshold.

The scope and sophistication of risk indicators employed by Ukraine and Latvia appear broader than those observed in other countries. In the previous survey, States that reported using risk indicators generally referred to a more limited and standardized set of red flags. The most frequently cited indicators included: data inconsistencies or discrepancies; missing or incomplete data; delayed submission; discrepancies between declared behaviour and the content of the declaration; and the holding of high-risk positions or functions.

2.2.3 Consequences

A comparative analysis of AID regimes across interview respondents unveils distinct, yet often convergent models regarding competent authorities for verification and the crucial dynamics of inter-agency exchange of relevant information.

The competence for verifying asset declarations is predominantly attributed to centralized bodies with anti-corruption or integrity mandates. In numerous contexts, the Anticorruption agency itself holds primary competence for verification. As pointed out before, this happens in Georgia, Montenegro, Romania, Serbia and Ukraine[16]. On the other hand, other approaches involving shared or decentralized competence also exist. In Latvia, oversight is divided between the Corruption Prevention Bureau (KNAB) – which focuses on identifying conflicts of interest and compliance – and the State Revenue Service (SRS) – which screens officials' assets for income legality and tax compliance. In Italy, initial verification is the responsibility of each individual administration; nonetheless, the National Anti-Corruption Authority (ANAC) can intervene if an administration fails to meet publication or verification obligations for "at-risk" declarations. Germany employs a distinct model, where a specific Division within the Bundestag conducts the verification process for "at-risk" declarations, initiating formal procedures for clarification and potentially imposing sanctions in cases of severe breaches.

Effective management of "at-risk" declarations seems to require a well-coordinated network of communication and collaboration among various governmental agencies. Usually when initial verifications reveal potential criminal offences, anti-corruption agencies tend to forward the relevant materials to competent law enforcement bodies for further investigation[17].

[16] For instance, Georgia's Anti-Corruption Bureau (ACB) is the sole institution responsible for collecting and monitoring declarations, employing a commission to select which officials' declarations will be verified each year. Similarly, Montenegro's Agency for the Prevention of Corruption handles verification duties. Romania's National Integrity Agency (ANI) conducts verification through cross-checks with public registers, including direct access to some databases and requesting access to others like bank records. In Serbia and Ukraine, specialized anti-corruption agencies—the Agency for Prevention of Corruption and the National Agency on Corruption Prevention (NACP), respectively—serve as the competent authorities, often with internal structures dedicated to in-depth analysis and verification. Bulgaria has a structure where the Public Registry Directorate within the Anti-Corruption Commission is specifically tasked with verifying declarations submitted by high-level officials.

[17] For example, if intentional violations with essential elements of an offense are identified, the Anti-Corruption Bureau in Georgia forwards the declaration and relevant materials to the competent law enforcement body for further investigation, with criminal violations subsequently transferred to prosecuting authorities. Similarly, in Italy, if a false declaration is discovered during verification, the responsible administration is obliged to report the matter to the Judicial Authority, aligning with public officials' general duty to report crimes. In Latvia, instances of false information regarding large amounts of illegal income detected by the State Revenue Service are forwarded to the Finance Police for criminal investigation. Moldova's integrity inspector notifies law

Beyond referrals for criminal offenses, inter-agency communication extends to financial and fiscal information exchange. In Italy, individual administrations are required to provide information to the Financial Intelligence Unit (UIF) in cases of inconsistencies in declarations, in line with Bank of Italy guidelines. In Moldova, if inspectors gather additional material beyond what is necessary for their findings, these documents are sent to the tax service, although thresholds for discrepancies may limit the tax service's interest in smaller amounts. In Romania, an "integrity warning" is issued to both the National Integrity Agency (ANI) and the contracting authority when potential conflicts of interest are detected, and the National Agency for Public Procurement then verifies the implementation of corrective measures. Moreover, internal agency communication is also prevalent, as seen in Serbia, where follow-up information regarding procedures initiated due to "red flags" is shared within the Agency for Prevention of Corruption.

Overall, there appears to be a strong emphasis on robust cooperation between integrity and anti-corruption agencies and investigative, fiscal, and financial authorities, ensuring that the outcomes of asset declaration verifications can translate into appropriate legal action and foster a broader financial intelligence picture.

2.2.4 Digitalisation

The pathway toward digitalization in risk analysis methodologies across various countries has generated significant advancements, yet persistent challenges remain. Countries like Ukraine have made notable progress and digital transformation has enhanced transparency and efficiency in public administration.

However, these improvements are not without challenges. In Germany, while the e-filing system aims to improve efficiency, the “plausibility check” and verification process remain manual, with ongoing legal and technical challenges. Montenegro's system, recently introduced in 2024, still faces technical challenges, such as outdated or incomplete data and difficulties in integrating the new system with the previous ones. Ukraine faces significant legal and technical challenges, particularly in cross-referencing data between submitted declarations and external registers, leading to misalignments due to differing data recording methodologies. Organizational and legal obstacles also slacken progress. In Italy, the primary challenges are organizational, with risk analysis responsibilities delegated to individual administrations, making a unified global risk analysis difficult. In Moldova, the biggest challenge was securing parliamentary approval for the draft law implementing digitalization, rather than financial or technical obstacles. In Romania, the implementation of the electronic submission system was challenging due to the requirement for a certified electronic signature, which not all public officials possessed, prolonging the transition for two to three years.

In conclusion, even though digitalization has undeniably enhanced efficiency, transparency, and data management in many national contexts, its full realization is often slowed down by technical integration issues, fragmented organizational structures, slow and complicated legislative procedures, and challenges related to user adaptation.

enforcement authorities and/or the state tax service upon reasonable suspicion of a criminal offense or tax legislation violation, with these authorities then required to inform the inspector of their decision. Ukraine demonstrates a structured collaboration where the National Agency on Corruption Prevention (NACP), during full verification, cooperates with other state authorities such as the National Anti-Corruption Bureau, the National Police, the State Bureau of Investigation, and prosecution authorities for further investigation, sending a motivated conclusion and documentation to pre-trial prosecution authorities if discrepancies are detected.

3. Best practices for implementing a standardised EU risk analysis framework and roadmap for automated and digital AID systems

The results of the in-depth interviews conducted, combined with extensive desk research, provide useful indications to develop guidelines and general principles for a standardised EU risk analysis framework and roadmap for implementing automated and digital systems. A detailed analysis of the national experiences reveals a heterogeneous landscape and several differences among national systems. In each country, the risk analysis mechanism implemented is currently highly specific and adapted to its unique context. Consequently, a uniform and rigid model applicable across all EU Member and Candidate States does not seem to be the best solution or fit well with the described situation. Nevertheless, despite such inherent diversity, a standardised risk analysis framework can indeed be developed: it should strive to achieve an adequate level of harmonisation through a set of general principles and guidelines that should allow each country to tailor their risk analysis mechanisms to their country-specific features, needs and operational environments.

The following suggestions and general principles are thus to be interpreted within this framework, and thus not as a rigid set of rules to be uniformly applied across EU Member and Candidate States alike.

Standardised EU risk analysis framework

A robust risk analysis mechanism should adhere to and incorporate the following general principles.

- **Risk-based approach.** AID systems must be inherently risk-based, prioritizing proactive and substantive control of declarations, particularly those submitted by persons with top executive functions (PTEFs). This involves real-time identification of potential red flags, thus moving beyond purely formalistic or reactive checks, which should be followed by in-depth verification.
- **Public database interoperability**. An effective risk analysis mechanism requires the integration of multiple databases. This enables the identification of specific risk indicators, such as individuals holding multiple roles, significant changes in assets or income, or discrepancies in property ownership, shares, loans, or other financial factors. The detection of red flags can trigger in-depth reviews. International cooperation is also essential to ensure interoperability across national borders for tax, property, company, and employment records.
- **Efficient system architecture**. In order to tailor a methodology that can guarantee flexibility and prompt adaptation to specific national needs, national risk analysis systems design should either facilitate collaboration and comparison among different administrations through centralized access to information or, conversely, simplify processes by assigning clear responsibility and accountability to individual administrations, potentially distributing control for enhanced effectiveness.
- **Strong internal oversight and resources.** Adequate human and financial resources, along with strong internal oversight mechanisms, are crucial for fairness and consistency, especially within key bodies like National Anticorruption or Integrity Agencies.
- **Continuous learning and international cooperation.** The development and strengthening of national risk criteria and overall systems benefit significantly from seeking guidance and sharing best practices with international partners, particularly countries with well-developed anti-

corruption systems like Ukraine. International benchmarking and studying advanced models are strongly recommended.

- **Transparency.** An advanced AID system should be transparent enough to allow citizens to scrutinize public officials' declarations, fostering accountability and public trust. Greater public access to aggregated control statistics is also advocated.
- **Digitally supported mechanisms.** Digitalisation is a cornerstone of modern AID systems. This includes leveraging electronic submission and checking of declarations, implementing IT tools for verification and reporting, and developing machine-readable data for continuous system training. However, automation supports but does not replace human analysis. That is why a mixed-method risk analysis model, combining IT tools and manual intervention, could ensure accuracy and comprehensive coverage while overcoming the limitations of each method.

Roadmap for implementing automated and digital AID systems

Digitalisation is strongly supported as a fundamental pillar of modern AID systems, significantly enhancing efficiency and better investment of limited human resources. The implementation of an automated risk analysis system draws on insights from various national experiences, offering crucial benefits regarding cost-effectiveness and reduced manual labour.

Key automated functionalities and implementation strategies include:

- **Electronic submission and verification**. Systems should enable the electronic submission—preferably through pre-compiled forms—and automated checking of all declaration items. E-filing declarations streamlines the process of submission, ensuring higher levels of compliance, allows better data management, swifter and more effective reviews, and facilitates publication.
- **IT tools for verification and reporting**. Leveraging IT tools for in-depth verification and systematic reporting is an essential component of a digital risk analysis system.
- **Machine-readable data.** Data should be machine-readable to facilitate continuous system training and analysis.
- **Automated data checking and prioritization.** Automated tools are vital for checking all declaration items, automatically grouping and prioritizing declarations that present higher risk or multiple "red flags".
- **Red-Flags and cross-checks.** Automated red-flag detection algorithms and cross-checks with other government registers are crucial. Algorithms, along with data-matching with public registers and prioritization mechanisms, greatly improve the efficiency of verifications, leading to a higher rate of identifying irregularities.
- **Interoperable systems and integration with external data.** Implementing electronic submission platforms and interoperable systems allows for better integration of financial, property, and employment databases, which is essential for identifying high-risk declarations. International cooperation can further facilitate this by enabling AID systems to communicate effectively with records not only nationally but also across borders, particularly in an increasingly globalized context. Integration with external data—both governmental and non-governmental—allows to draw a clearer and more exhaustive picture; however, it should be implemented gradually, to allow familiarisation with the different databases and their resources.

The experience of Ukraine provides a compelling example of the benefits of such digitalization, demonstrating significant improvements in cost-effectiveness and reductions in manual labour. Ukraine's advanced models illustrate how technology and intelligent system design can transform risk analysis mechanisms into powerful tools for corruption prevention and institutional integrity.

4. Annex A

Interview on risk analysis in AID systems in EU Member and Candidate States

Co-funded by the European Union

Project qAID – Interview on risk analysis in AID systems in EU Member and Candidate States – Interview protocol

Introduction

Dear respondent,

We thank you for accepting to carry out this interview. Your support is crucial and we thank you for your previous support in filling out the questionnaire.

As you know, this interview is made in the framework of the **European project "qAID** - Towards contemporary knowledge and innovative tools for assessing and enhancing effectiveness of Asset and Interest Disclosure (AID) systems in EU Member States and Candidate States", co-financed by the **European Commission**, Directorate-General for Migration and Home Affairs – Internal Security Fund (2021-2027). The project is coordinated by the **Centre for Security and Crime Sciences**, Joint Research Centre of the University of Trento and the University of Verona, and carried out in partnership with the **Romanian National Agency for Integrity** (Agenția Națională de Integritate), the **Regional Anti-Corruption Initiative** (RAI) **Secretariat**, the **Italian Anticorruption Authority** (Autorità Italiana Anticorruzione), and the **Centre for the Study of Democracy** (Bulgaria). The general objective of the qAID project is to address the national asset and interest disclosure (AID) systems in EU Member and Candidate States in order to make them more effective and efficient.

The **aim of the interview is to collect further information about the risk-analysis mechanism in your country**. More in detail on:

- the method to conduct the risk analysis of submitted asset and interest declarations;
- the indicators/red flags used to qualify declarations as "at risk", and the further steps taken when this happens;
- the role of digitalisation in the implementation of risk analysis mechanisms at national level;
- the identification of relevant best practices.

The analysis of the data collected will allow not only to identify the most effective risk analysis models, but also to develop a standardised EU risk analysis framework and a roadmap for implementing automated and digital risk analysis of AID declarations in Member and Candidate States.

Before proceeding further, we would like to clarify that:

1. the interviewer will not collect any personal information (e.g. name, surname, email address, etc.);
2. respondents will not be identified or identifiable in any way in the publication of the results;
3. results will be published anonymously;
4. the interview is expected to last no longer than 30/45 minutes.

Do you agree to record the interview? The recording will be used exclusively for research purposes (i.e. to refine the notes we are taking during the interview), not be shared with anyone, and deleted immediately after the completion of the task.

Background information

Q1 - When was the AID system first developed/implemented in your country?

Q2 - Has it ever since been updated? If yes, how often and why?

1 - Risk analysis method

Q3 - What method is used for the risk analysis in your country? [See also survey]

Q4 - What does manual/mixed/automatic mean?

Q5 - Can you describe the process step by step?

Q6 - Is every declaration submitted assessed/checked?

Q7 - Have any issues or difficulties been encountered in the implementation of the risk analysis mechanism? If yes, how have they been solved?

2 - Indicators/Red flags

Q8 - What indicators/red flags are used to qualify a declaration as "at risk" in your country? *[See also survey]*

Q9 - How are the indicators/red flags identified?

Q10 - How is the risk level determined (i.e. how are indicators/red flags combined)?

Q11 - Are indicators/red flags periodically updated?

3 - Consequences

Q12 - What happens if a declaration is qualified as "at risk"?

Note: this is a very broad question, main items to be considered are the following:
- *Is there a "risk threshold" triggering verification or are all "at-risk declarations" verified?*
- *Which is the competent authority (for the verification)?*

Q13 – Is follow-up information collected regarding procedures activated after the identification of a red flag?

4 - Digitalisation

Q14 - Does/could digitalisation support/improve the risk analysis in this field in your country?

Q15 - Are there any difficulties or limitations (e.g. legal, technical, etc.) to the implementation of digital risk analysis mechanisms?

5 - Best practices

Q16 - On the basis of your experience, how should an ideal risk analysis mechanism work/be structured?

5. Bibliography

COUNCIL OF EUROPE, GRECO, *Group of States against Corruption. The Council of Europe's anti-corruption body* Strasbourg.

COUNCIL OF EUROPE, *How does GRECO work?*, information available at https://www.coe.int/en/web/greco/about-greco/how-does-greco-work, last accessed on 8/05/2025.

COUNCIL OF EUROPE, *On the twenty guiding principles for the fight against corruption*, Resolution (97)24.

EUROPEAN COMMISSION. (2023). 2023 Rule of Law Report. The rule of law situation in Europe, COM(2023) 800 final, Brussels.

EUROPEAN COMMISSION. (2024). The 2024 EU Justice Scoreboard: Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, COM(2024) 950, Luxembourg.

EUROPEAN PARLIAMENT RESEARCH SERVICE (2023). A comparative analysis of financial disclosure obligations on members of parliament, Brussels.

GRECO (2023). *Bulgaria Evaluation Report. Fifth Evaluation Round.*, Strasbourg.

GRECO (2024). *Germany Evaluation Report. Fifth Evaluation Round*, Strasbourg.

HOPPE, T., KALNIŅŠ, V. (2020). *Red flags for prioritizing asset declarations*. Regional Project "*Strengthening measures to prevent and combat economic crime*". European Union and Council of Europe.

JENKINS, M. (2015). *Income and Asset Disclosure: Topic Guide*. Transparency International. https://knowledgehub.transparency.org/assets/uploads/kproducts/Topic_Guide_Income_and_Asset_Disclosure.pdf

KOTLYAR, D., POP, L. (2021). *Automated Risk Analysis of Asset and Interest Declarations of Public Of cials* (StAR Initiative).

KOTLYAR D., POP L. (2020). "Case Study 18: Reform of Asset and Interest Disclosure in Ukraine", in World Bank, *Enhancing Government Effectiveness and Transparency – The fight against corruption* (Chapter 8), World Bank, Washington, DC.

KOTLYAR, D., POP, L., ROSSI, I. (2023). *Asset and Interest Disclosure: A Technical Guide to an Effective Form*. StAR Initiative. https://star.worldbank.org/publications/asset-and-interest-disclosure-technical-guide-effective-form

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). (2023). *Integrity of asset declarations and conflict of interest disclosure: Towards better frameworks and implementation* (GOV/PGC/INT (2023)12/FINAL). OECD Publishing, Paris.

POP L., STEFAN L., POPA S. (2020). "Case Study 19: Enhancing Effectiveness of Asset Declarations inRomania", in World Bank, *Enhancing Government Effectiveness and Transparency – The fight against corruption* (Chapter 8), World Bank, Washington, DC.

REGIONAL ANTI-CORRUPTION INITIATIVE (RAI) (2024). *Assessment of the legal framework and technical capacities to conduct asset declaration collection, verification, and exchange of data with other jurisdictions in the Southeast Europe – REPORT*.

ROSSI, I., POP, L., BERGER, T. (2017). *Getting the Full Picture on Public Officials: How-To Guide for Effective Financial Disclosure*. StAR Initiative. https://star.worldbank.org/publications/getting-full-picture-public-officials-how-guide-effective-financial-disclosure

STAR INITIATIVE (2012). *Public Office, Private Interests: Accountability through Income and Asset Disclosure*. StAR Initiative. https://star.worldbank.org/publications/public-office-private-interests

UNODC - CORRUPTION AND ECONOMIC CRIME BRANCH. *Thematic compilation of prevention - related information*, information available at the following link: https://www.unodc.org/corruption/en/cosp/WGP/financial-disclosure-declaration-of-assets.html, last accessed on 19/03/2025.

UNODC (2009). *Technical Guide to the United Nations Convention Against Corruption.* https://www.unodc.org/documents/treaties/UNCAC/Publications/TechnicalGuide/09-84395_Ebook.pdf.