



Automated Risk Analysis of Asset and Interest Declarations of Public Officials

A Technical Guide

Dmytro Kotlyar
Laura Pop



Automated Risk Analysis of Asset and Interest Declarations of Public Officials

A Technical Guide

**Dmytro Kotlyar
Laura Pop**

© 2021 International Bank for Reconstruction and
Development / The World Bank
1818 H Street NW, Washington, DC 20433
Telephone: [202-473-1000](tel:202-473-1000)
Internet: star.worldbank.org
Email: starinitiative@worldbank.org
Twitter: [@returningassets](https://twitter.com/returningassets)
Some rights reserved.

StAR—the Stolen Asset Recovery Initiative—is a partnership between the World Bank Group and the United Nations Office on Drugs and Crime (UNODC) that supports international efforts to end safe havens for corrupt funds. StAR works with developing countries and financial centers to prevent the laundering of the proceeds of corruption and to facilitate more systematic and timely return of stolen assets.

This work is a product of the staff of the World Bank and the United Nations Office on Drugs and Crime. The findings, interpretation and conclusions expressed in this work do not necessarily reflect the views of the World Bank, its Board of Executive Directors, or the governments, they represent, the United Nations, or its Member States. The World Bank and the United Nations do not guarantee the accuracy of the data included in this work.

The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of the World Bank or the United Nations concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Nothing herein shall constitute or be considered to be a limitation upon or waiver of the privileges and immunities of The World Bank or the United Nations, all of which are specifically reserved.

Cover photos: whiteMocca/Shutterstock,
Thanumporn Thongkongkaew/Shutterstock.
Further permission required for reuse.

Design by Sole Proprietor Buria O.D.

Acknowledgments

The authors would like to thank Emile van der Does de Willebois (Lead Financial Sector Specialist and Stolen Asset Recovery Initiative Coordinator) who supported this study from the conceptual stage through research and drafting.

The authors benefited from the expert advice and guidance provided during the peer review process, which was chaired by Yira Mascaró (Practice Manager, Financial Stability and Integrity unit, World Bank Group). The peer reviewers were Alexandra Habershon (Senior Governance Specialist, WBG); Shervin Majlessi (Chief, Conference Support Section, UNODC); Ruslan Piontkivsky (Senior Economist, WBG); Silviu Popa (Secretary General, National Integrity Agency, Romania) and Ivana Rossi (Financial Sector Expert, IMF).

The authors are also grateful to Jean Pesme (Global Director, Finance, Competitiveness, and Innovation) for his guidance in the final stages of drafting this guide.

We would like to thank Dmytro Chaplynskyi (Consultant, StAR) for his contribution to the advisory work on automatic verification of asset declarations, which was used for drafting some parts of the technical guide.

About the Authors

Dmytro Kotlyar has been a consultant with the World Bank/Stolen Asset Recovery Initiative (StAR) since 2015. He focuses on asset declarations, conflict of interest, beneficial ownership, criminalization of corruption, e-governance and other related issues. He has more than 13 years of experience working on anticorruption and rule of law issues. He helped design and implement the electronic asset disclosure system in Ukraine and has advised other governments on anticorruption reforms. Dmytro has also worked as a consultant on anticorruption and good governance issues for other organizations and technical assistance projects, including OECD, Council of Europe, UNDP, EU, USAID. He co-authored several StAR and World Bank publications, including: “E-filing Asset Declarations: Benefits and Challenges” (2019) and the chapter on asset and interest declarations in “Enhancing Government Effectiveness and Transparency: The Fight Against Corruption” (2020). Working for the OECD Anticorruption Network for Eastern Europe and Central Asia, Dmytro led peer reviews of anti-corruption systems of several countries in the region. Before working as a consultant, he served as a Deputy Minister of Justice and worked in the civil society sector of Ukraine. He holds a BA and MA in Law from the National University of Kyiv Mohyla Academy in Ukraine.

Laura Pop is a Senior Financial Sector Specialist with the World Bank Group Financial Stability and Integrity and a member of the Stolen Asset Recovery Initiative (StAR) team. Since joining the World Bank in 2009, she has advised more than 20 countries across all regions on multiple areas of asset and interest declaration systems (enhancing the legal framework, using electronic tools, increasing the effectiveness of verification, operationalizing the concept of beneficial ownership in declarations, inter-agency cooperation). She co-authored several StAR and World Bank publications on asset declarations: “Getting the Full Picture on Public Officials: A How to Guide for Effective Financial Disclosure”, “E-filing asset declarations: Benefits and Challenges”, “Using Asset Disclosure for Identifying Politically Exposed Persons” and the chapter on asset and interest declarations in “Enhancing Government Effectiveness and Transparency: The Fight Against Corruption”. She also works on policy and advisory programs in the areas of asset recovery, anti-money laundering, and the strengthening of specialized anti-corruption investigative and prosecutorial bodies. She holds a BA from Princeton University and MA from Harvard University.

Contents

1. Introduction	1
2. The Role of Automated Risk Analysis in the Business Process of the Asset and Interest Disclosure System	4
2.1. Definition	4
2.2. Validation of Data in the Electronic Declaration Form	7
2.3. Automated Check of Submission	8
2.4. Verification Framework	9
2.5. Role of the Automated Risk Analysis	11
2.6. Preconditions and Challenges for Introduction of Risk Analysis	13
2.7. Benefits of Automated Risk Analysis	14
3. Organizing the Process of Automated Risk Analysis	15
4. Development of the Risk Analysis Framework	21
4.1. Preparation Stage	22
4.2. Data Extraction Stage	23
4.3. Data Exploration Stage	23
4.4. Rules Testing Stage	23
4.5. Final Stage and Review	24
5. Why Integration with External Data Sources Is Needed	25
6. Extent to which the Automated Risk Analysis Framework Should Be Open to the Public	27
Appendix. Examples of Risk Indicators (Red Flags)	28
A. Analyzing Data within One Declaration	28
B. Comparing Data with External Databases	30
C. Comparing with Data in the Previous Declarations of the Same Declarant	31
D. Comparing with Declarations of Other Declarants	31

Figures

Figure 2.1. Business Process of an Asset and Interest Disclosure System	6
Figure 2.2. Workflow of Data Validation in the Electronic Declaration Form	8
Figure 2.3. Using Risk Analysis in the Asset and Interest Declaration Verification Process	12
Figure 3.1. Workflow of the Automated Risk Analysis	16
Figure 4.1. Evolution of the Automated Risk Analysis Framework	21

1. Introduction

Asset and interest declarations of public officials¹ are used globally to identify unjustified variations of assets of public officials, prevent conflicts of interests, improve integrity, and promote accountability of public officials. Financial disclosures play an important role in national anti-corruption systems. Moreover, they are part of the global normative framework on anti-corruption through several articles in the United Nations Convention against Corruption (UNCAC).² According to World Bank research, more than 160 countries have introduced a system of asset, interest disclosure, or both for public officials.³

Although most systems are still paper-based, more and more countries are upgrading their financial disclosure systems by introducing electronic filing and digitizing other elements of the system, including parts of the verification process of declarations.⁴ One of those elements is the automated risk assessment of asset and interest declarations (AIDs). Introducing an automated risk analysis is one of the main benefits of digitizing financial disclosure systems.

Verification of declarations is important to ensure deterrence and thus enable the AID system to reach its preventative potential. Introducing automated elements using information technology (IT) solutions in the verification process can significantly improve efficiency. Often, enforcement agencies must analyze a significant number of asset and interest declarations. In some countries, laws set a rigid framework that requires mandatory verification on the basis of formal grounds (for example, late

¹ A mechanism by which a public official must periodically submit information about his or her income, assets, liabilities, expenditures, and interests. Also referred to as financial disclosure, asset disclosure, asset and income declarations, or wealth reporting.

² Article 8.5 of UNCAC calls on its state parties to establish measures and systems requiring public officials to make declarations to appropriate authorities regarding, inter alia, their outside activities, employment, investments, assets, and substantial gifts or benefits from which a conflict of interest may result with respect to their functions as public officials. The Convention (article 52.5) also requires States Parties to consider establishing effective financial disclosure systems for appropriate public officials and to provide for appropriate sanctions for noncompliance, and to consider taking such measures as may be necessary to permit its competent authorities to share that information with the competent authorities in other States Parties when necessary to investigate, claim and recover proceeds of offences established in accordance with this Convention.

³ See an overview and analysis of national systems and global trends in: Ivana M. Rossi, Laura Pop, and Tammar Berger, “Getting the Full Picture on Public Officials: A How-To Guide for Effective Financial Disclosure,” Stolen Asset Recovery (StAR) Series (Washington, DC: World Bank, 2017). doi:10.1596/978-1-4648-0953-8.

⁴ See discussion of the e-filing systems in: Dmytro Kotlyar and Laura Pop, “E-filing Asset Declarations: Benefits and Challenges,” Stolen Asset Recovery (StAR) Series (Washington, DC: World Bank, 2019). <https://openknowledge.worldbank.org/handle/10986/32066>.

submission of the form, external complaint). Automated risk analysis helps to filter declarations and prioritize verification. It increases the capacity of the agency tasked with verifying asset and interest declaration data by focusing the agency's limited resources on the verification of high-risk declarations. Automating the assessment of declarations also removes discretion from the initial stages of the verification process and minimizes manual processes thus making the whole process more impartial and credible. Besides detecting individual declarations with high risks, by exploring the data in the declarations, the risk analysis also provides valuable insights that can then inform policy makers on how to improve disclosure regulations. Although the automated risk analysis is not the only element of the verification that can be automated, it is one of the essential elements.

The majority of countries that have introduced electronic filing do not automate their verification processes. In those cases, declarations are filed electronically, but all verification processes are still manual. Some countries with electronic filing systems are now exploring and testing the introduction of electronic risk analysis of declarations mostly alongside automatic cross-checks with public registries. At least one country (Ukraine) has implemented such a system of automated risk analysis. The Republic of Korea's system does not have electronic risk analysis, but there are automatic cross-checks with public sector and private sector registries and databases coupled with automatic analysis of disclosed data to flag inconsistencies between income values and acquired assets. Several other countries (Armenia, Moldova, and Mongolia) have also implemented less sophisticated data cross-checks with public registries.

Implementing an automated risk analysis is a challenging exercise. Verification agencies may lack in-house IT expertise or the funds to outsource the development or system support. A new IT tool may require an upgrade to the agency's hardware and hosting capacity. Effective automated risk analysis also depends on external factors, like access to external sources of information through automated data exchange. There are also challenges of data quality and availability. Therefore, the development of an automated risk analysis module is a complex process involving various technological, financial, and institutional aspects. It requires interagency cooperation and high-level political commitment.

Risk management can be used in different parts of the AID system (whether paper-based or digitized)—from deciding on who should file the asset and interest declaration to selecting declarations for in-depth verification. Using risk-based approaches strengthens the AID system, makes it more reliable and trustworthy, and reduces the possibility of arbitrary application and abuse.

This technical guide focuses on the concept of automated risk analysis of asset and interest declarations, explains how it fits in the general framework of verification of assets and interests of public officials, and proposes options and recommendations for developing and using such an automated analysis as well as technical solutions that can make it effective.

Asset and interest declaration in this guide means an electronic form of declaration submitted by public officials to disclose assets, income, liabilities, expenditures, and/or interests of the officials and their family members. Automated risk analysis means an analysis and assessment of data in the submitted declaration form conducted by software using a predetermined set of rules (risk indicators). The goal of the automated risk analysis is not to establish that a violation occurred but to raise “red flags” that the government agency could then review through the verification process.

The technical guide distinguishes the automated risk analysis from the general verification of the AID, which is a comprehensive legal procedure carried out by the staff of the verification agency. The automated risk analysis could be a part of the general verification framework.

This technical guide builds on the advisory work conducted by the Stolen Asset Recovery Initiative (StAR) team in different countries that use or contemplate using the automated risk analysis of AIDs and consultations with practitioners from other asset declaration systems that use some automation in their verification processes. The proposals and recommendations are not a reflection of one system’s approach to electronic risk analysis but rather include elements from different systems and build on them. The guide goes beyond describing existing approaches and proposes possible solutions that can solve some of the implementation challenges faced by countries. The authors adopted this approach given the limited number of countries that use automatic risk analysis in their verification process at the moment and to allow for sharing the lessons learned from the ongoing work advising countries.

The intended audience of this guide is management and staff of the anti-corruption or other agency responsible for the AID system, including anti-corruption and IT specialists working on the development and implementation of electronic risk analysis of asset and interest declarations. The guide may help leadership of anti-corruption agencies and lawmakers to endorse and promote the innovative approaches in the verification of asset and interest declarations. Practitioners in law enforcement agencies can also use this guide when developing their analytical tools to detect and investigate cases of unjustified assets and false declarations. Civil society may use parts of the guide in reviewing asset and interest declaration data if made available to them. Civil society may also use the guide to advocate new approaches in the verification of declarations conducted by the verification agency.

2. The Role of Automated Risk Analysis in the Business Process of the Asset and Interest Disclosure System

2.1. Definition

The electronic system of asset and interest disclosure can include different elements: registration of the declarant in the system, submission of the electronic asset and interest declaration form, validation of the electronic form, control of submission, automated risk analysis, recording actions taken to process AIDs, management of verification cases by the verification agency officers, publication of declaration data online for public use, and data exchange with external databases and entities.

Verification of declarations is one of the key processes of the AID system. It reinforces the preventive role of the AID system and aims to uncover cases of noncompliance with the asset and interest disclosure requirements. The automated risk analysis can trigger the verification process or have other roles in facilitating an effective verification. It is one of the parts of the verification process that can be automated and made more efficient by using algorithms.

The risk analysis aims to establish the level of likelihood that a person committed a violation. The risk, therefore, means the possibility that a person committed a violation. Violations include false data in the AID, illicit enrichment (unjustified variation of wealth), conflicts of interest, incompatibility of public office with other positions or activities, prohibited gifts or sponsorships, prohibited financial interests, and violation of other anti-corruption restrictions (for example, postemployment restrictions). The risk indicators or “red flags” show exposure to risks or signs of the risk.

The automated risk analysis is an automated algorithm to check data in the submitted forms according to preset logical rules that produce results by comparing certain data values (that is, the system checks whether a declaration returns a positive or negative result for each predetermined rule). The verification agency can determine such rules based on the risk indicators (red flags). The rules assign each risk indicator a weight to take account of its risk level. The risk level (and, accordingly, the risk weight) reflects the probability of the risk indicator occurring in the context of illicit enrichment, false information in the AID, conflicts of interest or unjustified variations of wealth, and other corruption or related offenses (such as violation of rules on incompatibility, gifts, postemployment restrictions). The indicator’s weight shows the relative importance of the indicator.

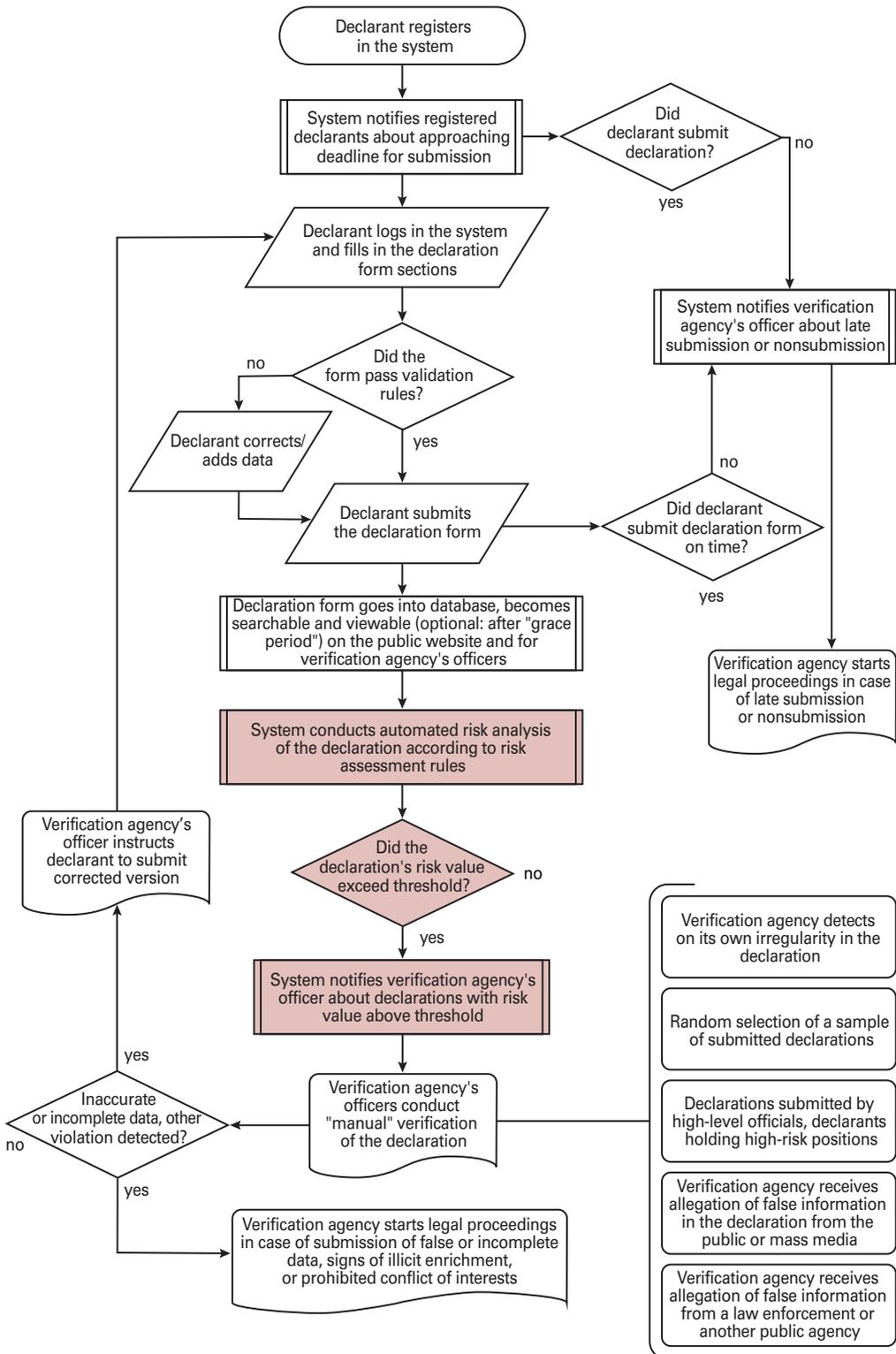
Though this guide focuses on automated risk analysis of data in submitted declaration forms, the risk-based approach can be used for other purposes in the asset and interest declaration system (whether it is paper-based or digitized). For example, it can be used when designing the system to decide on the categories of public officials who should file the disclosures, to determine the content of the declaration form (what data it should capture to be useful), or to prioritize verification of the submitted declarations.

The risk analysis described in this guide has its limitations. First, the risk analysis does not detect or confirm violations, it only highlights cases that may require follow-up. The reverse is true as well—if the risk analysis does not highlight any risks or determines them to be low, that does not mean that there are no violations and that manual verification would not identify them. That is why the risk analysis should never fully replace other triggers of the verification (such as media and civil society reports) or replace the verification of declarations as such.

Second, because of data limitations, most risk analysis rules will target situations of possible misrepresentation of information in the declaration or cases of unjustified wealth. Risk indicators aimed at detecting potential conflicts of interest would be harder to develop and use, although not impossible (for example, by comparing data in the declaration about business interests of the declarant and family members with any public procurement database).

Figure 2.1 shows an example of the business cycle of an asset and interest disclosure system and the place the automated risk analysis can have in it.

FIGURE 2.1 Business Process of an Asset and Interest Disclosure System



2.2. Validation of Data in the Electronic Declaration Form

Automated risk analysis of AIDs should be distinguished from the validation built into the electronic declaration form. Both tools use automated software and are based on algorithms and rules (that is, they compare data values against certain benchmarks and perform an action based on a “yes/no” result). However, they have different purposes and content. Validation aims to check whether fields of the form contain a correct value in terms of format, logical connection between different fields, and that the mandatory fields are not empty. Automated risk analysis compares data filled in by the declarant to detect risk indicators that may show irregularities. Automated risk analysis happens later, after the form was validated and submitted in the system.

The electronic AID system validates data while the declarant fills in the form and when the form is submitted in the system. The system conducts this validation based on the validation rules, which the verification agency can develop and implement through the system’s software.

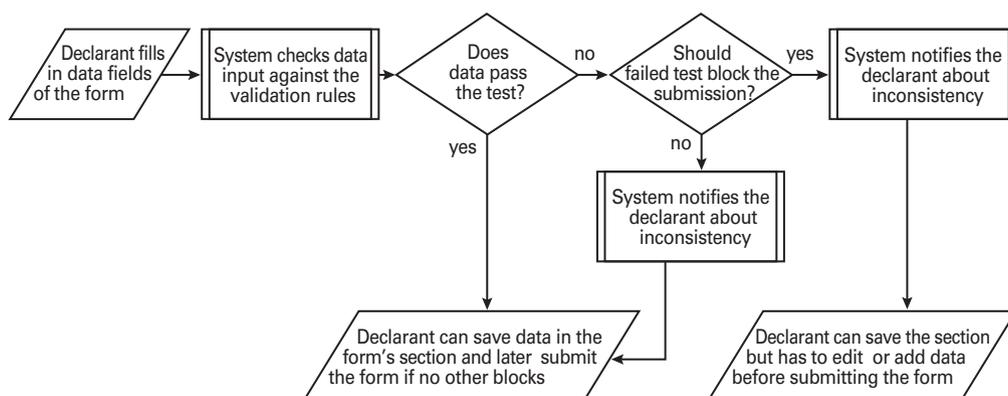
The validation rules can cover the following:

1. Requirements for each field’s format (digits or letters; ID number, amounts, area values, cadastral numbers). If the field is not valid because of wrong value entry, the declarant would receive an error message with the explanation of why the validation failed and an example of the correct value.
2. Correct range or dates (for example, the declarant should not be able to enter a future date of birth or a declaration period covering a future period or a period already covered by an earlier submitted declaration).
3. Requirements on what fields may remain empty or should be filled in for the system to accept the submission.
4. Standard values that may be entered in each field if the declarant does not know information that must be entered or the field is not applicable to the declarant’s situation (such as “Not applicable,” “Unknown”).
5. Logical links between different fields in the form (for example, if a real estate item was mentioned as a place of residence of the declarant, it has to be reflected in the form’s section on real estate assets).
6. Checks whether an asset declaration form for the same type of declaration and covering the same period has already been submitted.

The system should prevent the submission of the form if mandatory fields remain empty or if logical inconsistencies exist. The validation rules may also provide for cases when the field failed to pass the test, but the system can accept the submission if the declarant confirmed acceptance after a warning.

Figure 2.2. shows the workflow of data validation in the electronic AID form.

FIGURE 2.2 Workflow of Data Validation in the Electronic Declaration Form



2.3. Automated Check of Submission

The automated risk analysis is also different from another tool of the electronic AID system, namely the automated check of compliance with the obligation to submit asset and interest declarations by the declarants registered in the system. This automated control may not cover all cases when the declarants must file declarations (for example, declaration of declarants who apply for public office or declaration before leaving public office). The automated check could cover at least the following cases:

1. The declarant is registered in the system and should submit the annual declaration before the deadline established in the legislation. The system should check whether the declarant submitted the annual declaration and whether it was submitted on time.
2. If there is a register of declarants or public officials (such as civil servants) and information on the new declarant appears in the register, the system should check whether this new declarant submitted the entrance declaration.
3. The declarant submitted end-of-office declaration before leaving public office and should submit the postemployment declaration one or two years after leaving public office. The system should check whether the declarant submitted such postemployment declaration and whether it was submitted on time.
4. If the declaration is not submitted or if the verification agency has established that the submitted asset declaration form is inaccurate or incomplete, the declarant should submit the declaration form or corrected declaration form within the period established in the law or by the date decided by the verification agency. The system should check whether the declarant submitted such declaration form (corrected declaration form) and whether it was submitted on time.

The functionalities of the automated control of submission depend on the overall asset and interest disclosure framework, such as whether the law requires submission of a postemployment form or whether there is a unified roster of declarants against which the system can check the submission.

2.4. Verification Framework

The automated risk analysis is part of the verification process. We assume that a central verification agency (such as an anti-corruption agency) conducts the verification of submitted electronic asset and interest declarations.⁵ The verification of AIDs is an administrative procedure that can lead to a criminal investigation, administrative sanction, or disciplinary action.

The legislation should clearly define the scope of the verification, including the following:

- Checking the accuracy and completeness of the information provided in the AID form.
- Detecting signs of unjustified/unexplained wealth (illicit enrichment).
- Detecting conflicts of interests, incompatibilities, prohibited gifts, and other violations of the anti-corruption requirements.

The verification framework includes aspects such as: what triggers verification, which declarations should undergo verification, if there is any prioritization in terms of verification, what verification methods may be used, what sources of information are available to the verification agency, when and how the verification agency should obtain an explanation from the declarant, how the process should conclude, who decides on the outcome of the verification, and what follow-up action the verification agency should take.

In general, because verification procedures are conducted by authorized personnel of the verification agency, this verification is sometimes called manual or human verification to differentiate it from the automated process. However, some elements of verification can be automated. This guide focuses on the automated risk analysis, which is one component of the verification processes that can be automated. In legal terms, the automated risk analysis can be a part of the verification procedure or it can be a process outside of the formal verification. The verification process may differ depending on the country context and this may affect the role and scope of the automated processes used in the verification.

The legislation can establish, in particular, the following triggers for the manual verification (all of them or a combination of individual triggers):

- Results of the automated risk analysis.
- Notification of an allegation, which the verification agency receives from the public or another public authority.

⁵ In this guide, the term “verification agency” means an agency that carries out the verification of asset and interest declarations as its only task or along with other anti-corruption tasks or other tasks not related to anti-corruption (for example, supreme audit institutions or tax authorities that deal with AIDs of public officials along with other core tasks).

- *Ex officio* detection by the verification agency on the basis of media and internet monitoring, or other proceedings (such as criminal investigations).
- Random selection of a sample of AIDs for mandatory verification.
- Mandatory verification of AIDs of certain declarants (such as high-level officials, officials holding positions with a high risk for corruption, declarants who did not submit the AID or failed to submit on time).

In the case of the above triggers, the verification case will be assigned to the authorized officer by the supervisor (such as the head of the unit), or randomly. In the latter case, it is advisable to use an automated random distribution tool that can be part of the electronic AID system. The authorized officer will collect the information to conduct the manual verification of the asset declaration. In case of an external signal of an irregularity (for example, a notification from the public or detection by the agency) the officer can first conduct a preliminary check of the received/detected allegation and then decide whether to launch the manual verification of the asset declaration.

Verification can include the following:

- Receiving information from government-held databases and registers (remotely through direct read-only electronic access or by sending written inquiries).
- Accessing online registers and databases in foreign jurisdictions.
- Obtaining information from public and private entities and individuals, including from abroad, and accessing bank information.
- Conducting or commissioning appraisal of assets.
- Receiving an explanation and supporting documents from the declarant.
- Reviewing the results of the automated risk analysis of the declaration.
- Searching other publicly available information on the internet.

After the manual verification of the asset and interest declaration, the authorized officer may close the case with no additional action taken or by taking or initiating a legal action. The latter can include referring the case to criminal investigators for opening of criminal proceedings (for example, on illicit enrichment or false/incomplete asset disclosure), sending information to the employing public institution to start a disciplinary proceeding, or taking direct administrative action (such as imposing a fine). The verification may also contradict an allegation of violation and establish the accuracy of information submitted in the form. The verification may establish minor irregularities that do not merit taking further legal action. In some systems, the supervisor or head of the agency has to make or endorse the final decision on the conducted verification.

2.5. Role of the Automated Risk Analysis

The automated risk analysis can play different roles in the verification process:

- Results of the automated risk analysis can trigger the manual verification if the risk value of the AID is above a certain threshold or if the system identified certain individual risks (see figure 2.1 for an example of such an arrangement).
- The verification agency can take into account results of the automated risk analysis during the manual verification triggered by the risk analysis or triggered by other reasons (see figure 2.3 for an example of this type of verification framework).

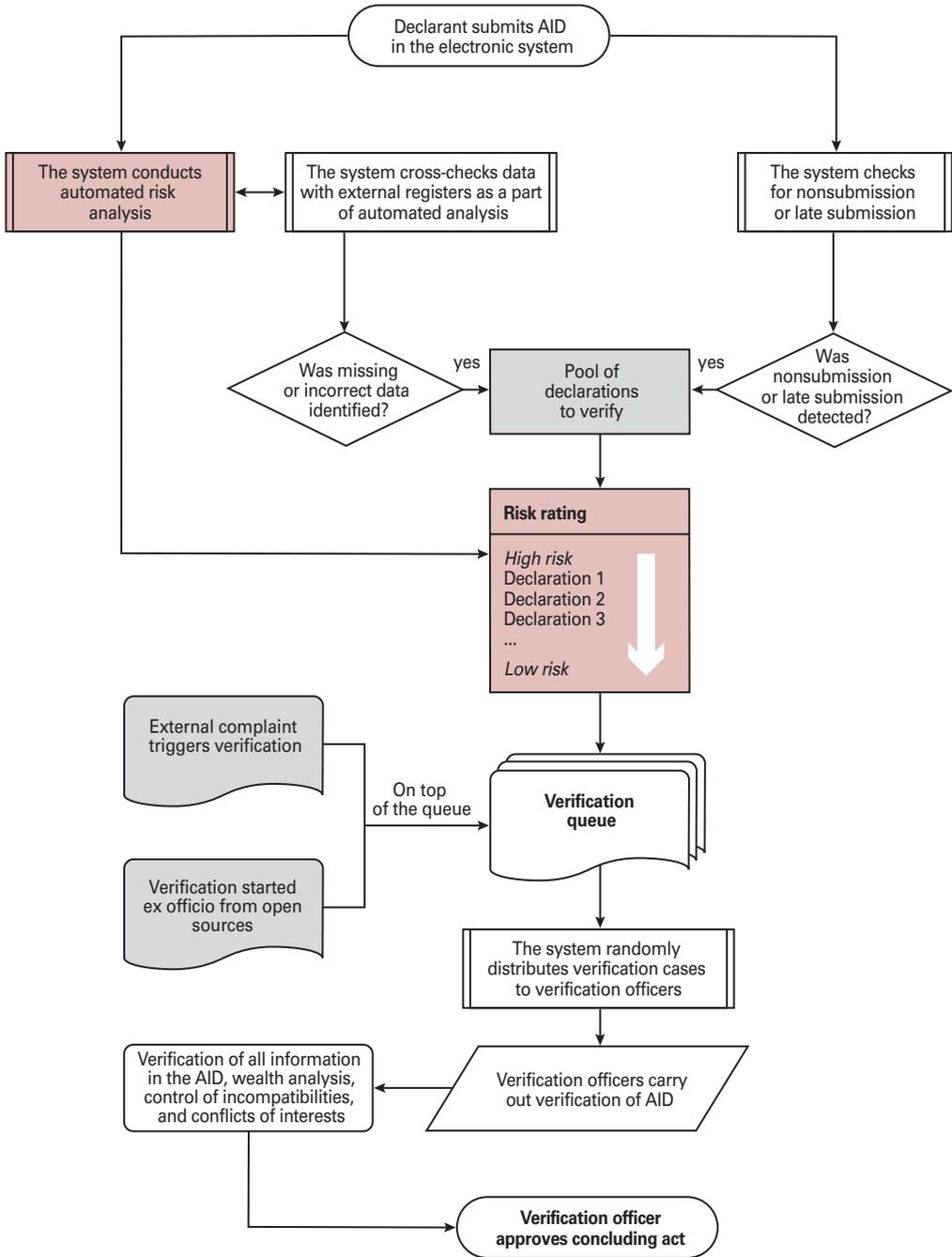
The automated risk analysis limits the number of declarations that undergo the more labor-intensive manual verification and focuses such verification on high-risk declarations. The automated risk analysis is both a prioritization and detection tool. It helps prioritize the verification of numerous declarations. In addition, it can be used to better detect violations following the risk indicators identified by the analysis. The automated risk analysis helps to remove or limit the discretionary decision-making concerning the targets of verification. It also serves to eliminate corruption risks in the verification procedure itself and to increase the effectiveness of the AID verification.

It is important to note that the automated risk analysis is not a process that produces evidence of a false statement in the declaration or other breaches. The analysis only shows the risks that the authorized verification officers should further verify. Even if the automated risk analysis detected discrepancies between two data sets (for example, a discrepancy between data in the declaration and data in an external register), such a discrepancy may not trigger infringement proceedings in all cases. During the course of manual verification, it can be concluded that this is a technical mistake, or the inconsistency can be explained by gaps or inaccuracies in data.

Figure 2.1 shows an approach in which risk analysis is one of the triggers for the verification of declarations. Figure 2.3 shows another approach for using risk analysis in the verification process. In this example, the automated risk analysis is not a trigger for manual verification, but the verification agency can use its results to prioritize the verifications that are mandatory according to the legislation. When the grounds provided in the legislation trigger the verification, the declaration's risk value (rating) determines the order in the verification process – that is, which declaration should be verified first. As shown in figure 2.3, the result of the data comparison with external registers and databases is a separate trigger for the manual verification. Therefore, comparison with external databases is not a part of the automated risk analysis. These examples are not exhaustive – there may be other options of how to use risk analysis in the verification process.

FIGURE 2.3

Using Risk Analysis in the Asset and Interest Declaration Verification Process



2.6. Preconditions and Challenges for Introduction of Risk Analysis

An automated risk analysis requires a number of preconditions involving various technological, financial, and institutional aspects. Beyond ensuring sufficient funding and making sure relevant agencies have the required capacity, developing the module for risk analysis is a collaborative effort that requires involvement of different actors. It means that there should be an institution or a senior manager put in charge of the process and its coordination.

To implement the automated risk analysis, the AID system itself should be digitized and require submission of declarations in a structured form that can be processed. If the system uses earlier declarations submitted on paper, the implementation of the risk analysis project should also include digitizing such information and preparing it for data analysis.

The AID form should capture sufficient information to make the risk analysis possible. The risk analysis can only use the available data and even the most ingenious risk analysis rules will not yield results if the AID form has gaps and misses important information. The system relies on the availability of external sources of structured information against which AID data can be verified. Connecting to such data sources requires legal and technological conditions, which are discussed in more detail in chapters 3 and 5.

The policy makers and managers responsible for the development and implementation of the automated risk analysis should be aware of the challenges they may face in the process. Such challenges, among others, include the following:

- Poor planning and lack of clear mandate to coordinate and implement the project of the risk analysis system development.
- Lack of financial and technical resources to design, implement, and maintain the risk analysis system.
- Insufficient expertise in verifying AIDs or obstacles in transforming such expertise into the risk analysis framework.
- Lack of a clear legal framework that allows using risk analysis in the verification process.
- Lack of the automated access to external data sources.
- Poor quality of external data used for the risk analysis (for example, gaps and mistakes in the data of other government registers).

2.7. Benefits of Automated Risk Analysis

The automated risk analysis of asset and interest declarations helps to upgrade the AID system and introduce innovative IT solutions in the business process of asset and interest disclosure of public officials. The automated risk analysis can streamline the verification process and make it more focused and efficient. The benefits of the automated risk analysis include the following:

- Risk analysis allows for the review of a large number of asset and interest declarations that otherwise may not have been examined at all. Automated software allows bulk analysis of AID data that would not be reviewable on the same scale by human intervention alone. This is especially relevant for countries in which AID systems cover significant numbers of officials (tens or hundreds of thousands). The automated risk analysis allows extending the verification efforts to all declarations and thus strengthens the verification and AID system in general.
- In some countries, the AID law requires mandatory verification of many declarations on the basis of rigid formal grounds, which makes meaningful verification impossible in view of the large number of submitted declarations. The automated risk analysis allows for the filtering of declarations and narrows down the verification to declarations that can be considered a priority because of their high risk. Therefore, it introduces risk management in the AID verification process.
- By prioritizing the verification process, the automated risk analysis can increase the capacity of the verification agency and focus its limited resources on the verification of high-risk declarations.
- Using automated algorithms in the data analysis reduces the possibility for arbitrary judgment. Being an anti-corruption instrument, the AID system should be devoid of corruption and undue influence. The automated risk analysis contributes to this, but it is important to remember that this analysis represents only the first step in the verification process and that the ultimate conclusions are made by the technical staff of asset declaration agencies.
- By removing discretion from the initial stages of the verification process and minimizing manual processes, the automated risk analysis makes the whole process more impartial and credible. It raises the public trust in the verification process and in the agency conducting the verification of AIDs.
- By exploring data in the declarations, the risk analysis provides valuable insights that can then inform policy makers on how to improve disclosure regulations.

3. Organizing the Process of Automated Risk Analysis

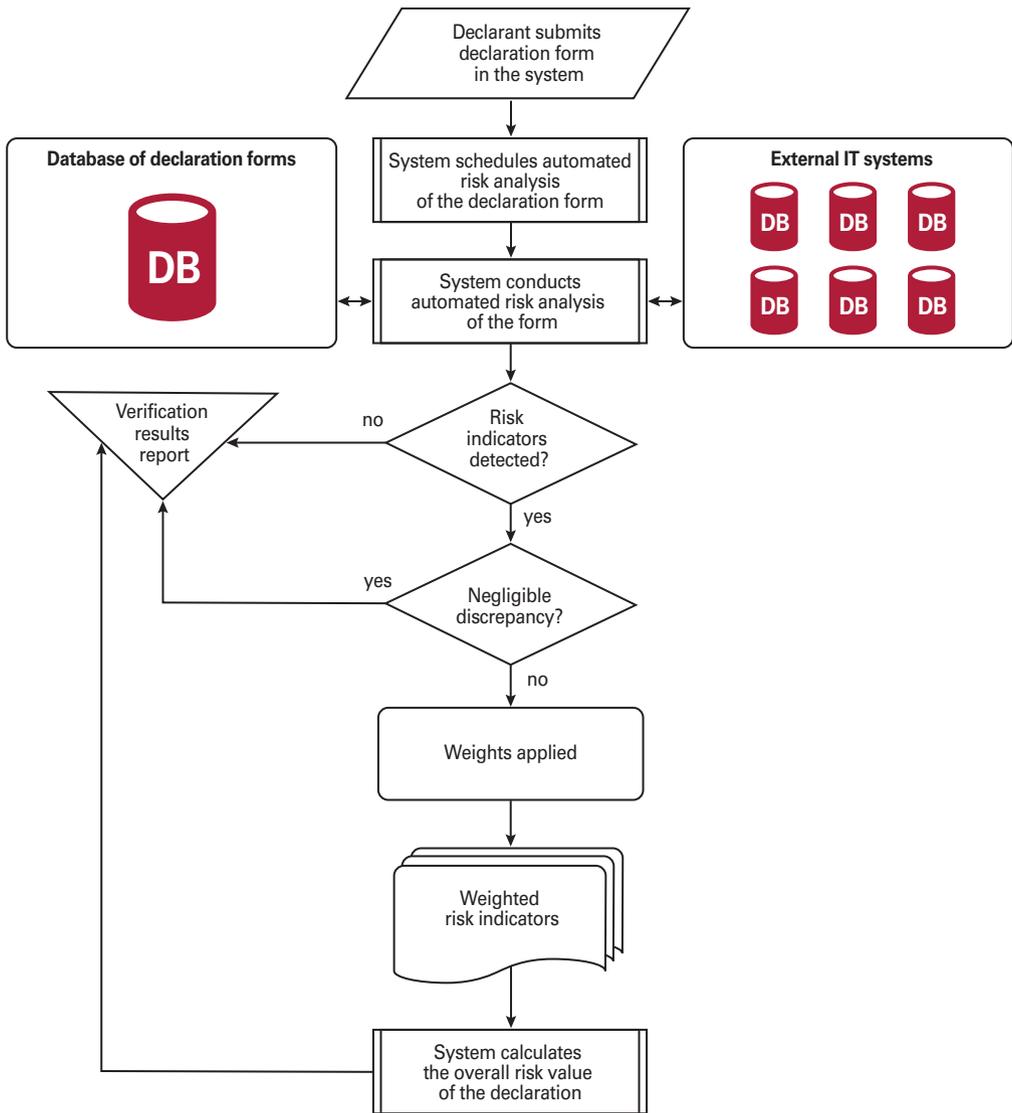
Once the declarant submits the AID form, the system should schedule its automated risk analysis. The system can carry out the analysis once the declarant submits the declaration form in the system; or the system can delay the analysis to accommodate a large number of forms that declarants may submit during the peak submission periods and to allow processing numerous queries to the external databases. The system may distribute the risk analysis tasks evenly to ease the burden on the processing capacity and moderate queries to external systems. For example, the system may conduct automated analysis operations in phases: first, perform an analysis of the data within the declaration form and its comparison with other data in the database of electronic AIDs; second, perform a comparison with data in the external sources, such as external government-held databases and registers.

The automated analysis based on the risk indicators could include the following operations:

- Checking for internal inconsistencies within one AID of the declarant.
- Comparing data from one AID with other declarations that the same declarant previously submitted. Such a comparison looks for inconsistencies, omissions, suspicious changes in assets, etc.
- Comparing the declarant's AID with declarations of similar declarants (a category of declarants) to find unusual discrepancies (outliers). For instance, the system can compare the declaration of a judge with declarations of other judges in the country or in the region.
- Comparing the declarant's AID with declarations of the declarant's family members if they submit declarations as well or with declarations of other persons who are declarants and are mentioned in the AID.
- Comparing data from the submitted AID with external data sources (such as external IT systems like government-held registers and databases, a database of standard or medium prices for certain goods, or a public procurement database).

Figure 3.1 shows the automated risk analysis workflow.

FIGURE 3.1 Workflow of the Automated Risk Analysis



The automated risk analysis framework includes the following elements:

- Risk indicators
- Weights of risk indicators
- Formula for the calculation of the total risk value
- Operations or methods of analysis

The risk indicators can be of the following main types:

- Showing high-risk status or function (for example, the declarant belongs to the category of high-level officials or performs high-risk functions).
- Showing that some data is missing (for example, no real estate owned on any right; the declaration form shows the asset, but minimum details of its description are missing, or the declarant claimed not to know them).
- Showing data inconsistency (for example, discrepancy with the data in the external data source; linked data values do not match in two declarations that were compared—for example, when the value of asset acquisition in one declaration does not match the sale value of the same asset in the next declaration).
- Showing unusual behavior or irregular data value (for example, the declarant received income from a high-risk source, like consultancy, gambling, gifts, etc.; total income of the declarant and family members is lower than a minimum threshold; the declarant has an unusually high number of assets of a certain class, such as real estate, expensive movable property; there is a significant increase in assets compared with the previous declaration; the declarant is a beneficiary of assets in trust; the declarant is a nominal owner of assets controlled by another person).

See the appendix for examples of risk indicators (red flags).

The automated analysis rules may set minimum fault values that the system will take into account. For example, if the system finds a discrepancy in any value or amount that is less than a certain minimum number, it will disregard such discrepancy and not flag it as a risk.

Each risk indicator (“red flag”) can have a certain assigned weight (for example, from 10 to 100), and the system can calculate the overall risk value of each declaration based on the formula

$$R = \sum_{i=1}^N AR_i \times W_i$$

where:

- R is declaration’s risk value;
- N is total number of risk analysis rules used to calculate R;
- i is risk analysis rule;
- AR is answer to the risk analysis rule (“yes” = 1, “no” = 0); and
- W is weight of each risk analysis rule (from 10 to 100).

For example, if 30 risk analysis rules were applied to a declaration, out of which 15 returned a “yes” answer (meaning that the declaration triggered 15 risk indicators), including five indicators with the weight of 25, five indicators with the weight of 50, and five indicators with the weight of 100, the risk rating of the declaration (R) would equal 875.

A risk indicator may also have different weights depending on the result of the rule application. For example:

Rule	Weight
Declaration mentions income in the form of prizes, awards, lottery or gambling wins, etc., in the total amount of more than the equivalent of:	
US\$10,000	50
US\$50,000	75
US\$100,000	100

To introduce a degree of objectivity in assigning weights and to avoid arbitrary decision-making, the developers can use a set of criteria to decide how much weight to give to any specific risk indicator. An example of such a matrix is shown below:

Risk indicator	Criteria	Weight result
Incoming cash flow does not match the outgoing cash flow during the reporting period	Indicator is established through an automated calculation	+
	Discrepancy is significant (above established threshold of X)	+
	Other violations of law are possible (such as not declaring incoming cashflow from a commercial company to avoid disclosure of a possible incompatibility)	+
	Case could lead to a criminal prosecution (for example, illicit enrichment or false statement)	+
	Low occurrence of risk indicator based on previous analysis (that is, review of the previous application of a similar risk indicator to AID data showed that the indicator was triggered in a relatively low number of declarations, for example, not more than 5 percent)	+
	High probability of successful follow-up verification based on previous analysis (that is, review of the previous application of a similar risk indicator to AID data showed that manual verification of declarations in which such risk was detected returned positive results in a large number of cases)	+
		6

The declaration mentions an apartment of more than X square meters	Indicator is established through an automated calculation	+	1
	Discrepancy is significant (above established threshold of X)	-	
	Other violations of law are possible (such as not declaring incoming cashflow from a commercial company to avoid disclosure of a possible incompatibility case)	-	
	Case could lead to a criminal prosecution (for example, illicit enrichment or false statement)	-	
	Low occurrence of risk indicator based on previous analysis (that is, review of the previous application of a similar risk indicator to AID data showed that the indicator was triggered in a relatively low number of declarations, for example, not more than 5 percent)	-	
	High probability of successful follow-up verification based on previous analysis (that is, review of the previous application of a similar risk indicator to AID data showed that manual verification of declarations in which such risk was detected returned positive results in a large number of cases)	-	

After applying the risk analysis rules to the declaration, the electronic system calculates the risk value as a number and assigns it to the declaration. The declaration’s risk value represents a probability score for irregularity that the AID system can detect. The risk value of each declaration should be visible to authorized officers of the verification agency, who should be able to filter declarations by their total risk value and by individual risk indicators identified. The system can also generate a report of the risk analysis that will include the results of the application of each rule to the declaration form and overall risk value of the declaration. The reports can be searchable by the verification agency officers.

All declarations with the risk value above the pre-established threshold can undergo a mandatory manual verification if the law or regulation stipulates it as a trigger for the verification. The verification framework may require that if the declaration’s overall risk value is below the threshold, it would still undergo manual verification but only for the risks identified. For example, if the risk value of the declaration is below the threshold, but by cross-checking with other registers the risk analysis showed that the declarant did not report certain assets (such as real estate), then the verification could look into assets missing in the declaration form without immediately launching a full review of all assets and interests. Should such a limited verification find a willful misrepresentation, then the agency can start a full audit.

The threshold is a value that can be established during the development stage after applying risk rules to the data of declarations and reviewing the distribution of risk

values among the declarations. If the verification framework stipulates that declarations with a risk value above the threshold should undergo mandatory verification, then it should be assured that the threshold is realistic and leaves a feasible number of declarations for the verification agency to process.

Another approach is not to use the risk analysis results as the trigger to verify declarations but rather use the results only if other grounds trigger the verification. In such a case, the verification agency can use the risk rating of the declarations to prioritize the verifications by starting from the declarations with the highest risk value.

Besides the threshold and regardless of the overall risk value assigned to the declaration, the verification agency could still select the declaration for verification if the analysis triggered certain “red flags.” An example of such a red flag could be if the declaration mentions a significant loan (above a certain value) received from a family member or a significant gift. The rules can determine such red flags on the basis of the known typologies of hidden proceeds of corruption or the typologies identified while carrying out verification of declarations or investigating offenses such as illicit enrichment.

As the volume of declarations that undergo manual comprehensive verification grows and new patterns of falsifying data in the declarations or hiding ill-gotten assets emerge, the verification agency should be able to adjust the risk analysis framework. Therefore, such a framework should be sufficiently flexible and continuously reassessed. The risk analysis software should provide a convenient tool to amend its various parameters through a relatively simple process, including by adding analysis methods, such as comparing data from the AID with additional external sources of information.

The verification agency should describe the automated risk analysis process in a legal document, so its results can serve as a basis for further verification and legal action. To avoid system rigidity, it is advisable that the document describing the automated risk analysis framework belong to the verification agency in charge of the electronic AID system and that such an agency could change it without external approval.

4. Development of the Risk Analysis Framework

The risk analysis should be a living system that evolves over time and is upgraded using the experience from its application. The system should provide for such flexibility from the start of its design.

FIGURE 4.1 Evolution of the Automated Risk Analysis Framework



When the automated risk analysis framework is designed after introduction of the electronic AID system, the developers of the framework can use the existing data of declarations. Developers can use any data sets of historical declarations (if digitized) to test assumptions and design a sound risk analysis framework. When setting assumptions, the developers can rely on the previous verification work, examples of previous violations, and other sources (for example, research on the subject).⁶

It is important that the developers of the framework are a mixed group of both IT specialists and asset declarations experts. At different stages, the contribution of one group of experts might be greater than that of the others, but overall, they need to work together. Asset declarations experts (from the verification agency and law enforcement agencies that conducted relevant investigations) will bring their experience of reviewing declarations and detecting and investigating possible violations. They would be the key persons in setting initial assumptions that can then be tested.

Also, it would be useful to collect information and study examples of risk-based detection methodologies used in other areas of public administration, such as in tax, customs and anti-money laundering. The developers could also seek the involvement of practitioners who developed or operated such risk assessment frameworks in these areas.

It is also a good approach to involve experts from other areas, such as risk analysis experts who deal with fraud and money laundering prevention in the financial sector. Analytical products developed by civil society and the media may also be useful in

⁶ See, for example, “Set of Indicators for Corruption Related Cases from the FIUs’ Perspective” (Egmont Group, 2018). <https://egmontgroup.org/en/content/new-publication-set-indicators-corruption-related-cases-fius-perspective>.

developing risk indicators and other elements of the risk analysis framework. Engaging civil society and private sector experts will enrich the process and contribute to its transparency.

Developers should explore available data from declarations to get a better understanding of the data as a whole: ranges of values, mean and median values, outliers, etc. This understanding will help developers to get the big picture on the available data and will help them come up with an initial set of hypotheses for the risk indicators.

Also, the developers can use this approach to recalibrate the risk analysis parameters if the initial framework was launched without access to data sets of declarations.

Development of the risk models, their testing, and their review is resource-intensive work that requires numerous iterations. Sufficient resources should be planned and allocated from the start to enable the development of the risk analysis framework.

The entire process can follow the following structure: the preparation stage, the data extraction stage, the data exploration stage, the rules testing stage, and the final review.

4.1. Preparation Stage

Review the data that the verification agency or the system developers have access to. Review both the data that was submitted electronically as well as the historical data obtained from the digitization of the paper-based forms (if applicable). Developers should assess the data format, the data quality, the coverage of different aspects in paper and electronic forms, and the amount of data.

Developers will have to make certain decisions at this stage: whether to use paper-based declarations, what areas of declarations to use for further analysis, and what kind of aggregated values to calculate.

For example, they will consider:

- Land
 - Total area of land owned by declarant
 - Total area of land owned by family members (if applicable)
 - Total number of land plots
 - Total number of land plots in the capital
 - Total number of land plots bought since the beginning of public service
 - Total number of land plots bought in the past two to five years
- Vehicles
 - Total number of vehicles
 - Number of vehicles bought in the past two to five years

4.2. Data Extraction Stage

Once the developers define the scope, they should update the software to get the required aggregated values out of each declaration. The deliverable of this stage could be a table in which each declaration is represented by a row that comprises meta information (declarant, year, position, office) and aggregated information, defined during the preparation stage. At this stage, the data is also anonymized (stripped of data that identifies a person).

4.3. Data Exploration Stage

Developers should load the tables obtained this way into software for the business analysis. Many tools exist that can help analyze data; some of them are open source and available for free, and some require a subscription.⁷ Such tools will help to analyze and visualize data without the need to change the electronic declaration system software repeatedly just to explore another hypothesis.

Because the data that will be fed in such analytical software is now anonymized, the data security risks are low. However, prior to starting such analysis and choosing a software package, it is recommended to conduct a needs and security assessment and to determine the security parameters in which such analysis would fit. For example, solutions that can be run or hosted locally, in a secured environment, are preferable to cloud-based solutions to prevent possible data leaks.

Even tools as simple as Excel will work to help visualize and run simple queries on the data.

4.4. Rules Testing Stage

The expertise received during manual verification (if already conducted) and the insights gained during the data exploration stage should be converted into the list of hypotheses. For example, “manual” verification in one country often shows that having a land plot abroad is a sign of potential unjustified wealth, so owning a plot of land abroad could become a risk indicator.

Data exploration and visualization should provide not only options for the risk indicators but also reasonable default values for indicator thresholds (the level at which the red flag would be triggered) and weights. For example, the draft indicator assigns a certain degree of risk to declarations of filers who have more than X plots of lands. Visualizing the distribution of the number of plots of land among all declarants or

⁷ Examples of open source software include Kibana, <https://www.elastic.co/products/kibana>; Metabase, <https://www.metabase.com>; Superset, <https://github.com/apache/incubator-superset>; Redash, <https://redash.io>. Examples of free versions of market products include QlikView Personal Edition and PowerBI Desktop. Examples of paid software include Tableau Desktop Personal Edition, PowerBI Pro, and QlikCloud Business.

their sample can help with choosing the X value (reasonable default value), so that a red flag is neither assigned too often nor too rarely.

In another example, a possible risk indicator could be the increase in income over a certain percentage. To establish the appropriate level of threshold (percent of income increase), the data set could be analyzed for the average income fluctuations over a number of years.

By the end of this stage, the developer of the risk analysis framework can have a list of tested and validated risk indicators with thresholds and variables adjusted.

4.5. Final Stage and Review

Applying the full range of risk indicators to all declarations available in the database will produce the list of red flags for each declaration with their weights. The sum of the weights of all indicators applicable to the specific declaration will represent its risk value. The developer can then adjust the weights to see how it affects, for instance, the top 10 or top 30 declarations sorted by risk.

To adjust the risk analysis framework, the verification agency should keep relevant statistics and regularly review results of the conducted risk analysis, for example, after each declaration period. The stages described previously should be occasionally revisited as new insights come up, more data become available, and new typologies to hide assets are identified. Changes in the legislation may also require adjusting the risk analysis framework (for example, changes in the AID form, new violations). Risk analysis is an open-ended task and it can and should be continuously improved.

The review should look at the following:

- How often different rules were triggered when applied to actual declarations (for example, rule X was triggered in Y number of declarations). If the rule was triggered often (for example, in more than 50 percent of declarations) that means that the rule should be changed. Similarly, if the rule was triggered only in a marginal number of cases, it may also have to be adjusted to be more relevant.
- How often the verification of the declarations discovered actual violations after the risk analysis found certain risk indicators in the declaration. If the risk analysis of certain declarations triggered rule X but the follow-up manual verification did not confirm violations regarding any of these declarations (or confirmed them only in a small proportion of these declarations), then the rule may not be effective and should be changed.

Results of such a review should then be used to recalibrate the risk indicators, their weights, and thresholds.

5. Why Integration with External Data Sources Is Needed

An important element of the verification process is cross-checking data from declarations with external sources. As the previous examples show, data cross-checks can technically be a part of the automated risk analysis or they can be separate from the verification.

Given the limitations described below, in most cases, cross-checks with external data sources should not be the only element triggering verification. Results of data cross-checks can show risks that require verification if they are serious. The risk assessment framework should take into account limitations of data cross-checks. The cross-checks with external sources can also be gradually introduced in the risk analysis framework of asset and interest declarations, in which the risk analysis starts with internal data of asset declarations and uses external sources as they become available. Cross-checks with external data sources can start with a few registers and gradually extend to include other data sources.

The external data sources usually include government databases and registers that hold information about ownership of assets, company registration, civil status, financial liabilities, tax payments, etc. Examples of external data sources that may be useful for verification include the following:

- Register of land rights and encumbrances
- Registers of different types of vehicles (cars, aircrafts, water vehicles)
- Company register, including information on beneficial ownership (if recorded)
- Register of associations and foundations (if separate from the company register)
- Databases of tax administration and pension fund/social security agency
- Register of civil acts (birth, death, marriage, etc.)
- Register of inheritance
- Register or database of issued powers of attorney
- Intellectual property rights registers
- Centralized register of bank accounts
- Database of public procurement operations
- Database of market prices for certain assets or goods
- Database of border crossing
- Registers of court decisions and arbitration awards

The external data sources might also include nongovernmental information. The declaration verification system may access private sector products, such as data aggregators, online marketplaces, and analytical products. The verification agency can also take advantage of the analytical products and other products built by civil society using AID data, such as the database of Politically Exposed Persons that contains historic data on PEPs and their related persons, results of media monitoring, and other sources.

The verification agency can also link data from declarations to other data it has collected or generated. Some agencies use media and open-source monitoring IT tools to search, collect, and analyze information on the declarants. Cross-checking declarations data with the results of such monitoring can result in additional alerts that need to be verified.

The verification agency may access external data sources based on bilateral data exchange agreements with the respective agencies or database owners. Access required for the automated risk analysis differs from manual remote access in which the verification agency officials can access a necessary data set by submitting individual requests or searching the database. The rationale of the automated risk analysis is to exclude human intervention at the initial stage and automate this process. The access mode, therefore, should provide for automated data exchange according to fixed parameters. Connecting two databases may take time. It would require mapping data categories in each database, agreeing on the format and content of data requests sent by the database of declarations and respective responses from the external data source. Such a connection may also face problems related to the lack of a common identifier (such as a unique personal identification number) or the use of several identifiers. Any data exchange should also use secure communication channels and secure methods of data transfer, and this may also require additional investment of resources.

Another option for data integration is using a government-wide interoperability platform that connects different government databases and offers standardized secure data exchange. Having such a digital government infrastructure will significantly facilitate introduction of the automated risk analysis of asset and interest declarations. However, at this time, such platforms are only operational in a few countries.

Cross-checking data is an important part of the verification of asset and interest declarations. However, it has its limits related mainly to the quality of data in external government registers. Often these registers include information that dates back only to the time of establishment of the register and do not hold historic data or data from legacy solutions. Data in registers often contain mistakes or are incomplete, which may cause many false-positive or false-negative results when the system applies risk indicators related to external sources to the declarations. In a framework where an inconsistency resulting from cross-checks of data triggers a mandatory verification of the declaration, this inconsistency may lead to a radical increase in the number of verifications that the verification agency has to carry out.

6. Extent to which the Automated Risk Analysis Framework Should Be Open to the Public

Transparency of the verification framework is important to build trust in the AID system and the verification agency's work. The public and officials who have the obligation of filing declarations should know and understand the verification procedures, including what triggers a verification; the scope and goal of the verification; what actions the verification agency can take to check information; the rights of the declarant in this process; and what information about a specific verification the public can have access to, under what condition, and at which stage.

This transparency includes the automated risk analysis. However, some details of the automated risk analysis may be withheld from public access subject to a country's legislation. The general approach to the risk assessment may be open to the public—the public and declarants should know how the verification agency conducts the analysis, what tools it uses, and how the analysis fits within the general verification framework. The agency could consider not to disclose the list of specific risk indicators (rules) that it applies to declarations and their weights. Knowledge of the specific indicators could help the declarants to hide assets or income or to try gaming the system in other ways. Disclosure of such indicators could be detrimental to the verification and limit its effectiveness.

Appendix. Examples of Risk Indicators (Red Flags)

A. Analyzing Data within One Declaration

- The declarant holds a high-risk position or performs high-risk functions.
- The declaration mentions a company registered abroad in which the declarant or family members have shares or which they control.
- The declaration does not mention any real estate held on any right.
- The declaration mentions real-estate property acquired in the reporting period without indicating the property's value (or mentioned that the declarant does not know it).
- The declaration mentions real estate located abroad, which belongs on any right to the declarant or family member.
- The declaration mentions more than X land plots belonging to the declarant or family members.
- The declaration mentions more than X apartments belonging to the declarant or family members.
- The declaration mentions more than X buildings belonging to the declarant or family members.
- The declaration mentions plots of land with the total area exceeding X square meters.
- The total value of real estate mentioned in the declaration exceeds the equivalent of US\$X.
- The declaration mentions an apartment with the area of more than X square meters.
- The declaration mentions real estate (except land) with the total area exceeding X square meters.
- The declaration mentions a residential building, farmhouse, etc. belonging to the declarant or family members and does not mention any plots of land.
- The declaration includes more than X items of valuable movable property (other than vehicles and collections).
- The declaration includes a collection of art, weapons, antiques, or other collection item in the movable property section of the form.
- The declaration mentions vehicles acquired during the reporting period without indicating the property's value (or mentioned that the declarant did not know it).

- The total value of vehicles mentioned in the declaration exceeds the equivalent of US\$X.
- The declaration mentions aircraft belonging on any right to the declarant or family members.
- The declaration mentions a water vehicle with the value of more than the equivalent of US\$X.
- The total value of securities mentioned in the declaration exceeds the equivalent of US\$X.
- The declarant or family member controls any asset as a beneficial owner.
- The declarant or family member is a nominal owner of an asset controlled by a third person (beneficial owner).
- The declarant has an interest in a trust (for example, is a settlor or beneficiary of a trust).
- Financial assets belonging to family members equal or exceed X percent of the total financial assets mentioned in the declaration.
- The total amount of financial assets mentioned in the declaration exceeds the equivalent of US\$X.
- The total amount of financial assets mentioned in the declaration exceed the total income received during the reporting period by X or more times.
- The amount of cash at hand mentioned in the declaration exceeds the equivalent of US\$X.
- The declaration does not mention any income received by the declarant during the reporting period.
- The declaration mentions a gift (several gifts) received by the declarant or family member during the reporting period whose total value equals or exceeds the equivalent of US\$X.
- The total value of monetary gifts received during the reporting period equals or exceeds X percent of the total income of the declarant and family members.
- The aggregate value of gifts received in connection with one event (such as a wedding) exceeds US\$X.
- The declaration includes income received from a foreign source (foreign national or foreign legal entity).
- The declaration includes income in the form of prizes, awards, lottery, or gambling wins in the total amount of or more than the equivalent of US\$X.
- The declaration mentions income in the form of royalty in the total amount of or more than the equivalent of US\$X.
- The total amount of income received by family members exceeds the income of the declarant X or more times.
- Income received by the declarant from sources other than main employment exceeds income from the main employment.

- The total combined income of the declarant and family members is below a certain threshold (for example, X minimum annual salaries).
- The declaration mentions income in the form of dividends though there are no corporate rights belonging to the declarant or family member that have been declared.
- The declaration mentions debts of the declarant or family in which the creditor is a foreign national or foreign legal entity.
- The declaration mentions that the declarant lent money to a third person in the amount exceeding US\$X.
- Total amount of money lent by the declarant to third persons is X times more than the overall income received by the declarant.
- The declaration mentions bank account(s) opened in financial institutions abroad.
- The declaration mentions valuable assets (above threshold X) that were acquired during the declarant's time in public office.

B. Comparing Data with External Databases

- Data mentioned in the declaration does not match data in the Land Register (a mismatch in the characteristics of the asset or asset not mentioned).
- Data mentioned in the declaration does not match data in the Register of Vehicles (a mismatch in the characteristics of the asset or asset not mentioned).
- Data mentioned in the declaration does not match data in the Company Register (a mismatch in the details of the company or company not mentioned).
- Data mentioned in the declaration does not match data in the National ID Register.
- Data mentioned in the declaration does not match data in the tax database (a mismatch in the details on the income or income not mentioned).
- Data in the declaration matches data in the public procurement database and alerts to the possible conflict of interest (for example, the cross-checks show that the company controlled by the declarant or family member was awarded procurement contracts by the agency where the declarant works).
- Data in the declaration matches data in the company register and/or tax database and alerts to the possible conflict of interest (for example, the cross-checks show that the declarant or family member acquired shares or control in the entity conducting commercial activity in the declarant's area of work).
- Data in the declaration matches data in the tax database and/or company register and alerts to the possible violation of postemployment restrictions (for example, the cross-checks show that the declarant—who used to work in tax administration—following dismissal from office received income as a tax consultant; or the declarant who worked in a regulator has acquired shares in a regulated entity shortly after dismissal).

C. Comparing with Data in the Previous Declarations of the Same Declarant

- The verified declaration mentions X or more new real estate items compared with the previous declaration of the declarant.
- The verified declaration mentions X or more new vehicles compared with the previous declaration of the declarant.
- The verified declaration mentions increase in the area of land plots of X or more square meters compared with the previous annual declaration of the declarant.
- The verified declaration mentions X or more new movable property items (except vehicles) compared with the previous annual declaration of the declarant.
- The verified declaration does not mention an asset that was mentioned in a previous declaration and does not mention any income from the disposal of such asset.
- The comparison of incoming and outgoing financial flows shows discrepancy above a certain threshold that may show signs of illicit enrichment or undeclared assets.
- The total amount of debts exceeds the sum of total financial assets in the previous annual declaration (the declaration filed a year before the declaration undergoing verification) and total income received in the reporting period (that is, the declaration that is verified).

D. Comparing with Declarations of Other Declarants

- The total income mentioned in the declaration exceeds the average income mentioned in the declarations of officials of the same category (such as judges, heads of departments) by a certain percentage.
- The total income mentioned in the declaration exceeds the average income mentioned in the declarations of all declarants in the same district/region by a certain percentage.
- Declarations with the highest number of certain types of assets when compared with declarations of the same type (for example, comparison among annual declarations submitted by all declarants in one period), for example:
 - Most land plots
 - Most apartments
 - Most vehicles
 - Highest income
 - Highest amount of private loans
- Declaration mentions items/values related to another declarant that are not mentioned in the other declarant's declaration (such as declaration of a family member who is also a declarant).



Asset and interest declarations of public officials are an essential part of the anti-corruption and integrity instruments used by governments all over the world to identify unjustified variations in assets of public officials, prevent conflicts of interests, improve integrity, and promote accountability in the public sector. To increase the effectiveness and efficiency of these instruments, many countries have started digitizing the various elements of the process including verification. Verification is key to an effective system of asset and interest declarations, as it ensures deterrence and thus enables the declaration system to fulfill its preventative function. Introducing automated elements in the verification process can significantly improve its efficiency. One of those elements is an automated risk analysis of declarations.

Automated risk or “red flag” analysis helps to filter declarations and prioritize verification. It increases the capacity of the agency tasked with verifying assets and interests of officials by focusing the agency’s limited resources on the verification of high-risk declarations. Automating the assessment of declarations also removes discretion, minimizes manual processes, and makes the whole system more impartial and credible.

This Technical Guide explains the role of automated risk analysis in an asset and interest disclosure system. It gives advice on how to organize the process of the risk analysis and what steps to take to develop the risk analysis framework. It also covers the issues of integration with external data sources and the level of the system’s transparency.

This guide builds on the advisory work conducted by the Stolen Asset Recovery Initiative (StAR) team with practitioners in different countries. It is intended for the management and staff of the anti-corruption or other agencies responsible for asset and interest disclosure systems. The guide will also help leadership of anti-corruption agencies and lawmakers endorse and promote innovative approaches in the verification of asset and interest declarations. Practitioners in law enforcement agencies can use this guide when developing their analytical tools to detect and investigate cases of unjustified assets and false declarations. Civil society may use parts of the guide in reviewing asset and interest declaration data if made available to them and to advocate new approaches in the verification of declarations conducted by state authorities.