



IntegriTAS Threat Assessment System: Process Guide





IntegriTAS Threat Assessment System: Process Guide

Catalina Uribe Burcher and Victoria Perotti

© 2018 International Institute for Democracy and Electoral Assistance

International IDEA publications are independent of specific national or political interests. Views expressed in this publication do not necessarily represent the views of International IDEA, its Board or its Council members.



The electronic version of this publication is available under a Creative Commons Attribute-NonCommercialShareAlike 3.0 (CC BY-NC-SA 3.0) licence. You are free to copy, distribute and transmit the publication as well as to remix and adapt it, provided it is only for non-commercial purposes, that you appropriately attribute the publication, and that you distribute it under an identical licence. For more information visit the Creative Commons website: http://creativecommons.org/licenses/by-nc-sa/3.0/.

International IDEA Strömsborg SE–103 34 Stockholm Sweden Telephone: +46 8 698 37 00 Email: info@idea.int Website: <http://www.idea.int>

Cover illustration: International IDEA Design and layout: International IDEA

Created with Booktype: https://www.booktype.pro

Contents

Acknowledgements 5	5
1. Introduction	5
2. Structure of the IntegriTAS system 8	3
1. Knowledge resources92. Analytical instruments103. Prevention and mitigation11)
3. Building the right IntegriTAS team 12	2
4. Stages of implementation	3
Cross-cutting activities14Preliminary decisions15Preparing the system16Implementation phase18Post-implementation analysis19	5
References 20)
About the authors	l
About IntegriTAS 22	2
About International IDEA	3

Acknowledgements

The authors would like to express their greatest appreciation to everyone who contributed to the conceptualization, design and piloting of the IntegriTAS Threat Assessment System, and to this Guide. Kristen Sample first encouraged International IDEA to pursue this idea, and Keboitse Machangana supported throughout the process of making it a reality. Nathalie Ebead, Kimana Zulueta-Fülscher and Brechtje Kemp guided the design process from the outset and provided valuable feedback. Catalina Perdomo contributed ideas, input and energy at various stages of the drafting process.

International IDEA would also like to thank Adam Boys, Raul Cordenillo, Elin Syberg Falguera, Karin Gardes, Lisa Hagman, Samuel Jones, David Prater, Annika Silva-Leander and Jorge Valladares for their careful reading, useful comments and helpful suggestions. Their contributions helped shape this Guide into what it is today.

International IDEA is especially grateful to staff in its regional and national offices, as well as the Institute's external partners and collaborators, for pooling their time, resources and efforts to pilot the IntegriTAS system in general, and this Guide in particular. Percy Medina and Luis Egúsquiza in Peru, and Nicholas Matatu in South Africa, invested countless hours to help ensure the success of the piloting exercises in each country. The Peruvian Electoral Tribunal and the Global Initiative against Transnational Organized Crime worked relentlessly in Peru in 2016, and in South Africa in 2017, providing the regional perspective that is at the core of this system.

Finally, thanks to the external peer reviewers, Francesco Strazzari and Gerd June, who provided constructive comments and concrete ideas, and to editor Kelley Friel, who helped make this Guide accessible for all kinds of readers.

1. Introduction

Transnational organized crime threatens democracy. Supporting the capacity of national and local institutions to prevent and mitigate the nexus between organized crime and democratic politics is an important part of fighting against these networks.

The IntegriTAS Threat Assessment System helps national and local institutions identify the threat that organized crime poses to politics. Focusing on the threat, instead of seeking to establish the existence of such links or their impact, allows users to map and focus on the factors that contribute to this type of corruption, and to identify strategies to prevent or mitigate the threat.

The system therefore uses a bi-dimensional approach, examining the incentives and drivers of these relations using a political economy analysis that considers the relevant stakeholders by focusing on (a) the democratic structure and specific vulnerabilities at different geographical levels according to the phase of the electoral cycle (International IDEA n.d.) and (b) the presence and scope of organized crime networks in the area. Coupling the analysis of these two dimensions allows users to identify, map and monitor the threat factors and subsequently plan and implement evidence-based prevention and mitigation strategies.

Users conduct the analysis by collecting and interpreting existing qualitative and quantitative data. The system is not designed to produce a detailed portrait of either dimension, but rather to highlight key factors according to the geographical scope assigned to the analysis, as well as to systematize and interpret existing data at that level.

The assessment process is based on two assumptions. The first is that a local institution leads the process from the onset. It could be the electoral management body, the office of the ombudsman, an anti-corruption agency, a law enforcement

agency, a civil society organization or an academic institution. The second assumption is that the process creates further opportunities for consultation and inclusion of various stakeholders throughout the country. The system therefore encourages users to complement the analytical process with dialogues in order to further interpret the data.

About this Guide

This Guide describes the process of implementing IntegriTAS, and includes a description of the system's structure and its implementation stages. It complements two other Guides: the *IntegriTAS Factors Guide* and the *IntegriTAS Prevention and Mitigation Guide*. The IntegriTAS software is also accompanied by a User Manual.

Access the IntegriTAS software and supporting documentation: <https://www.idea.int/integritas>.

2. Structure of the IntegriTAS system

IntegriTAS is a multipurpose data-driven software. It includes stand-alone knowledge resources to learn about the problem. If used together with the software, these resources help users analyse the situation by systematizing the data, displaying complex and sensitive information in different formats, creating early warnings, and collaborating between different communities of practice, including those working with elections, law enforcement, anti-corruption, security and peacebuilding. Most importantly, the system helps users take action by identifying and prioritizing prevention and mitigation strategies.

IntegriTAS is structured around three interactive modules:

- 1. *Knowledge resources*. A virtual library providing a list of factors that increase the threat that organized crime will distort democratic politics;
- 2. *Analytical instruments*. A software application that helps users easily map, geo-reference, present and visualize different types of democratic vulnerabilities and organized crime activities to build a country-specific model; and
- 3. *Prevention and mitigation*. A framework that equips users with global good practices and lessons learned for preventing and mitigating the influence of organized crime on democratic politics.

The three modules are integrated into a software application. They can be customized to respond to the context and needs of the user, and are designed to evolve as information is being uploaded. The modules are described below.

Table 2.1. Dimensions of the virtual library

Organized crime	Democratic vulnerabilities
 Drug trafficking Firearms trafficking Human trafficking Contraband smuggling and trafficking in counterfeit goods Illicit trafficking in wildlife Illegal mining Systematic abuse of state resources Illegal waste dumping Cybercrime Protection rackets Money and asset laundering 	Foundational 1. Socio-economic conditions 2. Political transition processes 3. Geostrategic conditions Institutional 1. Rule of law and access to Justice 2. Political parties 3. Legislature 4. Public administration 5. Electoral system Associated 1. Media and civil society watchdogs 2. Financial system

1. Knowledge resources

This module is a virtual library providing a list of factors that increase the threat that organized crime will distort democratic politics. The factors are divided into two parallel dimensions: (a) organized crime and (b) democratic vulnerabilities (see Table 2.1). In each dimension the user can customize the list of factors according to the specific geographic area or local context. The content of the democratic vulnerabilities dimension is derived and adapted from International IDEA's State of Democracy Assessment Framework (Beetham et al. 2008). Each factor includes (a) a general definition and explanation of the context in which it can contribute to the nexus between organized crime and politics; (b) examples in which the factor contributed to the nexus between organized crime and politics; and (c) observable indicators. After the knowledge resources are customized, the user can create analytical models by selecting factors to monitor.

The analysis of these two dimensions may entail dynamics with different territorial scopes: while democratic vulnerabilities typically apply to national or local actors and processes, organized crime includes local, national and transnational networks. Even the analysis within each dimension may highlight dynamics at different geographic levels. Indeed, various criminal networks with different territorial reach may operate in the same place; likewise, institutions with different levels of competence might have a stake in the nexus between organized crime and politics. Therefore, to take full advantage of the system's capacity to highlight these dynamics at various levels, the user should be clear from the onset regarding the geographic level of analysis, the purpose of the assessment, and the reach of the potential prevention and mitigation strategies.

2. Analytical instruments

This module consists of a software application that helps users easily map, georeference, present and visualize different types of democratic vulnerabilities and organized crime activities to build a country-specific model. The user uploads relevant qualitative and quantitative data on particular factors according to the regions and dates selected to create threat maps, threat trends and alerts. The maps can be adapted to highlight certain information through colour codes, numbers, static markers and trend charts (see Figure 2.1). In addition, the user can populate and maintain a 'threat and action register' that suggests actions based on the prevention and mitigation module.



Figure 2.1. Examples of mapping exercises, colour coding and trend charts

Source: IntegriTAS Threat Assessment System [screenshots]

Customization features include a mapping manager that allows users to upload or draw geographic maps (SHP and DB files), and a model customization to create country-specific analytical models.

The analytical component includes:

- 1. Data entry interfaces that allow entries for selected factors, regions and dates according to the threat level (Uribe Burcher and Perotti 2018).
- 2. Data presentation interfaces that display data in the form of (a) colourcoded geographic areas, (b) numerical values, (c) static markers, and (d) trend charts. Data can be viewed for selected regions, dates and factors.
- 3. A threat and action register that allows users to generate alerts and recommend prevention and mitigation actions.

The IntegriTAS system allows users to export, import or delete analytical models. Maps can be saved within the model and exported as high-resolution pictures or KML files that are Google Earth compatible. Outputs generated by analytical instruments can present complex and multi-layered threat data in a simple and user-friendly format.

3. Prevention and mitigation

This module is comprised of a framework that equips users with global good practices and lessons learned for preventing and mitigating the influence of organized crime on democratic politics. These can be used to inspire the design of integral context-specific strategies, which orbit around the two dimensions used to select the factors: democracy and organized crime. These dimensions focus on (a) combating organized crime in areas that target political corruption and (b) curbing political corruption related to the interests of organized crime networks. Looking at these two sets of policies and practices in tandem creates a coherent approach to preventing and mitigating organized crime involvement in democratic politics.

3. Building the right IntegriTAS team

Building a competent pool of personnel ensures the users' capacity to implement the system. Team members should have professional experience in data collection and analysis, as well as relevant knowledge of local democratic vulnerabilities and organized crime activities. The team should include:

- 1. a hub manager or thematic coordinator who coordinates information exchanges, directs analysis on the factors and indicators, guides the preparation of reports and shares alerts;
- 2. a data analyst who coordinates internal and external data collection and ensures data quality, analyses data to generate threat maps and trend charts, and generates alerts and drafts reports; and
- 3. data entry clerks who compile and consolidate data and make data entries, and provide analytical outputs for specific regions, factors and periods.

The local institution leading the process also creates a steering group with all institutions that contribute to the assessment process. This platform helps the lead institution focus the assessment and create momentum to implement prevention and mitigation measures.

4. Stages of implementation

Table 4.1 and Figure 4.1 outline the key stages of the IntegriTAS process.

Table 4.1. Key stages of the IntegriTAS process

Stage	Activity
Cross-cutting activities	Ownership and broader committment Gender mainstreaming Conflict sensitivity
Preliminary decisions	Establishing the purpose and added value of the assessment Stakeholder mapping Formalizing the process and consultative arrangements with stakeholders Agreeing on the content and priorities of the assessment Building a team and division of labour Deciding on the timing of the process Planning upcoming reports and socialization strategy
Preparing the system	Context overview exercise IntegriTAS customization process Operational design
Implementation phase	Data collection Data analysis Model revision Periodic reports Validation dialogues
Post-implementation analysis	Final report with prevention and mitigation strategies Dissemination and advocacy strategy Feedback exercise

Figure 4.1. IntegriTAS threat assessment process



Cross-cutting activities

Ownership and broader commitment

The assessment process requires full ownership and empowerment of the local institution leading the process. Further commitment by a wide range of partner organizations also facilitates synergies and information sharing, and gives credibility to the process and its results. The more representative this group of institutions is, the greater the legitimacy of the assessment and the chances it will influence public debate and policy making. A steering group that involves these institutions therefore serves to formalize the process and guide the lead institution to focus and direct the assessment. It also functions as a platform to discuss

preliminary findings and help formulate adequate measures based on the prevention and mitigation framework (third module).

Gender mainstreaming

Users should employ a gender-sensitive lens throughout the assessment process to include specific considerations that affect women and men in various aspects of the system, particularly the process design, the data collection phases, the selection of factors and indicators, and the selection and implementation of prevention and mitigation strategies.

Conflict sensitivity

Users should consider how the planning and implementation of the assessment exercise may exacerbate tensions and conflict, and should consider strategies to mitigate those potential threats. Thus, the system should be customized to ensure that it captures these sensitive conditions to minimize harmful effects, while retaining its integrity and original purpose. Particularly polarizing events, such as upcoming elections, may require users to adapt the assessment process to decrease potential risks to the team and the organizations providing data.

Preliminary decisions

The lead organization takes seven types of decision in consultation with the steering group.

- 1. It establishes the purpose and added value of the assessment and how it fits within the electoral cycle. Depending on the user and timing of the assessment, the system can help prioritize resources for electoral observation, deploy security personnel to critical areas, improve interagency coordination, and present legislative initiatives to curb illicit political finance. By providing a broader understanding of the process and how it responds to the users' goals, this decision also shapes the content of the assessment and focuses the recommendations, thus informing the timescale. It also serves to inform the public and potential donors about the focus of the project.
- 2. It engages in stakeholder mapping to identify which institutions and experts need to be engaged in the process, how and when. Different people and institutions might be engaged during different phases of the assessment, including target users and audiences who can potentially endorse and follow up on the assessment findings.

- 3. It formalizes the process and consultative arrangements with stakeholders through informal arrangements or official agreements, depending on the inter-institutional dynamics. Formal agreements (e.g. memorandums of understanding, cooperation agreements, letters of understanding and contracts) clarify commitments from (and coordination with) main partners and other stakeholders, ensuring communication flows across institutions.
- 4. It facilitates agreement on the content and priorities of the assessment according to its relevance to stakeholders and the timing of the process within the electoral cycle. This allows the process to be targeted to the institutional objectives of the partner institutions and their expertise in relation to the democratic vulnerabilities and the organized crime activities that are most relevant in the local context.
- 5. It builds a team and division of labour to ensure that the user has the required technical and thematic expertise to collect and analyse the data.
- 6. It decides on the timing of the process in accordance with the purpose of the assessment and in relation to the timing of the electoral cycle. This decision sets the parameters for how far reaching the analysis can be, and how the prevention and mitigation strategies will be tailored.
- 7. Finally, it plans upcoming reports and the socialization strategy, including formats (e.g. print or digital) and whether they will be public or confidential. Since the reports seek to support reform processes, they should be used to engage policymakers and citizens in the implementation of recommendations according to the main purpose of the assessment. Also, deciding if and how the validation exercise, report launch, and other dissemination and advocacy activities will be conducted shapes relations with the public and partners. Clarity regarding how, when and with whom the information will be shared helps avoid misunderstandings during the implementation stage.

Preparing the system

First, a context overview exercise should be conducted that allows users to customize the system to focus on the most important factors that might increase the threat of organized crime influencing democratic politics. This process draws on a historical and trend analysis to identify: (a) factors based on democratic vulnerabilities and the presence of organized crime, which combined would increase the threat of organized crime distorting politics; (b) combinations of factors that might appear in different geographical regions and in different stages of the electoral cycle; and (c) possible strategies to prevent and mitigate the threat of organized crime's influence on democratic politics, which are informed by prevention and mitigation strategies in other country and regional contexts.

This exercise should include the views of a wide range of actors representing different communities of practice, such as experts on elections, security, peacebuilding and anti-corruption; different affiliations with government, nongovernmental organizations and academia, both national and foreign; different geographic regions at the national, subnational and local levels; and different social groups according to gender, age, ethnicity and religion.

Useful methodologies to facilitate combining different perspectives may include expert workshops, focus group discussions, public opinion surveys, ethnographic research and written contributions that compile data analysis.

Second, the IntegriTAS customization process creates a baseline document to capture the results of the context overview exercise based on IntegriTAS' knowledge resources. This document, which further informs operational planning, describes each factor in two sections: (a) introduction and (b) observable indicators.

The customization should be informed by the priorities chosen by the lead organization, which can be re-considered during the operation design stage. Indeed, the scope of the assessment should be limited to factors and observable dynamics that are relevant to the context. The customization process also includes using the system's software to create an analytical model according to the following parameters: (a) geographical scope of the analysis; (b) timing of the assessment process within the electoral cycle; (c) factors included in the model (a default tick box list re-selects the factors defined in the knowledge resources module); and (d) factors' properties (e.g. values of interval scale, weight and display options).

Third, the model's operational design draws on the baseline assessment document to operationalize factors by identifying four parameters:

1. The data sources and collection methodologies for measuring each factor and indicator. The user determines whether data already exists or can be collected, as well as who possesses it or can collect it. Accordingly, designing the data collection methodology includes determining: how each factor and indicator can be measured; how to obtain data (e.g. gather official records, conduct interviews or surveys, engage in fact finding, monitor the media, establish lines of citizens' reporting); and who is collecting or providing data—for example, internal staff, external partners agencies or contracted agencies. The amount of data and its collection and analysis methodology may require updating the resources allocated to the process and prioritizing them.

- 2. The periodicity—how often data should be collected and analysed—for example, daily, weekly, bi-weekly, monthly or one time only. If used on a continuous basis, the amount of data stored in the system increases over time, thus taking full advantage of its capacity to process large amounts of qualitative, quantitative and geo-referenced information. This will allow for a better targeting of the monitoring exercise, and inform and focus reform processes.
- 3. The training and translation needs. The implementation process may require increasing the capacity of the team at several levels, including: the management of the lead organization, who can benefit from an exchange with the technical personnel using the system; the technical staff, who can learn more about the system's knowledge resources and software from joint teams that combine thematic knowledge and IT skills, as well as from peers who have already used the system; and the data collection staff, including surveyors, who can be guided by the technical staff to ensure that the 'new data' collection effort is consistent and standardized across the country.
- 4. The available financial, human and time resources according to the factors and indicators selected, the timing and periodicity of the assessment, the methodology used to collect and analyse data, as well as the training and translation needs. Some prior decisions often need to be revised and factors prioritized to accommodate existing and incoming resources.

Implementation phase

The implementation phase entails five continuous processes. First, data is gathered and entered. Second, data is analysed, which includes (a) generating situation analyses and threat alerts with recommendations on possible prevention and mitigation actions; (b) sharing threat alerts and maps internally and externally; (c) generating a threat and action register to understand the effectiveness of actions undertaken; and (d) monitoring the results of specific actions.

Third, the model is revised periodically to ensure that the data collection and analysis focus on the most prominent and emerging threats throughout the process. Reviewing the threats and action register will help understand any gaps in data collection and analysis, and ensure that threat alerts are effectively issued and acted on.

Fourth, periodic reports are generated to allow users to present complex and multi-layered threat data in a simple and user-friendly format. Finally, validation dialogues are created to share preliminary analysis and recommendations with a wider audience, including the steering group and other strategic stakeholders. These spaces facilitate further commitment among relevant actors throughout the process, particularly when gathering support to implement prevention and mitigation strategies at a later stage.

Post-implementation analysis

A final report with prevention and mitigation strategies should be written to reflect the analysis generated throughout the process. The production of the report and its launch should be inclusive processes, thus facilitating dialogue and ensuring broad commitment to implement the recommendations. The user can also implement an advocacy strategy that entails organizing follow-up events to disseminate and monitor implementation of recommendations, further sharing the process with the public and other experts in the area. A final feedback exercise should be conducted with stakeholders to collect lessons learned about the implementation process, for example through interactive workshops, focus group discussions, surveys and consultations. This exercise will help users decide whether to continue using the system, and how, and to devise other efforts to combat political corruption and organized crime to maintain a collaborative environment that facilitates those efforts.

References

- Beetham, D., Carvalho, E., Landman, T. and Weir, T., Assessing the Quality of Democracy: A Practical Guide (Stockholm: International IDEA, 2008), http://www.idea.int/publications/catalogue/assessing-quality-democracy-practical-guide>, accessed 1 April 2018
- International Institute for Democracy and Electoral Assistance (International IDEA), Online Electoral Cycle, [n.d.], https://www.idea.int/data-tools/tools/online-electoral-cycle, accessed 1 November 2017
- ---, State of Democracy Assessments, [n.d.], <https://www.idea.int/data-tools/ tools/state-democracy-assessments>, accessed 1 November 2017
- Uribe Burcher, C. and Perotti, V., *IntegriTAS Factors Guide* (Stockholm: International IDEA, 2018), <https://www.idea.int/data-tools/tools/ integritas>, accessed 1 April 2018
- Uribe Burcher, C. and Sample, K., *IntegriTAS Prevention and Mitigation Guide* (Stockholm: International IDEA, 2018), <https://www.idea.int/data-tools/tools/integritas>, accessed 1 April 2018

About the authors

Catalina Uribe Burcher is a Senior Programme Officer at International IDEA. Her work focuses on research and policy-oriented analysis regarding the relationships between organized crime and democracy. She has co-authored reports and articles on this topic in relation to Latin America, West Africa and the Baltic States. She has also worked as an independent consultant for the Colombian Ministry of Foreign Affairs and as coordinator of a programme caring for victims of the armed conflict in Colombia. She is a Colombian lawyer with a specialty in criminal law, and holds a master's degree in international and comparative law from Uppsala University, Sweden.

Victoria Perotti is an Associate Programme Officer in the Democracy Assessment and Political Analysis Unit at International IDEA. Her work focuses on democracy, conflict and security and on research and policy-oriented analysis regarding post-conflict democratization processes. Prior to joining International IDEA, she coordinated a global network of parliamentarians and led projects on disarmament and arms control in Latin America, Europe and the Middle East. She earned her degree in international relations at the Universidad Siglo XXI in Córdoba, Argentina, and is currently specializing in security policy at the Swedish Defense University.

About IntegriTAS

Transnational organized crime threatens democracy. Supporting the capacity of national and local institutions to prevent and mitigate the nexus between organized crime and democratic politics is an important part of fighting against these threats. The IntegriTAS Threat Assessment System is a multipurpose datadriven software application that helps national and local institutions identify the threats that organized crime poses to politics.

Documentation

The IntegriTAS software is accompanied by three Guides. The *IntegriTAS Process Guide* describes the process of implementing IntegriTAS, and includes a description of the system's structure and its implementation stages. The *IntegriTAS Factors Guide* provides basic definitions of the threat factors used in IntegriTAS, and includes an Annex which provides a more comprehensive list of potential indicators that can be used to observe each factor. The *IntegriTAS Prevention and Mitigation Guide* discusses the various prevention and mitigation strategies that can be applied to reduce the undue influence of organized crime on democratic processes. The software is also accompanied by a User Manual and a help file.

Download

Access the IntegriTAS software and supporting documentation: https://www.idea.int/integritas

About International IDEA

The International Institute for Democracy and Electoral Assistance (International IDEA) is an intergovernmental organization with the mission to advance democracy worldwide, as a universal human aspiration and enabler of sustainable development. We do this by supporting the building, strengthening and safeguarding of democratic political institutions and processes at all levels. Our vision is a world in which democratic processes, actors and institutions are inclusive and accountable and deliver sustainable development to all.

What do we do?

In our work we focus on three main impact areas: electoral processes; constitution-building processes; and political participation and representation. The themes of gender and inclusion, conflict sensitivity and sustainable development are mainstreamed across all our areas of work.

International IDEA provides analysis of global and regional democratic trends; produces comparative knowledge of good international democratic practices; offers technical assistance and capacity-building on democratic reform to actors engaged in democratic processes; and convenes dialogue on issues relevant to the public debate on democracy and democracy building.

Where do we work?

Our headquarters are located in Stockholm, with regional and country offices in Africa, the Asia-Pacific, Europe and Latin America and the Caribbean. International IDEA is a Permanent Observer to the United Nations and is accredited to European Union institutions.

<http://idea.int>

Transnational organized crime threatens democracy. Supporting the capacity of national and local institutions to prevent and mitigate the nexus between organized crime and democratic politics is an important part of fighting against these threats.

The IntegriTAS Threat Assessment System is a multipurpose data-driven software application that helps national and local institutions identify the threats that organized crime poses to politics. Focusing on the threat instead of seeking to establish the existence of links between organized crime and politics, or their impact—allows users to map and focus on the factors that contribute to corruption, and to identify strategies to prevent or mitigate the threat.

The IntegriTAS software is accompanied by three Guides and a User Manual. The *IntegriTAS Process Guide* describes the process of implementing IntegriTAS. It includes a description of the system's structure and its implementation stages.

International IDEA Strömsborg SE–103 34 Stockholm Sweden Telephone: +46 8 698 37 00 Email: info@idea.int Website: <http://www.idea.int>