Government data-driven decision-making (DDDM) framework implementation.

Deliverable 3: Test case: crisis management

Technical Support Instrument
Supporting reforms in 27 Member States

Funded by the European Union

Republic of Estonia Government Office

This document was produced with the financial assistance of the European Union. Its content is the sole responsibility of the author(s). The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

The project is funded by the European Union via the Technical Support Instrument, managed by the European Commission Directorate-General for Structural Reform Support.

This report has been delivered in June 2022, under the EC Contract No. REFORM/SC2021/076. It has been delivered as part of the project "Government data-driven decision-making (DDDM) framework implementation. Test case: crisis management".

© European Union, 2024

The Commission's reuse policy is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39 – https://eur-lex.europa.eu/eli/dec/2011/833/oj).

Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated.

Directorate-General for Structural Reform Support
REFORM@ec.europa.eu
+32 2 299 11 11 (Commission switchboard)
European Commission
Rue de la Loi 170 / Wetstraat 170
1049 Brussels, Belgium

Funded by the European Union via the Structural Reform Support Programme and implemented by the OECD, in cooperation with the European Commission. Framework Delegation Agreement REFORM/IM2021/005

Project 21EE02
GOVERNMENT DATA-DRIVEN DECISION-MAKING (DDDM) FRAMEWORK IMPLEMENTATION
TEST CASE: CRISIS MANAGEMENT

Output 3

OECD’s recommendations for the implementation of the redesigned DDDM framework, including in crisis management.

This document has been produced by the OECD under the leadership of the Digital Government and Data Unit (Open and Innovative Government Division, Directorate for Public Governance) and the Risk Governance Unit (Governance Reviews and Partnerships Division, Directorate for Public Governance).

Background

1. This document is part of third Output **(Output 3)** that results from the activities implemented by the OECD in the context of the European Commission's (EC) Technical Support Instrument (TSI) Project 21EE02 *Government Data-Driven Decision-Making (Dddm) Framework Implementation. Test Case: Crisis Management* (hereinafter "*the Project*").

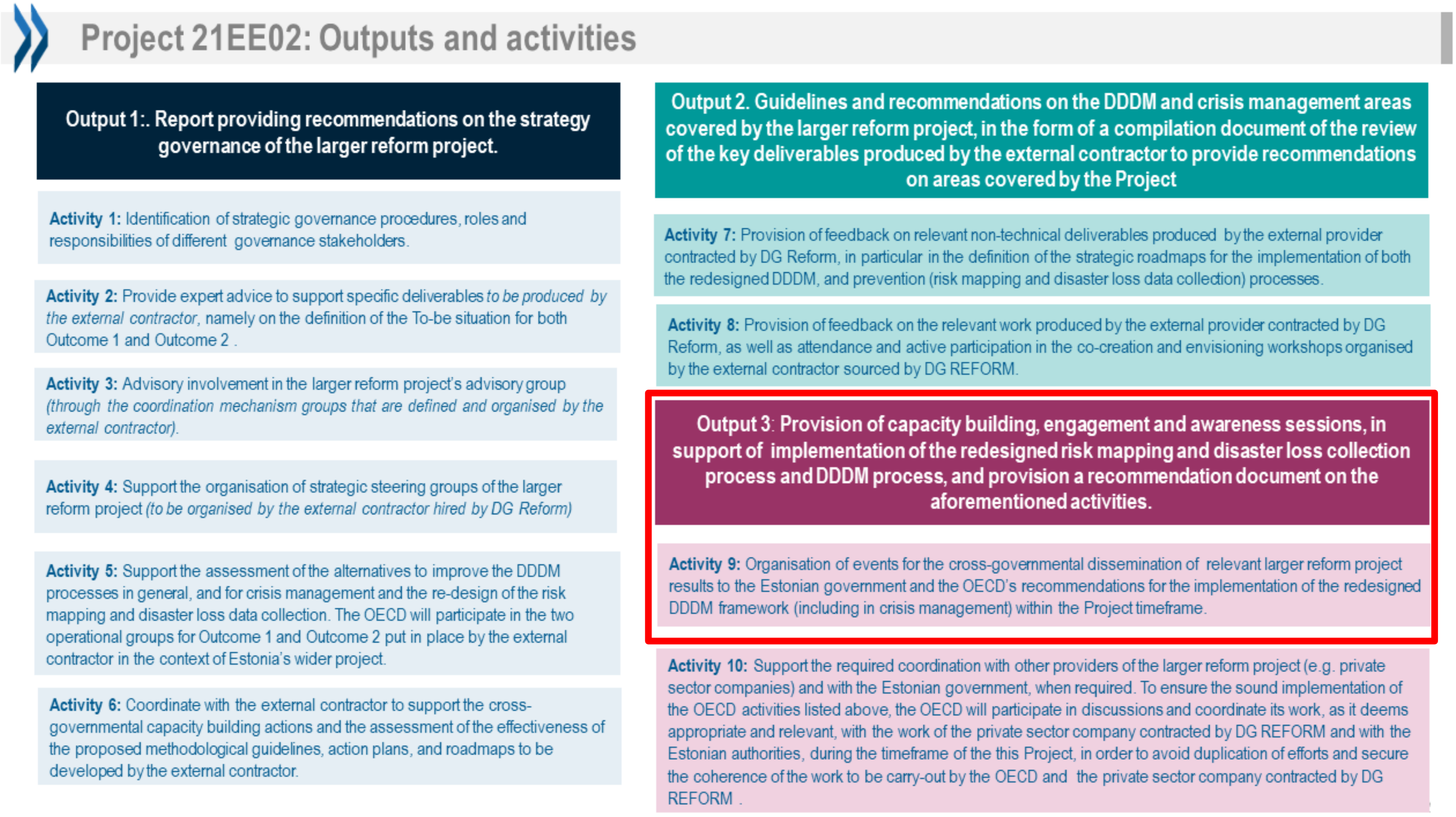
2. This Output 3 is framed in the context of the Outcomes, Outputs, and Activities described in the Project's final Detailed Project Description (DPD) endorsed by the EC Directorate General for Structural Reform Support (DG REFORM) on 18 May, 2022.

3. As described in the DPD, this document provides key OECD's recommendations for the implementation of the redesigned DDDM framework (including in crisis management) within the Project timeframe. As such, the recommendations aim to support for the implementation of the reform in line with OECD best practices and OECD frameworks in the areas of digital government, data-driven public sector, and crisis management.

4. This document mainly results from the implementation of this Project's Activity 9 under Output 3 by the OECD (see Figure 1):

- **Activity 9:** Organisation of events for the cross-governmental dissemination of relevant larger reform project results to the Estonian government and the OECD's recommendations for the implementation of the redesigned DDDM framework (including in crisis management) within the Project timeframe. The overall reform project's success depends greatly on the communication of its results, as well as on the understanding and acceptance of the recommendations not only by the Government Office of the Republic of Estonia but also by the stakeholders. For this purpose, the OECD will organise cross-governmental dissemination events with relevant stakeholders from the Estonian public sector to share the results from the overall reform project that are available at that time and relate the OECD's technical assistance described in this Project. These events will also be an opportunity for the OECD to present its recommendations for the implementation of the reform, to disseminate best practices and OECD frameworks in the areas of digital government and data-driven public sector, and crisis management. The OECD will share relevant information on reform results that may have yielded from this Project and will communicate it in a way that is both understandable and relevant. To this effect, the media used for this dissemination is at the full discretion of the OECD and will be discussed with Estonia.

Figure 1. Project 21EE02: Outcomes, Outputs and Activities



Project 21EE02: Outputs and activities

Output 1:. Report providing recommendations on the strategy governance of the larger reform project.

Activity 1: Identification of strategic governance procedures, roles and responsibilities of different governance stakeholders.

Activity 2: Provide expert advice to support specific deliverables *to be produced by the external contractor*, namely on the definition of the To-be situation for both Outcome 1 and Outcome 2 .

Activity 3: Advisory involvement in the larger reform project's advisory group *(through the coordination mechanism groups that are defined and organised by the external contractor).*

Activity 4: Support the organisation of strategic steering groups of the larger reform project *(to be organised by the external contractor hired by DG Reform)*

Activity 5: Support the assessment of the alternatives to improve the DDDM processes in general, and for crisis management and the re-design of the risk mapping and disaster loss data collection. The OECD will participate in the two operational groups for Outcome 1 and Outcome 2 put in place by the external contractor in the context of Estonia's wider project.

Activity 6: Coordinate with the external contractor to support the cross-governmental capacity building actions and the assessment of the effectiveness of the proposed methodological guidelines, action plans, and roadmaps to be developed by the external contractor.

Output 2. Guidelines and recommendations on the DDDM and crisis management areas covered by the larger reform project, in the form of a compilation document of the review of the key deliverables produced by the external contractor to provide recommendations on areas covered by the Project

Activity 7: Provision of feedback on relevant non-technical deliverables produced by the external provider contracted by DG Reform, in particular in the definition of the strategic roadmaps for the implementation of both the redesigned DDDM, and prevention (risk mapping and disaster loss data collection) processes.

Activity 8: Provision of feedback on the relevant work produced by the external provider contracted by DG Reform, as well as attendance and active participation in the co-creation and envisioning workshops organised by the external contractor sourced by DG REFORM.

Output 3: Provision of capacity building, engagement and awareness sessions, in support of implementation of the redesigned risk mapping and disaster loss collection process and DDDM process, and provision a recommendation document on the aforementioned activities.

Activity 9: Organisation of events for the cross-governmental dissemination of relevant larger reform project results to the Estonian government and the OECD's recommendations for the implementation of the redesigned DDDM framework (including in crisis management) within the Project timeframe.

Activity 10: Support the required coordination with other providers of the larger reform project (e.g. private sector companies) and with the Estonian government, when required. To ensure the sound implementation of the OECD activities listed above, the OECD will participate in discussions and coordinate its work, as it deems appropriate and relevant, with the work of the private sector company contracted by DG REFORM and with the Estonian authorities, during the timeframe of the this Project, in order to avoid duplication of efforts and secure the coherence of the work to be carry-out by the OECD and the private sector company contracted by DG REFORM .

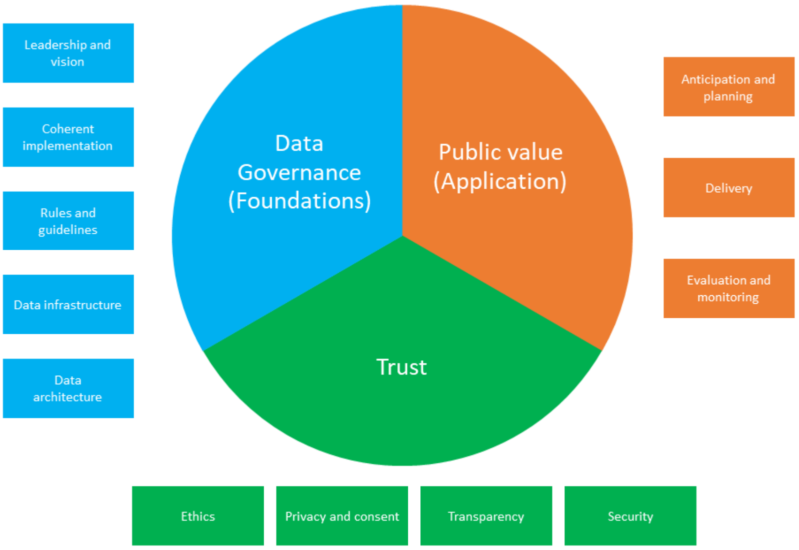
Source: Based on TSI Project 21EE02's Detailed Project Description

Outcome 1: Data-driven decision making (DDDM)

5. This section compiles key OECD observations and recommendations to support the implementation of the DDDM tool in Estonia. These are based on the data and insights collected by the OECD during the meetings organised with key stakeholders from the public sector in the context of the OECD mission to Tallinn, Estonia that took place on 21 – 22 February, 2023.

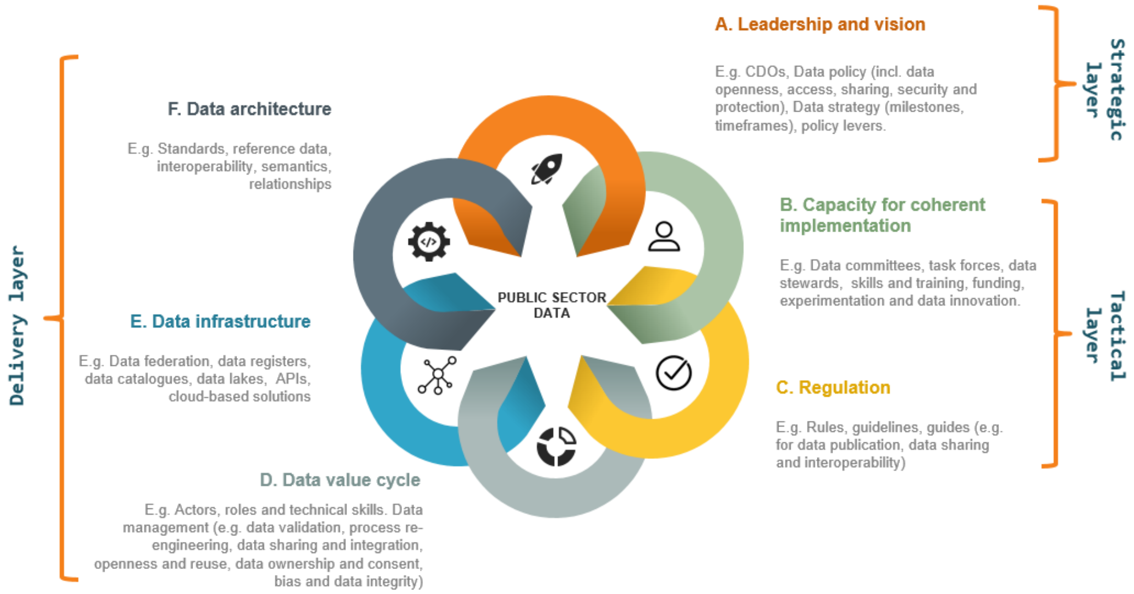
6. The analysis presented in the following sub-sections is based on the OECD framework for data governance in the public sector (Figure 2), the OECD model for data-driven public sector (Figure 3) (OECD, 2019[1]), and the OECD work on Artificial Intelligence.

Figure 2. OECD Model for a data-driven public sector



Source: 2019 OECD Report The Path to Becoming a Data-Driven Public Sector. Available at: https://www.oecd.org/gov/the-path-to-becoming-a-data-driven-public-sector-059814a7-en.htm

Figure 3. Data governance in the public sector


A. Leadership and vision
E.g. CDOs, Data policy (incl. data openness, access, sharing, security and protection), Data strategy (milestones, timeframes), policy levers.
Strategic layer
F. Data architecture
E.g. Standards, reference data, interoperability, semantics, relationships
B. Capacity for coherent implementation
E.g. Data committees, task forces, data stewards, skills and training, funding, experimentation and data innovation.
Delivery layer
PUBLIC SECTOR DATA
E. Data infrastructure
E.g. Data federation, data registers, data catalogues, data lakes, APIs, cloud-based solutions
Tactical layer
C. Regulation
E.g. Rules, guidelines, guides (e.g. for data publication, data sharing and interoperability)
D. Data value cycle
E.g. Actors, roles and technical skills. Data management (e.g. data validation, process re-engineering, data sharing and integration, openness and reuse, data ownership and consent, bias and data integrity)

Source: 2019 OECD Report The Path to Becoming a Data-Driven Public Sector. Available at: https://www.oecd.org/gov/the-path-to-becoming-a-data-driven-public-sector-059814a7-en.htm

Data governance

7. This sub-section assesses the current state of the data governance envinronment framing the DDDM tool. For this purpose, it follows the three main components of the OECD framework for data governance in the public sector (Figure 3) and underlines challenges, opportunities and recommendations that can help to support implementation in the main forward.

8. This section does not explore in detail the regulatory and technical aspects of the DDDM tool as those were covered as part of the deliverables produced by the external contractor. The Government Office is taking additional actions since February 2022 to further assess regulatory challenges and barriers.

Strategic layer

Leadership and strategy

> Whereas stakeholders acknowledge the relevant of the DDDM tool, co-desiging a roadmap for its implementation would help to increase clarity on the way ahead, including in terms of expectations.

9. In terms of the DDDM tool, the lead role of the Government Office and the supportive role of the National Statistics Office are well acknowledged by stakeholders. Challenges remain nevertheless in relation to the way ahead, timeframes, milestones and roles other stakeholders will play during the

implementation stage. During the OECD mission to Tallinn, stakeholders expressed the lack of clarity from the Government Office in terms of next steps and expectations in terms of the role that stakeholders from the public sector would play in advancing the DDDM tool. This, despite the availability of a draft roadmap developed by the external contractor.

10. While since February 2023 actions have been taken to further engage stakeholders, developing a revised roadmap for the way ahead could help to build up trust in the DDDM tool, its design and implementation, and shed further light for the short-, mid- and long-term. Engaging key stakeholders to co-design the revised version of the roadmap could also help to increase buy in and better align the DDDM tool with other initiatives in place.

The participation of Statistics Estonia and the Information System Autority (RIA) in both the DDDM tool governance structure and Estonia's National Data Governance Board offers a great opportunity to ensure aligment between the DDDM tool's goals and timeframes with those of Estonia's National Data Strategy. This in order to exploit synergies and avoid duplication of efforts.

11. At a larger scale, there is a need to further fit the DDDM tool in the broader context of Estonia's efforts to advance a data-driven public sector. The Government Office and Statistics Estonia (as owners of the DDDM tool) would need to align ambitions, timeframes and potentially its governance and operational mechanisms with those of broader national data strategies, initiatives and tools either in place or under development. This, including those related to Estonia's National Data Portal and the RIHAKE (both relevant for the design and implementation of the DDDM tool and its goal to pool data from multiple sources within the public sector).

12. Last, whereas great efforts would be needed at the technical level (e.g. in terms of data cataloguing, standardisation and integration), aligment with relevant available standards and guidelines on data interoperability would require self-assesing if the policy levers at hand are sufficient to enforce compliance with data standards at the data owner level and what organisation would be in charge of enforcing those standards and how.

Risk-management and accountability for the DDDM tool

Aligning the DDDM tool's governance with existing frameworks on AI in public sector, data ethics, AI ethics, personal data protection and with AI oversight mechanisms in the public sector could help to identify and better manage DDDM tool's related risks from the outset. Developing an *ad hoc* risk framework for the use of the DDDM tool with specific practical recommendations would help in this regard.

13. As a system owned by the Government Office and developed with the support of Statistics Estonia and other bodies, the DDDM tool is intended, in a first stage, to support the process of developing the Government Memorandum by tapping on data sources from inside and outside the public sector. Nevertheless, with the long-term vision of building a smart assistant for government's decision-making will

come need for clarity of the distribution of responsibility and accountability. For instance, should the DDDM tool does not respond to system users' expectation and needs, or should the decisions informed by the DDDM tool produce an unintended negative impact on people.

14. Failure to acknowledge and address risks can have an impact on the reliability of the DDDM tool and the decisions its outputs will inform. Taking a risk-mangement approach from the outset could help to better manage risks and avoid negative consequences at all levels – including at the political level. In particular as the system moves towards automation[1]. These concerns were raised by the OECD as part of the feedback provided to the deliverables produced by the external contractor (see Output 2).

15. Potential risks are observed at different levels and range from data-specific risks, to others which are more procedural or long-term. These can include but are not limited to:

- **Data holder:** Data is not prepared according to pre-defined standards but fed into the system, semantic interoperability, data does not exist, data is incomplete, data is not granular (when needed), data readiness does not match the needs of the DDDM system, data discoverability and accessibility, and conflicts between data sources (authoritative data, *source of truth*).
- **System user:** For instance, taking the DDDM system's outputs as definitive without putting them into perspective or bringing sectoral expertise to make better decisions; data selection being incomplete or biased; lack of data governance and transparency over data sources; data provenance.
- **System owner:** In the short term, explanibility will play a key role in building confidence in the DDDM system. For instance, in terms of ensuring any Government decisions (Memorandums) backed up or informed using outputs from the DDDM system are properly identifiable, transparent and auditable. In the long term, as explored by the OECD in the context with AI Generative tools (Lorenz, 2023[2]) and as the DDDM system matures and moves toward automation, power distribution (e.g. increasingly delegating decision-making to a future AI-powered DDDM tool), could potentially blur accountability and responsibility. At the same time, managing risks of a potential automated DDDM tool will require opening its algorithms for public audit.

16. Risks at the data holder and system user level can be addressed through investments on data management skills and training courses and supported by the development of guidelines for the use of the DDDM system. Yet, advancing towards more mature stages of data-driven decision making in Estonia would require investing greater efforts to explore and manage current and potential future risks of the tool not only from a data governance but also from an AI governance perspective. Approaching the DDDM tool from a AI and data governance point of view was stressed as part of the feedback provided by the OECD to the deliverables produced by the external contractor.

> Estonia's mechanisms for AI and data governance in the public sector should frame the design and implementation of the DDDM tool. But taking a forward -looking approach to risk management could help to built a more reliable and trustworthy DDDM system from the outset.

17. A forward-looking approach could also include interpreting and embedding the implications of Generative AI in the further conceptualisation and implementation of the DDDM system. Whereas exploring the development and use of Generative AI in government is still new and under development

[1] See for instance the case of the Australia's Robodebt and the Netherland's *toeslagenaffaire.*

across OECD countries, the Government Office could learn from instance from some available cases, including:

- **Australia:** Interim guidance for agencies on government use of generative Artificial Intelligence platforms and Australia's Ombudsman Automated Decision-making's Better Practice Guide.
- **Canada:** Directive on Automated Decision-Making and Guide on the use of Generative AI.
- **Denmark:** Guidance for responsible use and development of artificial intelligence - *Use of generative AI in the public sector*
- **United Kingdom**: Guidance to civil servants on use of generative AI - GOV.UK (www.gov.uk)

> Showing quick wins and impact in early stages is needed to secure continuous funding and sustainability of the tool.

18. A revised version of the roadmap, co-created with relevant stakeholders, would also need to include milestones with clear benchmarks and timelines for successful delivery. Being the DDDM tool a digital investment, its governance should be framed in the context of the governance arrangements for digital projects in Estonia. This would imply ensuring that decisions on the future of the DDDM tool are informed by available oversight mechanisms to take stock and decide on the way ahead, including potentially putting on hold further investments on the tool.

Tactical layer

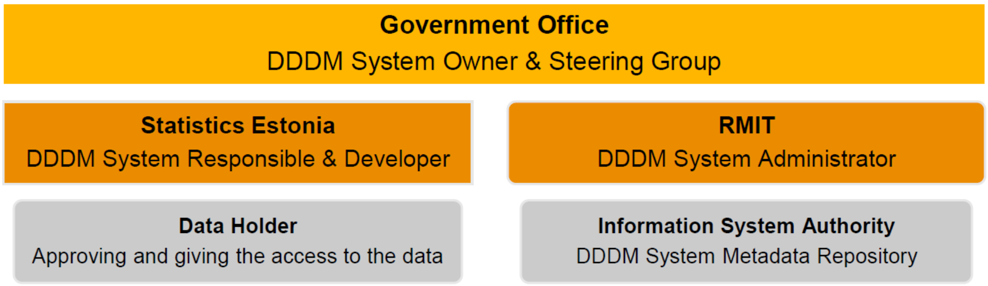
Steering and coordination

19. As described in deliverable 1.4 produced by the external contractor, the current governance of the DDDM tool includes a Steering Group chaired by the Government Office (DDDM's System owner). The Steering Group is integrated by representatives from the Government Office, the Ministry of Economic Affairs and Communications (MKM), Statistics Estonia, and the Data Proteciton Inspectorate. The Steering Group was established as a separate body to ensure coordination on national level without any restrains that may have arised from the agreed focus and modus operandi of the TSI project. At the time of the Project the Steering Group coordinated efforts of represented organisations towards agreeing next steps in DDDM implementation beyond the scope and time-frame of the Project. After the end of the Project the Steering Group has continued and its new focus is implementation of the DDDM roadmap, agreed as one of outputs of the Project.

20. A second governance layer is system-focused and includes also Statistics Estonia and the Information Technology Centre of the Ministry of Finance (RMIT) with key responsibilities in terms of the DDDM tool's development and management. Lastly, a third later (more data-specific) includes the Information System Authority (RIA) (a body within Estonia's MKM) and data holders across public sector bodies.

21. It is worth mentioning that together with Statistics Estonia (as mentioned in previous section), the Information System Autority (RIA) is part of Estonia's National Data Governance Board chaired by the Estonia's Chief Information Officer and the Estonia's Chief Data Officer (roles within MKM).

Figure 4. DDDM's tool governance structure


Government Office
DDDM System Owner & Steering Group
Statistics Estonia
DDDM System Responsible & Developer
RMIT
DDDM System Administrator
Data Holder
Approving and giving the access to the data
Information System Authority
DDDM System Metadata Repository

Source: Deliverable 1.4: To-be situation report. As shown in ginal version delivered by PwC to the Government Office.

> In a later stage, the DDDM governance structure could benefit also from the participation of oversight and auditing bodies and actors, including those from outside the public sector.

22. The participation of the Data Protection Inspectorate in the Steering Group is fundamental to ensure alignment with personal data protection regulations during the design and implementation stages of the DDDM tool. Yet, as the DDDM system evolves, its governance structure could benefit from the participation of other actors in charge of providing independent oversight and monitoring and decisions.

23. Actors such as Supreme Audit Institutions (SAIs) are growinly playing a key role in oversight the use of AI and data in the public sector. For instance, in Norway, the Office of the Auditor General (OAG) is auditing the use of AI in the central government since 2023 as part of its pipeline of new performance audits[2]. Another well-known case is also that of the Netherland's Court of Audit[3].

24. While these examples illustrate the growing role of SAIs in the auditing of algorithms within the public sector, the inclusion of similar bodies in Estonia as part of the governance of the DDDM tool could also help to make better decisions and manage risks on the way forward, secure real-world practice, and get independent advice, oversight and audit.

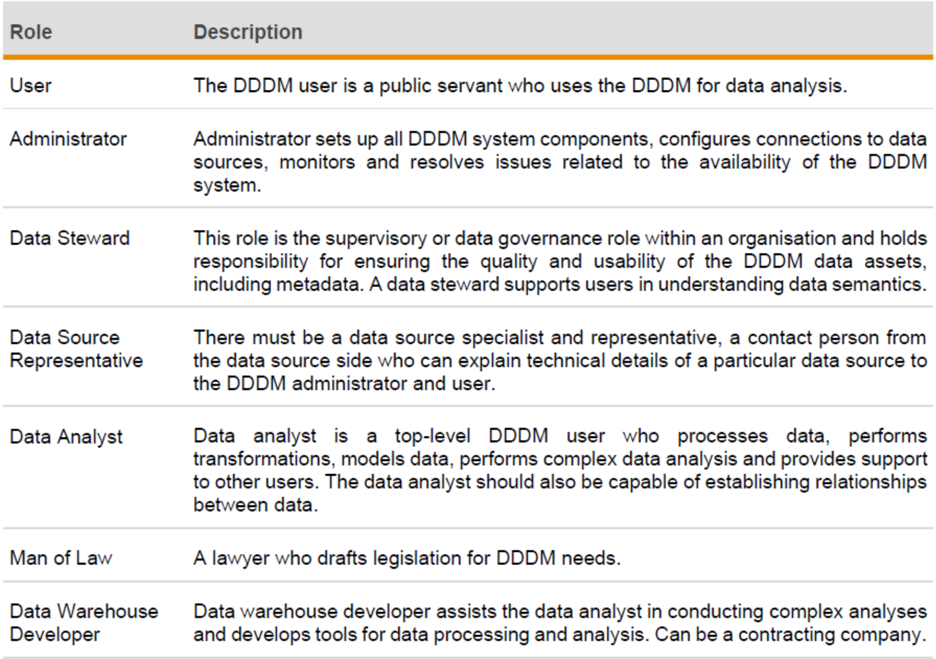
> Securing a solid network of data stewards will play a key role in ensuring coordination and the coherent implementation of decisions taken by DDDM tool's system owners.

25. At the data holder lever (public bodies), the DDDM tool's governance structure has also identified a a set of roles that should be in place across user organisations (Figure 5). These roles range from those relevant for the management of data (system administrator, data analysts, data source representative, data warehouse developer), to those with more tactical responsibilities (data steward, and "*man of law*").

[2] For more information see: Document 2 (2022–2023) (riksrevisjonen.no)

[3] For more information see: https://english.rekenkamer.nl/publications/reports/2021/01/26/understanding-algorithms

Figure 5. DDDM's tool governance structure: Roles



Role	Description
User	The DDDM user is a public servant who uses the DDDM for data analysis.
Administrator	Administrator sets up all DDDM system components, configures connections to data sources, monitors and resolves issues related to the availability of the DDDM system.
Data Steward	This role is the supervisory or data governance role within an organisation and holds responsibility for ensuring the quality and usability of the DDDM data assets, including metadata. A data steward supports users in understanding data semantics.
Data Source Representative	There must be a data source specialist and representative, a contact person from the data source side who can explain technical details of a particular data source to the DDDM administrator and user.
Data Analyst	Data analyst is a top-level DDDM user who processes data, performs transformations, models data, performs complex data analysis and provides support to other users. The data analyst should also be capable of establishing relationships between data.
Man of Law	A lawyer who drafts legislation for DDDM needs.
Data Warehouse Developer	Data warehouse developer assists the data analyst in conducting complex analyses and develops tools for data processing and analysis. Can be a contracting company.

Source: Deliverable 1.4: To-be situation report. As shown in final version delivered by PwC to the Government Office.

26. Data stewards play a key role in ensuring connection between strategic goals and ambitions and the interpretation of those into key actions within responsible public bodies. In this regard, the capacity of the Government Office to establish a network of data stewards across different organisations (in particular, those controlling key datasets relevant for the functioning of the DDDM system) will have a great impact in securing coordination among public bodies.

27. In doing this, the Government Office would benefit from:

- Clearly defining the roles and responsibilities of data stewards, in the context of the DDDM tool, to secure clarity of responsibilities and avoid duplication of tasks with other existing roles.
- Coordinating with the Ministry of Economic Affairs and Communications (MKM) to align these efforts to other initiatives which might have similar objectives to tap on synergies.

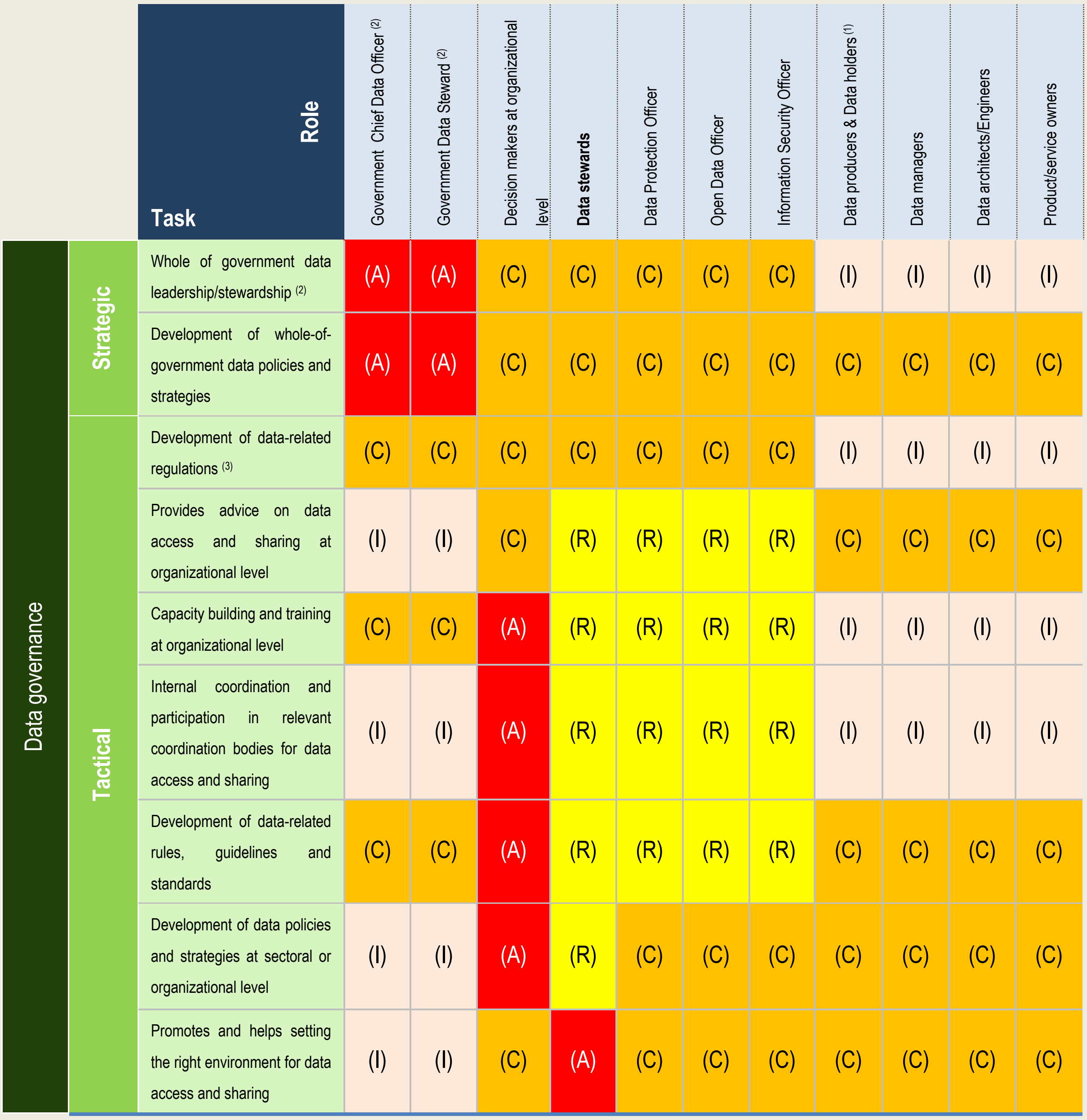
As implementation of the DDDM tool moves forward, roles such as Data Protection Officers will play a key role to ensure trust in the system.

28. Evidence collected during the OECD mission to Tallinn pointed out to the fact that the availability of formal Data Protection Officer positions across public bodies is still under development. Whereas in Esotnia the coordination of data protection efforts seem to greatly rely on social connections built among public officials across different bodies over time, advancing efforts to formalise the availability of these roles (in line with European regulation) would greatly contribute to increase trust in the DDDM system. This, by helping to clarify to whom DDDM system's user or data owners can reack to ask specific questions related to granting access and sharing personal data.

Box .1. Data stewardship in the public sector

29. The OECD has been working with OECD member countries in advancing data steward roles in the public sector. Figure 6 presents a matrix integrating a list of data-related tasks and their distribution/attribution across data-related roles currently in place in most OECD countries. Neither the tasks and roles are comprehensive and therefore may vary in terms of their application, attribution, definition and practice based on national contexts. This description is based on the Responsible, Accountable, Consulted, and Informed (RACI) Model and the OECD model for data governance in the public sector (OECD, 2019[1]). The purpose of this matrix is to further clarify where the Data Steward role at the organisational level fits into the broader data governance ecosystem in the public sector.

Figure 6. Main data-related tasks and roles in the public sector



		Role Task	Government Chief Data Officer (2)	Government Data Steward (2)	Decision makers at organizational level	**Data stewards**	Data Protection Officer	Open Data Officer	Information Security Officer	Data producers & Data holders (1)	Data managers	Data architects/Engineers	Product/service owners
Data governance	Strategic	Whole of government data leadership/stewardship (2)	(A)	(A)	(C)	(C)	(C)	(C)	(C)	(I)	(I)	(I)	(I)
		Development of whole-of-government data policies and strategies	(A)	(A)	(C)	(C)	(C)	(C)	(C)	(C)	(C)	(C)	(C)
	Tactical	Development of data-related regulations (3)	(C)	(C)	(C)	(C)	(C)	(C)	(C)	(I)	(I)	(I)	(I)
		Provides advice on data access and sharing at organizational level	(I)	(I)	(C)	(R)	(R)	(R)	(R)	(C)	(C)	(C)	(C)
		Capacity building and training at organizational level	(C)	(C)	(A)	(R)	(R)	(R)	(R)	(I)	(I)	(I)	(I)
		Internal coordination and participation in relevant coordination bodies for data access and sharing	(I)	(I)	(A)	(R)	(R)	(R)	(R)	(I)	(I)	(I)	(I)
		Development of data-related rules, guidelines and standards	(C)	(C)	(A)	(R)	(R)	(R)	(R)	(C)	(C)	(C)	(C)
		Development of data policies and strategies at sectoral or organizational level	(I)	(I)	(A)	(R)	(C)	(C)	(C)	(C)	(C)	(C)	(C)
		Promotes and helps setting the right environment for data access and sharing	(I)	(I)	(C)	(A)	(C)	(C)	(C)	(C)	(C)	(C)	(C)

		Aligns data access and sharing efforts with policy goals at the organizational, sectoral, national and international level	(I)	(I)	(A)	(R)	(C)	(C)	(C)	(C)	(C)	(C)	(C)
		Ensures data management complies with data governance rules, processes and standards [(4)]	(I)	(I)	(C)	(A)	(A)	(A)	(A)	(R)	(R)	(R)	(R)
		Develops and implement monitoring and evaluation mechanisms for data governance (Data dashboards, data catalogues, audits[5])	(I)	(I)	(C)	(A)	(C)	(C)	(C)	(R)	(R)	(R)	(R)
	Delivery	Data management	(I)	(I)	(I)	(C)	(C)	(C)	(C)	(R)	(R)	(R)	(I)
		(Personal) data protection	(I)	(I)	(C)	(C)	(A)	(C)	(C)	(R)	(R)	(R)	(R)
		Makes **first-hand** decisions on data access and sharing	(I)	(I)	(C)	(C)	(C)	(C)	(C)	(R)	(R)	(C)	(C)
		Opening data up	(I)	(I)	(C)	(C)	(C)	(A)	(C)	(R)	(R)	(R)	(C)
		Digital and data security	(I)	(I)	(C)	(C)	(C)	(C)	(A)	(R)	(R)	(R)	(R)

Note: **(1)** 'Data holders' refer to organisations or individuals who, according to applicable laws or regulations, are competent to decide on granting access to or sharing data under their control, regardless of whether or not such data are managed by that organisation or individual or by an agent on their behalf. Source: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463**;** **(2)** The data leadership task and the roles of CDO or whole whole-of governments data stewards could be attributed to a specific role or a specific body within the public sector; **(3)** Accountability and responsibility would fall into bodies or branches in charge of these tasks e.g. regulators, parliaments, etc. **(4)** Data management, includes creating, collecting, storing, curating, enriching, deleting, providing access to, and sharing data, as well as using data and managing the associated risk. Source: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463 **; (5)** Data audits can take place at a higher level and be performed by organisations such as Supreme Audit Institutions (SAIs) in the context of other exercises, including algorithm accountability mechanisms; **(6)** RACI **(R)** Responsible: In charge of implementing the task, **(A)** Accountable: Ensures the task is performed and finalised, **(C)** Consulted: Participates in decisions relevant to the implementation of the task, **(I)** Informed: Official is aware of the task.

Source: Author. Content under-development. OECD (*forthcoming*), An analysis of National Data Strategies across OECD countries. **Not for public sharing and access**

Hard skills vs. sectoral expertise

Initiatives to support data holders to better manage and prepare the data that will be fed into the DDDM tool can be connected to other on-going initiatives implemented by other bodies (e.g. the National Competence Centre, e-courses). Yet, training on hard-data skills can't replace the need for multi-sectoral expertise on the issue for analysis.

30. The importance of building greater data literacy and hard data skillls (data analysis, preparation, quality) across public bodies is clear for most public officials interviewed during the OECD mission to Tallinn. These needs were already described as part of the roadmap included in Deliverable 1.5 produced by the external contractor. At the same time, providing training on the use of the DDDM itself and safe testing environments will play a key role in increasing use and confidence in the tool as it evolves and matures.

31. However, some procedural factors play an important role henceforth:

- Public officials' skills and ability to understand and make sence the outputs delivered by the DDDM tool and its underlying data. This would be greatly dependent of sectoral expertise on a given topic, but also on the transparency mechanisms in place to get beyond aggregated data.
- Communicating in clear ways that the outputs of the DDDM tool are are only an input in the process of developing the Government Memorandum, but these do no intend to replace sectoral and contextual knowledge and *know-how*.

> It will be fundamental to ensure that the DDDM reflects in its design the need for multi-sectoral expertise, which might be outside the area of knowledge of the direct system user. Different views over a common topic translate into different data needs, sources and holders.

32. By default, public officials involved in the process of developing the Memorandum have already knowledge on their own sector policy issues. The process (as widely described in the deliverables produced by the external contractor) include weekly meetings with the Government Office to discuss on specific topics that need attention, agreements on issues that might require further exploration by analysts and sectoral experts, etc. In this context, views from different Ministries or bodies with a say on one single topic is collected in order to ensure different views and sectoral expertise are brought into the decision making process. This so that the policy issue ca be analysed from different perspectives.

33. Whereas one the goals of the current DDDM tool is to simplify the process of developing a Memorandum, there are critical milestones in this process that should be reflected in the tool itself. For instance, the possibility for different analysts and/or sectoral experts from different ministries to co-create directly on the platform the Memorandum, participate in the data selection process that will inform the outputs of the DDDM tool, or even being notified when a dataset they are responsible for has been selected or requested.

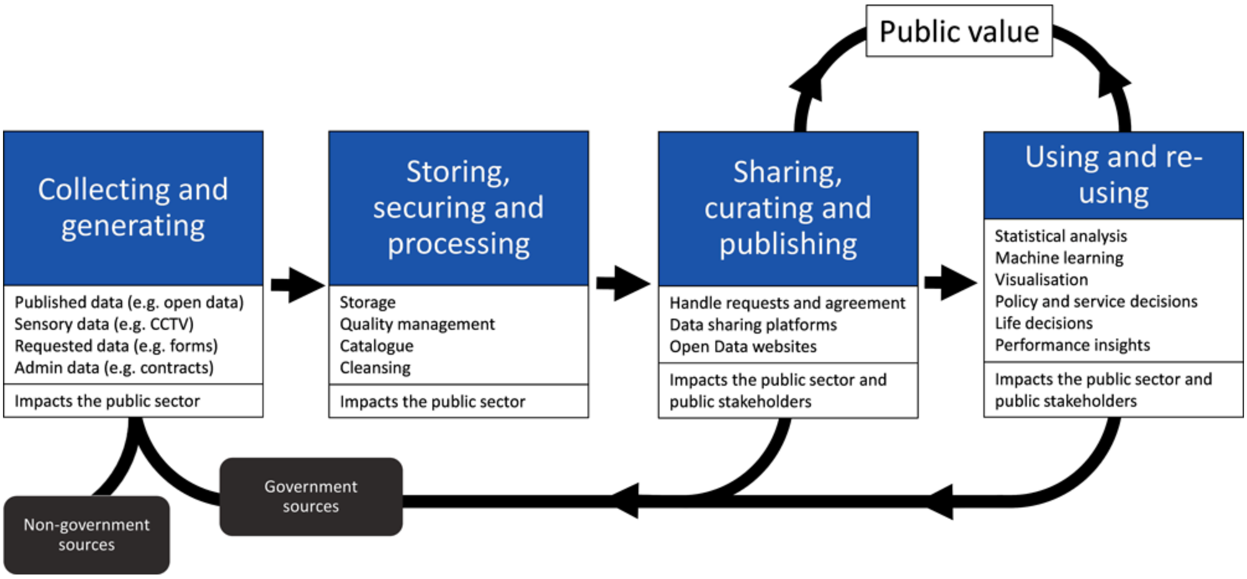
34. Ensuring that that multi-sectoral expertise is always brought in to the decision making process will remain a critical component of the way ahead to help the system deliver comprenhensive and well-informed outputs.

Delivery layer

35. Deliverables 1.5 (Roadmap) and 1.6 (Proof of concept) developed by the external contractor explored in detail technical challenges related to the design of the DDDM tool.

36. In line with the feedback provided by the OECD to these deliverables, and the data value cycle (Figure 6), briefly introduces some of the key challenges that require attention when developing data-intensive systems. Some of these aspects were highlighted by stakeholders during the OECD mission to Tallinn as key issues to be addressed in the context of the DDDM system.

Figure 6. The data value cycle


Public value
Collecting and generating
Published data (e.g. open data)
Sensory data (e.g. CCTV)
Requested data (e.g. forms)
Admin data (e.g. contracts)
Impacts the public sector
Storing, securing and processing
Storage
Quality management
Catalogue
Cleansing
Impacts the public sector
Sharing, curating and publishing
Handle requests and agreement
Data sharing platforms
Open Data websites
Impacts the public sector and public stakeholders
Using and re-using
Statistical analysis
Machine learning
Visualisation
Policy and service decisions
Life decisions
Performance insights
Impacts the public sector and public stakeholders
Non-government sources
Government sources

Source: 2019 OECD Report The Path to Becoming a Data-Driven Public Sector. Available at: https://www.oecd.org/gov/the-path-to-becoming-a-data-driven-public-sector-059814a7-en.htm

Table .1. Relevant technical aspects for data-intensive systems

	Tactical aspect (System owner or else if already available)	Technical aspect (Data holder)	Mainly relevant for:
Data generation	Data quality rules	Common identifiers and semantic standards	Data interoperability
	Data quality rules	Data classifications	Data interoperability
	Data quality rules	Metadata	Data understandibility
	Data quality assurance	*n.a.*	Data reliability
Data access and collection	*n.a.*	Data catalogues	Data discoverability
	n.a.		
Data storing	*n.a.*	Federated data warehouses	Data accesibility
Data sharing	Data access and sharing agreements	*n.a.*	Data accesibility
	Open data standards	Open data	Data accesibility
Data use and re-use	Data visualisations	*n.a.*	Data understandibility
	n.a.	Data dissagregation, granularity, and microdata	Data understandability, data auditing
	Data provenance rules	*n.a.*	Data traceability, data audting
	n.a.	Transparency of data sources	Data traceability, data audting
	n.a.	Data records	Data traceability, data auditing

Source: Author. Content under-development. OECD (*forthcoming*), An analysis of National Data Strategies across OECD countries. **Not for public sharing and access**

Outcomes 2 and 3: Risk mapping and disaster loss data management

37. This section compiles key OECD observations and recommendations to support the implementation of the risk assessment methods and tools in Estonia. These are based on the data and insights collected by the OECD during the meetings organised with key stakeholders from the public sector in the context of the OECD mission to Tallinn, Estonia that took place on 21 – 22 February, 2023; as well as discussions held during the follow-up mission on 8-10 November 2023.

38. The next steps for risk mapping and disaster loss data management presented in the following sub-sections are based on the OECD work on the principles contained in the Recommendation on the Governance of Critical Risks [OECD/LEGAL/0405] and the wider work of the OECD on risk assessment and disaster losses.

39. The Recommendation on the Governance of Critical Risks was adopted by the governing body of the OECD, the Council, in May 2014. The High-Level Risk Forum (HLRF) was instrumental in the development of this Recommendation. Since its adoption, 41 countries have signed up to the Recommendation, including Estonia as a member country of the OECD.

40. The Recommendation proposes that Adherents build preparedness through foresight analysis, risk assessments and financing frameworks, to better anticipate complex and wide-ranging impacts of critical risks.

41. The Recommendation calls on Adherents to:

- identify and assess all risks of national significance and use this analysis to inform decision making on risk management priorities,
- use the best available evidence to understand the potential likelihood, plausibility and impacts of risks the country is exposed to and set aside the necessary resources for addressing them,
- regularly revise their national risk assessment,
- analyse the drivers behind exposures, vulnerabilities and hazardous activities,
- develop location-based inventories of exposed populations and assets, as well as coping capacities (including protective infrastructure), and
- consider linked risks and cascading effects.

Suggested next steps for improving the assessment and management of critical risks

> *The Recommendation on the Governance of Critical Risks defines **critical risks** as those "threats and hazards that pose the most strategically significant risk, as a result of (i) their probability or likelihood and of (ii) the national significance of their disruptive consequences."*
>
> *Includes sudden onset events (like earthquakes, industrial accidents or terrorist attacks); gradual onset events (like pandemics) or steady-state risks (like those related to illicit trade or organised crime).*

42. The focus of the risk assessment component of the project has been on improving the way local municipalities understand the critical risks they face and the expectations placed upon them for their management. The important role local municipalities could play in both risk assessment and risk management in Estonia is only partially described in the current Emergency Act of 2017, as amended in 2023 (Riigikogu (Parliament of Estonia), 2017[3]). According to the act, every local municipality must establish a crisis management committee but but there is no obligation to assess the risks, communicate about the risks to those exposed to them, and engage with vital service providers is not detailed in the act.

43. As described in deliverable 3.1, most municipalities, including larger ones, lack a systematic review of their risk environment, focusing primarily on risks that may disrupt vital services rather than adopting an all-hazards approach.

44. It is expected that upcoming legislation will introduce a series of reforms that explicitly require local municipalities to conduct risk analysis, ensure all municipalities are recognised as vital services providers and clarify their responsibilities for guaranteeing the continuity of essential services during emergencies.

45. In order to make the best use of the methodology for risk assessment at the level of local municipalities, in line with the duties likely to be introduced as part of the upcoming legislation, it is key to ensure there is a connection between the increased risk awareness that is derived from engaging in a risk assessment process and the measures needed for improving the local preparedness.

46. Analysing the risks is the first step in the quest for comprehensive preparedness. This necessitates a cultural shift, where risk awareness is not perceived as an endpoint but as the initiation of a continuous cycle of refinement and adaptation.

Challenge the assumption that increased understanding of potential impacts automatically leads to better preparedness.

47. For example, in the **United Kingdom**, the Cabinet Office worked with the Department for Levelling Up, Housing and Communities (as well as range of government departments, agencies, professional institutions, and local emergency responders) to develop a set of National Resilience Standards for Local Resilience Forums (LRFs) (Cabinet Office, 2020[4]). These standards do not impose new duties but aim to articulate expectations of good and leading practices for LRFs, building on existing statutory duties under the existing legislation.

48. The purpose of these standards is to establish a consistent and progressive framework for LRFs to self-assess their capabilities and readiness. They guide continuous improvement against mandatory requirements, good practices, and leading practices.

49. The standards contain five sections:

- **Desired Outcome:** Defines what the LRF should be working to achieve.
- **Summary of Legal Duties:** Provides a summary of legal duties or requirements under relevant legislation.

- **How to Achieve Good Practice:** Details normative statements outlining how LRFs should meet legal requirements and expectations in a thorough and effective manner.
- **How to Achieve Leading Practice:** Highlights indicative statements describing innovative approaches that yield superior results, emphasizing efficiency and interoperability with multi-agency partners.
- **Guidance and Supporting Documentation:** Offers links to further sources of guidance and support, categorized by statutory and overarching multi-agency guidance, thematic multi-agency guidance, single-agency guidance, competence statements, standards specifications, and more.

50. The standards are designed to be used in two ways:

- **Guide for Continuous Improvement:** Focuses on what is important and effective, identifying practices recognized as good and leading. It serves as a guide for LRFs to enhance their capabilities continually.
- **Yardstick for Assessment and Assurance:** Provides a consistent means for LRFs to assess their capabilities through self-assessment, peer review, or other forms of scrutiny. It helps organizations understand their strengths and areas for development.

51. Overall, the standards aim to enable LRFs to make informed judgments about their overall readiness for handling emergencies identified in local risk assessments; while allowing flexibility for adaptation based on local needs and principles of subsidiarity and local accountability.

52. Local Resilience Forums (LRFs) in the **United Kingdom**, are a partnership formed between a range of agencies representating local public services, including the emergency services, local authorities, the health service, the Environment Agency and others.

53. LRFs group local actors at the International Territorial Levels (ITL) 2 which is roughly equivalent to the Regions in Estonia’s administrative geograpies.

54. Grouping local authorities and other relevant actors at this regional level facilitates coordination across administrative areas and enables the pooling of resources for conducting risk assessments and identifying mitigations / preparedness measures required.

> Explore and encourage coordination at the regional level for crisis management, drawing inspiration from Safety Regions in the Netherlands, Civil Preparedness Regions in Sweden and Local Resilience Forums in the United Kingdom.

55. Drawing inspiration from successful models like the Safety Regions in the **Netherlands**, Civil Preparedness Regions in **Sweden**, and Local Resilience Forums in the **United Kingdom**, Estonia could actively facilitate regional coordination for effective crisis management. The vision is to transcend municipal boundaries and foster collaborative efforts. Examples of this practice comes from **Sweden**, where the Civil Preparedness Regions enable municipalities to share expertise, resources, and strategies. This coordinated regional approach ensures a unified response, drawing strength from collective capabilities. In **Sweden**, civil preparedness activities have been traditionally organised at the level of county administrative boards, but in October 2022 a reform of the national civil preparedness system led to the establishment of “higher regional levels”. These were established by dividing the country's 21 county administrative boards into six civil preparedness areas. Each area includes between two and seven county administrative boards. For each area, a responsible county administrative board is appointed where the county governor will be called the civil area manager. (Swedish Ministry of Defense, 2022[5])

56. In the **Netherlands**, Safety Regions are organised as a public body tasked with responsibilities such as risk identification, advising authorities, crisis preparation, and managing emergency services. The management of the safety region is overseen by mayors, and a chairman is appointed through Royal Decree. Meetings may involve the chief public prosecutor, water board chairman, and the King's Commissioner. Periodic policy and crisis plans are developed, incorporating risk profiles. Disaster management plans are established for specific categories through government orders, and regulations may cover various aspects, including fire brigade operations and disaster response. Cooperation agreements are forged with the police and public prosecutor, with a specific agreement for Royal Military Police duties. (Kingdom of the Netherlands, 2010[6])

57. Pairing regional arrangements with a harmonised approach to risk assessments at the local level is a cornerstone of effective risk governance. Advocating for a minimum common methodology serves to standardize efforts across the country, fostering consistency and comparability across municipalities.

Emphasize the benefits of a minimum common methodology for risk assessments at the local level

58. For example, in **Sweden**, counties and municipalities have a legal obligation to conduct specific risk and vulnerability analyses for their areas of responsibility (Swedish Minstry of Defense, 2006[7]). In **Switzerland,** the Federal Office of Civil Protection coordinates a national risk assessment process that involves cantonal and municipal authorities. (Federal Office for Civil Protection FOCP, 2020[8]) and has developed a framework (named KATAPLAN) designed to facilitate practical intercantonal planning for prevention of and coping with catastrophes and emergencies. This framework is predicated on an integrated procedure for identifying hazards and the resulting risks, which is common for all cantons. (Federal Office of Civil Protection, 2013[9])

59. However, detailed guidance on a common approach to disaster risk assessment at the sub-national level requires a minimum level of funding in order to ensure municipalities have the resources available to to perform their risk assessment duties.

Clarify funding for risk assessment and for leveraging results of assessment

60. In **Colombia**, the law that establishes the National Disaster Risk Management System (Congress of the Republic of Colombia, 2012[10]) outlines, in its Article 7, one of the necessary conditions for achieving the overall objective of the System: the adequate financing of the disaster risk knowledge and the disaster risk reduction processes. The risk knowledge process encompasses risk assessment, evaluation, as well as related research, communication, and education activities. The risk reduction process covers the use of the risk knowledge acquired to address the drivers, exposures and vulnerabilities linked to the risks, thus mitigating their impacts.

61. Financing mechanisms at the municipal level, in the Colombian context, follow a long established strategy that includes the creation and running of Municipal Risk Management Funds. The National Disaster Risk Management Unit of Colombia has produced specific guidance tailored to the needs of a hugely diverse set of local municipalities (ranging from remote small rural municipalities to large urban government). (National Disaster Risk Management Unit of Colombia, 2014[11])

62. This approach underscores the importance of sustained financial support, ensuring that municipalities can not only conduct thorough risk assessments but also implement strategic interventions based on the outcomes of such assessments, thereby stengthening their long-term resilience.

However, the impacts of risks are not felt in equal measure by all across society. For example, whilst the impacts of the COVID-19 pandemic on public health, employment and education outcomes have been felt by all, it has been those most vulnerable in society who have felt them most acutely (OECD, 2022[12]). The impacts of COVID-19 revealed more clearly how income inequalities accentuate vulnerabilities and exposures, shaping remarkably different outcomes for vulnerable groups in populations (Bollyky et al., 2022[13]).

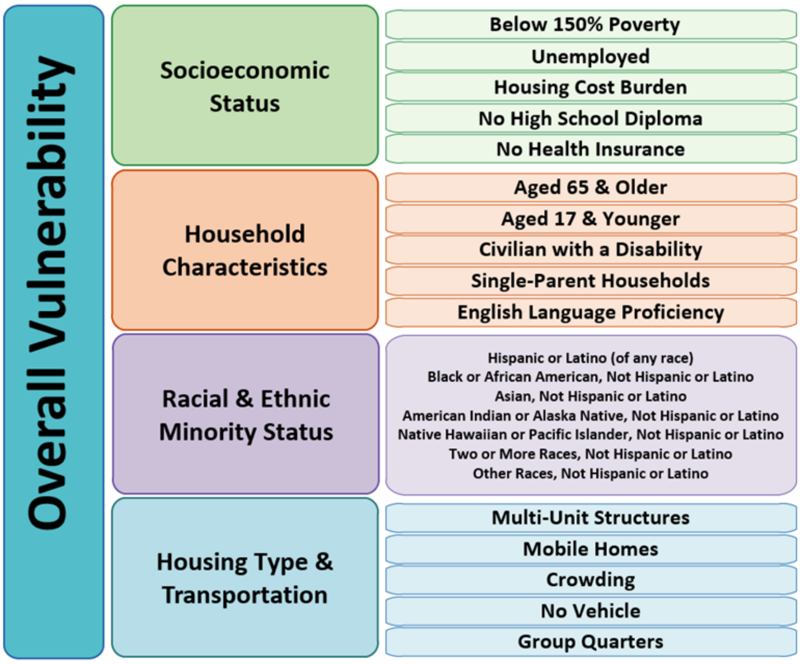
> Consider overall vulnerabilities in the wider population, such as levels of deprivation and health inequalities:

63. Social vulnerability is a common denominator that governs the impacts of both disasters and climate change on a place. It not only determines the local sensitivity and coping capacity to extreme events, it also influences public participation and the coping capacity of specific section of the local population when faced with disaster events.

64. Considering social vulnerabilities including socioeconomic disparities, health inequalities, and levels of deprivation within the population must be integral components of risk assessment, in particular at the local level.

65. For example, in the **United States**, the Centers for Disease Control and the Agency for Toxic Substances and Disease Registry have created a composite index known as the Social Vulnerability Index (SVI). The SVI is used for helping public health officials and emergency response planners identify and map the communities that will most likely need support before, during, and after a disaster.

Variables used in the social vulnerability index



Overall Vulnerability	Socioeconomic Status	Below 150% Poverty Unemployed Housing Cost Burden No High School Diploma No Health Insurance
	Household Characteristics	Aged 65 & Older Aged 17 & Younger Civilian with a Disability Single-Parent Households English Language Proficiency
	Racial & Ethnic Minority Status	Hispanic or Latino (of any race) Black or African American, Not Hispanic or Latino Asian, Not Hispanic or Latino American Indian or Alaska Native, Not Hispanic or Latino Native Hawaiian or Pacific Islander, Not Hispanic or Latino Two or More Races, Not Hispanic or Latino Other Races, Not Hispanic or Latino
	Housing Type & Transportation	Multi-Unit Structures Mobile Homes Crowding No Vehicle Group Quarters

Source: CDC SVI Documentation 2020, https://www.atsdr.cdc.gov/placeandhealth/svi/documentation/SVI_documentation_2020.html

66. Beyond its comprehensive rankings, SVI serves as a crucial tool for enhancing community preparedness. It aids in emergency preparedness planning by assessing community needs, estimating

required supplies, determining the necessary personnel for assistance, and identifying areas in need of emergency shelters. SVI also plays a pivotal role in developing evacuation plans that account for individuals with special needs, such as those without vehicles, the elderly, or individuals with limited English proficiency. Moreover, it helps identify communities that will require sustained support for recovery following emergencies or natural disasters.

Suggested next steps for improving disaster loss data management

67. The OECD Recommendations on the Governance of Critical Risks and on Disaster Risk Financing Strategies provide guidelines for member countries to enhance their governance and financial strategies in addressing critical risks and disasters.

68. The Recommendation of the Council on the Governance of Critical Risks calls for adherents to:

- Plan for contingent liabilities: Countries should develop plans for contingent liabilities, preparing for potential financial losses or obligations that may arise due to unforeseen events or risks.
- Take into account the distribution of potential losses among households, businesses, and insurers: When planning for contingent liabilities, member countries should consider how potential losses may be distributed among different stakeholders.
- Estimate, account and disclose contingent liabilities associated with losses to critical sectors in the context of national budgets; assess risk-related expenditures, at national and local level: The recommendation emphasizes estimating, accounting for, and disclosing contingent liabilities related to losses in critical sectors within the framework of national budgets.

69. Additionally, countries are encouraged to assess expenditures related to managing risks at both national and local levels.

70. The Recommendation of the Council on Disaster Risk Financing Strategies calls for adherents to:

- Estimate exposures and identify financial vulnerabilities: Countries are advised to assess and estimate their exposures to potential disasters while identifying financial vulnerabilities that may arise as a result.
- Produce, collect, share and make publicly available data on past losses: Member countries are encouraged to generate, gather, share, and publicly release data on previous losses resulting from disasters to enhance transparency and enable better-informed decision-making.
- Complete post-disaster loss assessments for significant events, based on a consistent methodology and co-ordinated with the private sector; harmonise the collection and reporting of data nationally, regionally and internationally: Countries are urged to conduct comprehensive assessments of losses following significant disasters using a consistent methodology and coordinate with the private sector.
- Additionally, there is a call for harmonization of data collection and reporting at the national, regional, and international levels to facilitate effective risk management and response coordination.

71. These recommendations provide a framework for Members to strengthen their governance structures and financial strategies in dealing with critical risks and disasters, emphasizing planning, transparency, data sharing, and coordination.

72. The following suggested next steps for disaster loss datasets in Estonia seek to complement the ones suggested for risk assessments, but will require active implementation of a national system for disaster loss accounting in the country:

- Emphasise the need for clear steady-state comparisons in data categories for losses data (also useful for crisis management).

- Address missing information on event intensity, suggesting the work of the Austrian meteorological service as a reference.
- Further explore and address data protection issues related to legal constraints.
- Follow transparency principles when publishing risk information.
- Specify the frequency and updating cycle for disaster losses databases in the national disaster loss management system.
- Consider further ways for municipalities to feed into the national disaster loss dataset and design incentives for them to do so.
- Estimate exposures of public finances to scenarios in the assessment and identify financial vulnerabilities.
- Ensure losses from public sector (including both direct spend on response and recovery) are included in the losses database.
- Complete post-disaster loss assessments for significant historical events, based on a consistent methodology and co-ordinated with the private sector.
- Use loss assessment of significant historical events to test the data structure of the disaster loss database and the impact assessment criteria for risk assessments (at both national and local level).

Visit our website:

Find out more
about the Technical
Support Instrument:

Funded by
the European Union