EFDI. EUROPEAN FORUM OF DEPOSIT INSURERS

Ensuring Stability: A Roadmap to Robust Risk Management in Deposit Guarantee Schemes

Proposed non-binding guidelines by the European Forum of Deposit Insurers (EFDI) Risk Management Working Group

This publication is available on the EFDI website (www.efdi.eu).

European Forum of Deposit Insurers (EFDI), Rue de la Presse 4, 1000, Brussels (Belgium) Belgium 1000, Registration Number: BCE 0892.945.871. Email secretariat@efdi.eu/ Tel: +34 605 790 858

EFDI. EUROPEAN FORUM OF DEPOSIT INSURERS

TABLE OF CONTENTS

Introduction

The management of risks on a macro level is widely acknowledged as a crucial aspect of organisational strategy. However, within the intricate financial landscape, the importance of establishing a robust risk management framework at the micro level, particularly within deposit guarantee schemes (DGSs), cannot be overstated. DGSs play a pivotal role in safeguarding depositor interests and maintaining financial stability, making the development of an effective risk management framework vital to a smooth operation.

It is necessary to recognise the inherent diversity among European DGSs, stemming from variations in legal structures, operational frameworks, and the systemic contexts of the environment. Consequently, the risk management systems implemented by these schemes exhibit notable disparities. This diversity underscores the need for tailored approaches to risk management within the realm of DGS operations. The working group has set up a roadmap with milestones covering the pillars of the risk management as set by the COSO framework. As we move forward, we will conduct in-depth analyses of governance and culture, strategic objectives, performance measurement, review and revision processes, and, nonetheless, the flow of information, communication, and reporting mechanisms. Given the diverse character of our community, in this paper we put more emphasis on the ISO standards because they offer more detailed guidelines and cater to a broader, global audience.

Against this backdrop, the primary objective of this paper is twofold. Firstly, it aims to delineate the foundational principles of risk management specifically tailored to DGSs. By doing so, it seeks to provide a comprehensive understanding of the unique risk landscape encountered by DGSs and the strategies best suited to mitigate associated risks effectively.

Secondly, this paper endeavours to offer a high-level overview of what constitutes a robust risk management framework within the context of DGS operations. It seeks to identify and analyse the key components essential for an effective risk management framework, thereby providing DGS stakeholders with valuable insights into best practices and guiding principles.

By setting forth these objectives, this paper endeavours to contribute to the advancement of risk management practices within DGSs, ultimately fostering depositor confidence, financial stability, and the integrity of the banking system.

1. The importance of risk management for a deposit guarantee scheme

Risk management is a pivotal element in the framework of a deposit guarantee scheme. The overall (risk management) framework contributes to the achievement and fulfilment of the missions of the DGS and to an efficient and coherent risk management ensuring stability and confidence in the financial sector.

Effective risk management is everyone’s duty. It enables the identification, assessment, and prioritisation of risks that could cause a scheme’s failure to fulfil its purpose or have a detrimental impact on effectiveness. By understanding these risks, the scheme can devise strategies to mitigate them.

Robust risk management practices support the financial sustainability of the scheme and its ability to protect depositors which in turn aids the stability of the banking system and contributes to broader financial and economic stability.

It is beneficial to approach risk in an organised manner and the ISO 31000 standard sets out some useful principles:

1. **Integrated**
   Ensure that risk management becomes cultural and a consideration of all your scheme's activities.

2. **Structured and comprehensive**
   Be well-organised with segregation of duties and thorough documentation of all known risks. With suitable oversight, ensure risks are assigned, so that decision makers are aware of their authority and restrictions.

3. **Customised**
   Your risk management framework and process should be tailored to your scheme acknowledging the need for proportionality due to resource limitations.

4. **Inclusive**
   Where appropriate, involve stakeholders in the risk management process. Stakeholders are any person, group of people or organisations that can impact or be impacted by your decisions or activities. By involving them, you can gain from their knowledge, views and perceptions.

5. **Dynamic**
   Change is constant. Therefore your approach to risk management needs to be regularly challenged and re-examined with a process for trigger events to result in reassessment of risks. Some risks might only become apparent after a default.

6. **Best available information**
   Good quality, up to date information will enhance the quality of the risk management framework. Understanding the data's limitations and uncertainties about accuracy is also important.

7. **Human and cultural factors**
   Human behaviours and scheme culture and capabilities can have an impact so recognise this in the framework.

8. **Continual improvement**
   Through experience, and over time, your approach to risk management can continually improve.

When any organisation adopts a new risk management policy or framework, it is crucial to understand that while eliminating all risks is impossible, they do have the control over certain elements and risks they are willing to take. While some risks are indispensable for achieving organisational goals, others could result in severe repercussions. In the realm of organisational decision-making concerning risk management, the principles of 'risk appetite' and 'risk tolerance' hold considerable importance.

Risk appetite is described as "**the amount of risk that an organisation is willing to**

accept to achieve its objectives." Through this definition, risk appetite introduces a concept that elaborates the following: risk can impact one's success and so can risk aversion. The world is full of risk, and organisations must determine what risk to accept to achieve its objectives and what risk requires further actions to **avoid, mitigate, transfer or accept.** On a positive note, risks can have a favourable effect, therefore the strategy can focus on exploiting, enhancing, or sharing it. This is a key task: evaluating which risks fit within the organisation's risk appetite and which risks require additional controls in place to reduce the residual risk to an acceptable level.
Generally, a **risk appetite statement** is approved by the board of directors and documents the organisation's risk attitude and its willingness to accept risk in specific scenarios, with a governance model in place for risk oversight (e.g., monitor if unacceptable risks are being pursued). Risk varies among organisations, and accordingly, each organisation has its own risk appetite that reflects its internal and external context.
Typically**, risk tolerance** is communicated in quantitative terms. Conceptually, risk tolerance sets the boundaries of risk taking that the organisation will not go beyond in pursuit of its long-term objectives. To support boundary setting, measures such as key risk indicators are used to align with risk tolerance limits, ensuring that the organisation remains within its risk tolerance bracket and on track to achieve its objectives.

1.1. Risk taxonomy

Rooted from two Greek words *taxis* (i.e. arrangement, division) and *nomos* (i.e. law), Taxonomy is the science of classification according to a predetermined system.

This classification system can be applied to the risk identification and should help obtain a structured and harmonised framework across DGSs. The DGS risk taxonomy is provided in Annex 1.

Also, using risk taxonomy principles will create a link between all the risk management components allowing a better risk identification, mitigation actions as well as an efficient reporting and governance.

2. Most common risks a DGS should consider

According to the International Association of Deposit Insurers (IADI), mandates are established to formally delineate the roles and responsibilities of DGSs. Within the domain of deposit insurers' mandates, differentiation typically occurs across four primary categories. However, achieving precise demarcation among these categories proves challenging due to the necessity of considering jurisdiction-specific circumstances. Consequently, a spectrum of combinations emerges, transcending the delineated boundaries.

While implementing a new function in a DGS, the mandate, and the complexity of the DGS's activity shall be taken into consideration. Meaning that a paybox having the responsibility of the reimbursement will have a humbler risk management framework compared to a risk minimiser, which in some cases may have prudential oversight responsibilities and sophisticated functions.

The primary objective of a DGS resides in fortifying the financial system, thereby prioritising its robust functioning, particularly during periods of economic distress. To

fulfil its purpose of timely and correct compensation, there are five particularly important aspects to be considered.

1. **Single Customer View (SCV) file data quality:** Foremost among the considerations for DGSs is the integrity of the data utilised during payout processes. It is imperative that the SCV files maintain a standard of impeccability. Consequently, during tranquil economic periods, DGSs are tasked with conducting rigorous testing to verify the comprehensive coverage of insured deposits within SCV files. This entails ensuring the absence of discrepancies, ascertaining the absence of missing entries, and validating the overall quality of the data. Prevalent risks faced by a DGS predominantly manifest as operational in nature and necessitate explicit acknowledgment, namely that **the SCV file containing important compensation-related data is faulty, leading to delays, absent, or poor-quality data in critical reports and analysis.**
2. **Financial risk (funding issues):** The operational mandate of a DGS necessitates proficient financing capabilities to facilitate compensation processes. Market fluctuations, even ones stemming from the degradation of the creditworthiness of an institution, can have a significant (negative) impact on the DGS's portfolio value. Consequently, proactive measures to anticipate unfavourable market movements and mitigate potential inadequacies in portfolio valuation are indispensable. Essential to this endeavour is the establishment of **alternative funding mechanisms** in compliance with the national law to supplement potential shortfalls in liquidity or fund size, highlighting the critical importance of accurate portfolio valuation methodologies.
3. **ICT risks:** The sound operation of a DGS relies on the resilience and integrity of its IT infrastructure. From an operational perspective, the availability of the IT systems bears with high importance, especially if the compensation process is diverted to online platforms. The omnipresence of cyber risk across various sectors necessitates heightened vigilance within DGS operations, as they are no exception to such threats.
4. **Reputational risk:** A DGS's immaculate reputation plays a pivotal role in bolstering depositor confidence within the financial system. False information or poorly worded corporate announcements about the DGS or the compensation can damage the reputation and can even exacerbate market distress through bank runs.
5. **Third party risk:** The DGS must have good professional relationships with its partner institutions, the liquidator, entities engaged to outsourced activities and other service providers, including those providing critical IT support. Such collaborative partnerships are indispensable for ensuring the seamless execution of DGS operations and safeguarding depositor interests. By thoroughly monitoring and rating third parties a DGS can mitigate third party risks. Preparing for the exit of a partner with alternative ones can ease the risks stemming from their failure.

DGSs confront a multitude of risks that necessitate prudent consideration to ensure the efficacy of their operations. These risks, albeit varied, encompass factors as mentioned above. However, the approach to risk management undertaken by DGSs is not uniform and it does not necessarily have to be, as it is tempered by the **principle of proportionality**. Under this principle, DGSs possess the discretion to calibrate the extent and depth of their risk mitigation strategies in accordance with the scale and complexity of their operations, as well as the prevailing regulatory framework. This approach allows DGSs to tailor their risk management practices aligning with their specific operational contexts while simultaneously ensuring the preservation of

depositor confidence and the stability of the financial system at large.

3. Risk assessment process

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. The way this process is applied is dependent not only on the context of the risk management process but also on the methods and techniques used to carry out the risk assessment.

3.1. Risk identification

Risk identification is the process of finding, recognising, and recording risks. The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organisation.

The risk identification process includes identifying the causes and source of the risk events, situations or circumstances which could have a material impact upon objectives and the nature of that impact. Risk identification tools are widely available. Within this array, DGSs can exercise discretion in selecting the most apt tool aligned with their organisational mission and can judiciously apply the principle of proportionality to tailor the chosen approach to the scale and scope of their operations. DGSs are afforded the flexibility to choose between simpler tools like facilitated brainstorming, or more intricate methodologies such as morphological analysis. Guidance on the implementation of these identification processes is provided in Annex 2.

Furthermore, intermediate to advanced methods such as Bow Tie or Ishikawa analysis can offer valuable insights, contingent upon the requisite level of granularity or analytical depth sought. Alternatively, DGSs may adopt a perspective aligned with the ISO 31010 standard, affording them the flexibility to either singularly select an analytical framework or amalgamate two or more methodologies, guided by the procedural delineations outlined in pertinent guidelines.

Additionally, DGSs must recognise and evaluate risks, regardless of whether they originate from factors within their control or external to their sphere of influence. Once a risk is identified, the organisation should identify any existing controls such as design features, people, processes, and systems.

3.2. Risk analysis

The purpose of risk analysis is to understand the nature of the risk, its characteristics and to assign a corresponding level of significance to each identified risk and it serves as a critical point for decision-making regarding risk treatment and for setting the organisation's risk appetite.

Key considerations in risk analysis encompass, but are not limited to:

- likelihood of the events and their consequences;
- qualitative and quantitative dimensions of these consequences;
- complexity and connectivity;
- time dimension and the ever-changing character;
- effectiveness of implemented controls;
- sensitivity level;

- internal and external influences.

A single risk event can have several consequences, some positive, some negative, some uncertain, depending on the strategies employed for risk mitigation.

Risk analysis provides valuable inputs for risk evaluation. This analysis provides the necessary understanding in order to decide whether to treat a risk and how to treat it. Meanwhile, risk analysis supports decision-making when different types and levels of risk are involved.

It is essential to acknowledge the **subjective nature of risk perception**. While stakeholder engagement remains paramount throughout risk management strategy development, measures must be in place to mitigate bias. Differing perceptions of risk severity and likelihood underscore the need for a standardised approach to risk measurement within the organisation, ultimately shaping the framework for risk assessment and analysis.

Risk analysis techniques can be quantitative, qualitative or a combination, depending on each DGS's circumstances and scope. It should be performed according to the risk criteria established by the person performing the analysis, controlled by the risk manager. Depending on the type of risk, purpose of the analysis, information and resources available, DGSs can undertake risk analysis in different degrees of detail – basic, intermediate or advanced. A comprehensive overview of the possible analysis tool is available in Annex 3.

3.3. Risk evaluation

Risk evaluation's role is to support decision-making. Risk evaluation involves comparing established risk criteria with findings from the risk analysis to assess:

- the effectiveness of criteria definition;
- identification of highest-priority risks;
- determination of the approach for subsequent risk treatment;
- evaluation of the success of the risk analysis process and identification of any remaining knowledge gaps.

Following risk evaluation, various courses of action may ensue, including further analysis, maintenance of existing controls, or realignment of risk strategy objectives to align with organisational goals. Therefore, it is important to define the scope: the decisions or actions should support the desired output.
Risk evaluation consists in benchmarking the result of the risk analysis against the agreed risk criteria to determine whether supplementary action is needed.

Regular evaluation fosters the development of a robust risk management strategy, enabling timely adaptation to change in risk factors, impact, consequences, and organisational objectives. The results at this stage may vary from "no action needed", "examine the options available", "more in-depth analysis" or even to "reassess the objectives".

A DGS may choose qualitative approaches that can use descriptive (e.g. "once per year/monthly/daily/never") or hierarchic (e.g. high/medium/low) scales to measure impact and likelihood/probability.

Combined approach uses a descriptive or hierarchical scale for one/some parameter(s)

(e.g. likelihood/probability, persistency etc.) and a numerical scale for the other(s) (e.g. impact, outcome). It needs to be mentioned that this method requires validation, detailed instructions, and rigorous application to produce the desired results.

Qualitative and combined approaches can only be used to compare risks measured in the same manner, using the same criteria and expressed in the same terms. Another drawback of these approaches is that they are difficult to use when the impact/outcome can be positive as well as negative.

The most used assessment tool is the risk matrix, or heat maps. The **risk matrix** serves as a visual tool for evaluating risks by considering the interaction of multiple factors, typically encompassing impact or outcome alongside likelihood or probability. These factors can be delineated with as much granularity as deemed necessary, and they can encompass both positive and negative consequences. Similarly, a **heat map** employs a similar approach by integrating two or more factors to depict both favourable and adverse outcomes, utilizing scales that can be as detailed as required. However, in contrast to the risk matrix, a heat map assigns specific risk values to individual cells within the matrix, rather than categorizing them into predefined "zones."

Table 1: Example of risk matrix and heat map

Impact				
	3	medium	medium	High
	2	low	medium	medium
	1	low	low	medium
		1	2	3
		Probability		

Impact				
	3	6 - "Black swan"	7 - Medium-high	9 - High
	2	2 - Low	5 - Medium - low	8 - Medium-high
	1	1 - "No action"	3 - Low	4 - Medium - low
		low	medium	high
		Probability		

Each cell within the risk matrix can be correlated with distinct risk management strategies. In the context of adverse outcomes, Cell No. 3, denoting "Low" risk, may necessitate the augmentation of control measures aimed at mitigating the likelihood of minor losses. Such losses, though individually inconsequential, possess the potential to accumulate into a substantial sum over time. Conversely, Cell No. 6, representing "Black Swan" events, underscores the imperative for a robust Business Continuity Plan (BCP) to fortify the resilience of the DGS, enabling it to endure and recuperate in the aftermath of such extraordinary occurrences.

3.4. Risk documentation

Documenting risks is crucial due to its multifaceted utility within organisational risk management frameworks. Primarily, it provides a comprehensive record of identified risks, their potential impacts, and the strategies proposed for their management, thereby fostering transparency, and boosting accountability across organisational hierarchies. Moreover, documentation serves as a reference point for future risk assessments, allowing for the tracking of risk trends over time and facilitating informed decision-making processes. Additionally, it aids in communication and knowledge sharing among stakeholders, fostering a shared understanding of the organisation's risk landscape, and promoting effective risk management practices across departments.

The risk registry serves as a central repository for cataloguing and managing identified risks within an organisation. It provides a structured framework for recording pertinent details about each risk, including its nature, potential impact, likelihood of occurrence, and mitigation strategies. By maintaining a comprehensive risk registry, organisations can systematically track and monitor their risk profile, enabling proactive

risk management and informed decision-making processes.

To facilitate the documentation process, various tools are available, ranging from simple spreadsheets and databases to more sophisticated risk management software platforms. The most used tool is the spreadsheet and for a smaller DGS, it perfectly serves the purpose for keeping track of risks. These tools offer functionalities such as risk identification, assessment, prioritisation, monitoring, and reporting, streamlining the entire risk documentation process and enhancing the organisation's risk management capabilities.

4. Monitoring and reviewing

Monitoring and reviewing the risk management process is an essential practice that encompasses more than just the identified risks. It extends to evaluating the effectiveness of the risk management procedures themselves. This ongoing evaluation is critical for several reasons. Firstly, it allows organisations to assess the efficacy of their risk mitigation strategies and adapt them as necessary in response to changing circumstances. Additionally, monitoring and reviewing them ensures that the risk management process remains aligned with organisational goals and regulatory requirements. Moreover, it enables the identification of areas for improvement and optimisation within the risk management framework. By regularly (once a year or continuously, depending on complexity or in case of trigger event) scrutinising both the identified risks and the risk management process itself, organisations can enhance their resilience and responsiveness to emerging threats and opportunities.

5. Stakeholder engagement

Stakeholder reporting is a strategic approach in communicating key information to stakeholders in a manner that is both succinct yet substantial. Stakeholders can include depositors, banks, governments, regulators and employees, each with their own expectations and requirements. An appropriate level of high-level reporting is crucial for maintaining trust, ensuring transparency, and fostering a positive relationship with these groups. To define and execute this effectively:

Clarity and Conciseness: Reporting should distil complex information into clear, concise summaries. Stakeholders often have limited time, may not be experienced in the subject, and prefer reports that quickly get to the point, highlighting critical data, outcomes, and strategic directions without delving into excessive detail and using simple non-technical language.

Relevance and Materiality: The content of reports must be carefully selected to ensure relevance to the audience. Focus on material information that significantly impacts the scheme or its stakeholders' decisions and perceptions. Prioritising data and insights that align with stakeholders’ interests and concerns is key.

Forward-Looking Insights: Beyond presenting the past and current state of affairs, reporting should provide stakeholders with forward-looking insights. This includes future strategies, anticipated risks, and how the scheme plans to address them. Such statements help stakeholders understand the scheme's direction and its preparedness for future challenges.

Regular and Timely Communication: The frequency and timing of reports are

critical. Regular, scheduled updates ensure that stakeholders are kept informed about the scheme's progress and any significant changes in its operating environment. Timely communication, especially in the wake of a default or other crisis, is essential for maintaining trust and confidence. Not all stakeholders will require the same reporting frequency.

Accessibility and Engagement: Reports should be accessible and engaging to the target audience, using visual elements like charts and infographics to aid in the understanding of complex information. The use of digital platforms for disseminating reports can also enhance accessibility, allowing for interactive elements and real-time updates.

Transparency and Accountability: High-level reporting must demonstrate the scheme's commitment to transparency and accountability. This involves openly discussing challenges, setbacks, and areas for improvement, in addition to achievements and successes. Such honesty fosters trust and credibility among stakeholders.

Compliance and Ethical Considerations: Ensure that reporting practices comply with legal and regulatory requirements and adhere to ethical standards. This includes respecting confidentiality agreements and avoiding the disclosure of sensitive information that could harm the scheme or its stakeholders.

In summary, an appropriate level of high-level reporting to stakeholders involves balancing the need for concise, relevant information with the requirement for comprehensive, forward-looking insights. It necessitates a strategic approach to communication that values transparency, accountability, and stakeholder engagement. By effectively implementing high-level reporting, schemes can strengthen their relationships with their stakeholders, enhancing their reputation and stakeholder confidence.

6. References

Capital Regulatory Requirements (CRR) - Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 Text with EEA relevance. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0575

Committee of Sponsoring Organizations of the Treadway Commission (COSO) - Internal Control - Integrated Framework Available: https://www.coso.org/guidance-on-ic

ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk (open-source information)

IADI Core Principles for Effective Deposit Insurance Systems (2014), Available: https://www.iadi.org/en/assets/File/Core%20Principles/cprevised2014nov.pdf

IADI Organizational Risk Management for Deposit Insurers (2007) Available: https://www.iadi.org/en/assets/File/Papers/Approved%20Research%20-%20Discussion%20Papers/Risk_Management_for_DIs.pdf

Reaiche C.; Papavasiliou S.; Anglani F. (2022), Risk Assessment and Quality Project Management. Available: Risk Assessment and Quality Project Management

Ritchey, T. (1998). General Morphological Analysis: A general method for non-quantified modeling, Available: https://www.swemorph.com/ma.html

Usability first (2015) Facilitated Brainstorming, Available: https://www.usabilityfirst.com/usability-methods/facilitated-brainstorming/index.html

Annexes

Annex 1: DGS risk taxonomy
Annex 2: Basic and advanced tools
Annex 3: A comprehensive overview of the possible analysis

Annex 1: DGS risk taxonomy

Risk Category (level 1)	Definition	Risk Category (level 2)	Examples
Strategic and governance risks	Risk that the DGS's operations do not meet the expectations of its stakeholders and risk that DGS governance structure and procedures are not adequate to its mandate	**Governance** **Planning & Resource allocation** **Communication and stakeholder relations**	Risk that the DGS's operations do not meet the expectations of its *stakeholders* (member banks, statutory bodies, depositors, suppliers, consultants, employees, authorities, international organisations, etc.); risk that information and/or documentation for the statutory bodies is not adequate, correct, complete, or is not aligned with existing standards and procedures; risk that external communication or *public awareness is not* adequate, correct, complete, not up-to-date or not timely.
Operational risks	Risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. It includes legal risk	**Internal fraud**	Theft and fraud risks, risk of IT security breaches, from internal sources.
		External Fraud	Theft and fraud risks, cyber security risks, from external sources; risk of undue influence and coercion to management and staff exercised by external sources.
		Employment practices and workplace safety / HR issues	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events / harassment failure to retain and retain key personnel; failure to attract qualified and/or sufficiently experienced personnel; inability to develop and enhance employee skills; risks derived from low employee satisfaction & morale; poor succession planning, failure to provide clear responsibilities and a clear chain of command.
		Depositors, products and DGS practices – compliance & legal risks	Risk of non-compliance, in the conduct of the DGS's activities, with external laws and/or regulations, internal rules and regulations, internal policies and/or procedures, or of incorrect application or disregard; risk of litigation; risk of breach of privacy Risk of incorrect management of corporate, tax and/or regulatory obligations; risk of breach of expenditure processes; risk of non-payment, incorrect payment;
		Damage to physical assets	Risk of loss or damage to physical assets from natural disaster or other events;

Risk Category (level 1)	Definition	Risk Category (level 2)	Examples
		Business disruption and system failures (ICT Risk)	Risks include equipment malfunction and/or system obsolescence, malfunctioning IT systems, day-to-day incident management and/or business continuity issues, and risks stemming from the compromise of the system, which encompass potential disruptions to **system availability**, breaches in data **integrity**, and violations of **confidentiality**. These risks can collectively undermine the overall security and reliability of the system.
		Execution, delivery and process management	Risk of malfunctioning of procedures; risk of absence of procedures and/or non-existent, incomplete and/or incorrect implementation of procedures; internal policies and/or procedures are not updated and/or not timely updated; risk of human error and/or professional negligence; risk of errors in calculation and/or processing of information; risk of unavailability and/or (qualitative) inadequacy of human resources; risk of inadequacy of equipment; risk of failure to comply with deadlines and/or agreements; risk of inadequacy of facilities and/or environments; risk of unavailability or non-accessibility of premises; risk of inadequate communication; risk of incorrect bookkeeping entries; third party risks.
Financial risks	Risk that the DGS's resources are not adequate/sufficient or not available for the interventions and risk of losses coming from financial investments	**Liquidity**	Risk that the DGS has not sufficient liquidity for intervention; Risk that financial investment cannot be liquidated;
		Funding	Risk that the DGS's resources are not adequate/sufficient or not available for the interventions. Risk that banks contributions cannot be levied;
		Market risk	Risk of losses arising from movements in market prices (interest rate risk, price risk, currency risk, hedging risk);
		Credit Risk	Risk that DGS counterparty exposure of financial investment will fail to meet its obligations;

Risk Category (level 1)	Definition	Risk Category (level 2)	Examples
Reputational risks	Risk of negative stakeholder perception of the DGS. Reputational risk can be direct or derived from other type of risks (indirect)		Risk of negative *stakeholder* perception of the DGS (direct and indirect risk); risk of incorrect and/or incomplete disclosure to counterparties; risk of incomplete or incorrect information being published on the institutional website and/or non-publication of relevant information.

Annex 2: Basic and advanced tools

Facilitated brainstorming (basic tool)

Facilitated brainstorming is a risk identification tool on its own but can also be used with other tools and processes. The key success factor to proper brainstorming session is a dedicated and coherent facilitator. Proper brainstorming demands focus and dedication from the facilitator, and it contributes to the outcome of the brainstorm session. The facilitator acts as the session leader, ensuring smooth and efficient progress. They create a safe and open atmosphere where all participants can freely express their thoughts. The facilitator guides the discussion towards the objective and prevents digressions and encourages constructive collaboration and creativity among participants. Following phases are essential to successful brainstorm session:

Preparation. Clearly define the session's objectives and schedule. Invite participants with diverse expertise and perspectives. Equip the session room with necessary tools. Remote sessions can be organized, but live events encourage much more participation and activity.

Conducting the Session. Begin the session by presenting the objective and instructions. Encourage participants to share their thoughts and ideas. Remind that the matters discussed are confidential. Accept all ideas without criticism or judgment. Write down identified risks. Encourage participants to build upon each other's ideas. Keep track of time. For example, set a goal of identifying 10 risks, and see that each risk gets 15 minutes of discussion. The session can be intense, so remember to keep a break when necessary.

Conclusion. Adhere to the schedule and ensure the session ends on time. Thank participants for their contributions and inform them of the next steps. Document all identified risks and their details and share the finished document with participants.

Morphological analysis (advanced tool)

The morphological analysis is a systematic method used to generate and explore potential risk events by systematically combining various parameters or factors. It allows for a structured exploration of different dimensions or aspects related to a problem, enabling comprehensive coverage of potential risks. Instructions for conducting morphological analysis as a risk identification tool:

Determine the key parameters or factors relevant to the risk context. These could include aspects such as technology, human behaviour, environment, regulations, etc.

Create a morphological chart. Construct a table or matrix with rows representing each parameter and columns for possible variations or states of each parameter.

Generate Combinations. Systematically combine different variations of parameters to create potential scenarios or risk events. This can be done by filling in the cells of the matrix with relevant combinations.

Brainstorm and analyse. Engage stakeholders in brainstorming sessions to explore each combination and its implications for potential risks. Select the most potential scenarios to be used in the next risk analysis phase.

Annex 3: A comprehensive overview of the possible analysis

Proposed activity	Tool/Objectives	Basic analysis	Intermediate analysis	Advance analysis
Defining & documenting the objective of the specific system or process for which the risk will be assessed	**Conducted SMART**: specific, measurable, achievable, relevant and time-bound).	X	X	X
Defining the risk criteria for likelihood/probability and for impact/consequences	- **likelihood/probability**: potential for fraud, complexity of the process, significant changes that occurred during the reference period, process sensitivity, reliance on ICT systems etc. - **impact/consequences**: financial loss; non-fulfilment of objectives; reputation damage, etc.	X	X	X
ESG factors*	**Environment**: i.e.: quantifying carbon footprint; **Social**: i.e.: engaging in social activities, employee benefits; **Governance**: i.e.: sustainability report, risk management.	X	X	X
Involving subject matter experts in the process.	Identifying the stakeholders who have useful knowledge in the analysed process and involving them in the risk analysis.		X	X

Proposed activity	Tool/Objectives	Basic analysis	Intermediate analysis	Advance analysis
Defining or revising risk indicators associated with the process's probability risk criteria	**Potential for fraudulent activities**: Evaluates the environmental factors surrounding the process, such as the prevailing conditions (e.g., highly favourable or unfavourable), and the level of difficulty inherent in perpetrating fraud. **Process complexity**: Considers the volume and diversity of operations within the process, as well as the requisite specialized skills or qualifications necessary for execution, and the susceptibility to cognitive strain. **Impact of significant changes**: Assesses the impact of notable alterations during the reference period, including shifts in the legal framework, modifications to IT&C systems, organizational restructuring, or fluctuations in staff turnover. **Business impact analysis focusing on system availability**: Analyses the repercussions of system unavailability on core business activities. **Dependence on ICT systems**: Examines the reliance on specific equipment, the nature of networks (internal or external, closed or open), the complexity and variety of applications (interdepartmental, volume of managed information), and the sensitivity of data (confidentiality, availability, integrity, logical and physical security).		X	X
Software	Implementing risk management software to keep track of risks.			X

* Given the increasing significance of Environmental, Social and Governance (ESG) risks, it is recommended to incorporate them into the risk assessment process.