EFDI. EUROPEAN FORUM OF DEPOSIT INSURERS

Laying the Groundwork: A Non-Binding Risk Management Policy for Deposit Guarantee Schemes 2025

This publication is available on the EFDI website (www.efdi.eu)[1]

European Forum of Deposit Insurers – Association of European Deposit Guarantee Schemes and Investor Compensation Schemes. 35, rue du Congrès, 1000 Brussels.
E-mail: secretariat@efdi.eu
Registered Office: Rue de la Presse 4, 1000 Bruxelles. KBO/BCE: 0892.945.871.

[1] Prepared by EFDI Risk Management Working Group
Drafting team: Melinda Friesz -RMWG Co-Leader-(NDIF, Hungary), Loïc Trintignac -RMWG Co-Leader-(FGDR, France), Jalal Rayi (ADIF, Azerbaijan), Iliya Ploshtakov (BdB, Germany) Oliver Gordon (FSCS England), Roxana Rătescu (FGDB, Romania), Snezana Ivanovic (fzdcg, Montenegro), Panayiota Dionysiou (Resolution Department-Central Bank, Cyprus), Kate Storey (DCS, Guernsey), Isabelle Gil (CSSF, Luxemburg), Alessio Greco (FGD, Italy), Cristina Cerbu (FGDB, Romania), Sylvie Godron – PRC Leader (FGDR, France).

EFDI. EUROPEAN FORUM OF DEPOSIT INSURERS

Table of content

I. Introduction

The European Forum of Deposit Insurers (EFDI) Risk Management Working Group (RMWG) has formulated this Risk Management Policy to support its members in strengthening their institutional risk management governance. This policy is intended as a practical framework that Deposit Guarantee Schemes (DGSs) can adapt to their specific legal, operational, and organisational environments.

This policy is designed in alignment with the European Union's Directive 2014/49/EU on Deposit Guarantee Schemes (DGSD2) and relevant guidelines issued by the European Banking Authority (EBA). It also draws on established principles of good governance and risk management from international standard-setters. EFDI acknowledges the diverse legal and institutional frameworks of its members and promotes a harmonised yet flexible approach to risk management across jurisdictions.

This policy promotes a principles-based approach, emphasizing core values such as accountability, transparency, and adaptability. Members are encouraged to implement risk management frameworks that align with these principles while considering their specific mandate, size, and complexity. Recognising the heterogeneity among EFDI members, the policy is designed to allow for scalable implementation based on available resources, risk exposure, and organisational maturity.

The content of this policy is intended to apply to all functions and activities of the member organisation, including governance structures, operational teams, strategic initiatives, and third-party relationships. Members may tailor its content to reflect their national context, legal obligations, and institutional responsibilities.

Governance & Reporting: The Board as the highest governing authority within the organisation is responsible for setting the risk appetite and approving the risk management framework. The Executive Management Team, who are responsible for operationalising the risk management framework, ensures that it is embedded across processes. The Risk Management Office (or similar) supports risk identification and assessment activities, maintains the risk register, and ensures regular review of controls. A robust risk reporting process that includes for example: periodic risk assessments, escalation mechanisms for emerging or critical risks and Board-level reporting on key risks and mitigation strategies.

Risk Identification, Triage and Review: The identification, treatment and review of risk should be systematic, covering both internal and external sources of risk. Common methods include stakeholder workshops, scenario analysis, and regulatory reviews. Areas of consideration here include: risk assessment (likelihood v impact), risk categories (i.e. strategic, reputation), risk mitigation (tolerate, treat, transfer, terminate) and review (review, challenge and reporting of the risk position).

Risk Culture: To be successful, a positive risk culture led from the top is required. It is recommended that there is organisation-wide awareness and shared responsibility for managing risk, that staff are provided with risk-related training appropriate to their roles and that everyone is actively encouraged to operate with transparency, reporting issues or incidents without fear of repercussion.

A first document produced by the Risk Management Working Group set out **non-binding guidelines on ensuring stability through a robust risk management framework**[2]. Its objective was to provide structured support to Deposit Guarantee Schemes (DGSs) in identifying, assessing, and mitigating the most common risks that could impact their operations. These guidelines present an overview of the five key risk categories a DGS should consider and offer practical recommendations, tools, and examples of good practices that can be adapted to the individual characteristics of each DGS.

A proportionate, well-designed risk management system is essential for the DGS to fulfil its mandate effectively. By systematically addressing the critical risk areas outlined in these guidelines, a DGS can enhance its resilience, operational readiness, and capacity to protect depositors. Furthermore, the guidelines emphasize the importance of integrating risk management into the DGS's governance structures, policies, and day-to-day operations.

In the following sections, we will discuss the principal risks highlighted in the guidelines, along with the corresponding proposed mitigation strategies and control activities.

These discussions aim to assist DGSs in designing a risk management system that is both effective and proportionate to their size, complexity, and risk exposure. Is important to note that the mere absence of certain risks or controls mentioned in this policy document does not necessarily indicate a gap or vulnerability. The relevance and criticality of each control depend on the size, complexity, and operational model of the specific DGS. For example, a DGS operating with a lean structure and limited ICT reliance may reasonably adopt a simpler set of controls, while a larger DGS managing multiple systems and vendor relationships may require a more comprehensive framework.

Governance and Oversight

Governance weaknesses within a DGS can have spillover effects, not only for the scheme itself but for the stability of the broader banking sector through lost confidence and in extreme cases, by bank runs. As the European Central Bank (ECB) defines, "Governance and risk culture are essential features of any well-functioning organisation, having an impact on its structure, culture, and people" (ECB, 2014).

While governance and risk culture are fundamental to the effective operation of a DGS, their implementation poses challenges, as they influence the structure, culture, and key decision-makers within the organisation. Establishing a well-defined governance framework is particularly critical for a DGS, given its role in safeguarding depositors and reinforcing confidence in the financial system.

A DGS must ensure that its core values[3] — such as trust, transparency, and

[2] https://www.efdi.eu/storage/2617371/download?refresh_at=1727778588

[3] Core values represent the behaviour and belief system of an organization. They are set of universal principles, and standards for choosing right course of action in day-to-day life of an organization. Values are not the exclusive property of any one group or institution. Core values explain and justify what people do and what organizations stand for. Since core values are ideology and purpose driven, they influence the vision of an organization. Therefore, working on core values and practicing on them in the organizational setting is of profound importance for creating and clarifying the vision of an organization. International Journal of Learning & Development ISSN 2164-4063 2013, Vol. 3, No. 3, https://www.academia.edu/download/31621665/Ideolology_Purpose_Core_Values_and_Leadership-_How_they_Influence_the_Vision_of_an_Organization.pdf

accountability—are clearly communicated, internalised, and consistently monitored throughout the organisation. It is imperative that all stakeholders understand how the board and senior management systematically assess and reinforce the DGS's risk culture. Furthermore, it is strongly recommended that the DGS defines and documents the material components of its risk culture, proactively identify gaps, and implement corrective measures where necessary.

The internal governance framework of a DGS must clearly delineate the functions responsible for managing and mitigating risks. This framework ensures that risks are properly identified, assessed, escalated, and addressed in alignment with the DGS's strategic objectives and risk appetite. Effective governance within a DGS is essential to maintaining depositor confidence, preventing governance failures—such as operational inefficiencies or inadequate crisis preparedness—and promoting sound risk management practices.

A robust governance framework within a DGS requires that members of the management body and key function holders possess the necessary expertise to oversee risk management effectively. Additionally, the DGS must ensure that decision-makers have timely access to high-quality data, enabling informed decision-making in both normal operations and crisis situations, such as bank failures or financial instability.

A well-defined risk appetite is particularly crucial for a DGS, as it determines the scheme's approach to risk-taking in areas such as fund management, payout processes.

The DGS's risk appetite and risk tolerance must be clearly articulated in its policy framework to ensure consistency in decision-making and alignment with its mandate of financial stability and depositor protection.

The governance framework should also establish clear roles and responsibilities for risk management. Typically, a designated risk manager oversees the implementation and effectiveness of the risk management framework. Each significant risk should have an assigned risk owner responsible for identifying hazards, evaluating and categorising risks, and implementing appropriate control measures. A structured review process must be in place to regularly assess the effectiveness of these controls and ensure that residual risks remain within acceptable limits.

II. Minimum risks of a DGS

II.1 Financial Risk Management

Effective financial risk management is a cornerstone of a robust and resilient DGS. Given the DGS's critical role in maintaining depositor confidence and ensuring financial stability, its ability to secure and deploy financial resources during times of stress—particularly during bank failures—is essential.

Financial risks faced by a DGS are varied and interconnected, encompassing funding risk, market risk, credit risk, and liquidity risk. Inadequate preparation could compromise the DGS's ability to fulfil its payout obligations, thereby undermining public trust in the financial system. To mitigate these risks, DGSs must adopt proactive, flexible, and comprehensive financial risk management frameworks that align with both domestic legal requirements and international good

practices, such as the guidelines from the International Association of Deposit Insurers (IADI).

It is important to note that the following **financial risk mitigation strategies and control measures should be viewed as recommendations rather than prescriptive mandates.** Their relevance and implementation depend on the specific structure, size, operational environment, and risk appetite of the DGS. Smaller or less complex DGSs may adopt a simpler approach, while larger schemes managing diversified funds may require more advanced financial risk tools.

By developing a tailored financial risk management framework, the DGS can ensure it remains adequately funded, maintains sufficient liquidity, and withstands potential economic or systemic shocks—thus safeguarding depositors and contributing to financial system stability.

Mitigation of Funding Risk in the DGS

Relevant financial data to be collected and analysed may include key economic indicators and figures regarding the economy in general as well as the economic cycle, the current level and trends of deposits (total and eligible), the outlook of the banking sector and particularly the financial position of DGS's members. Regulatory environment regards legislation in force and imminent / under preparation developments in national and European legislation related to deposit insurance.

RC Instruments: The DGS may seek to collect relevant data in common sources of information such as published reports and other information provided from national and competent authorities, the banking sector, financial net entities, and financial stakeholders.

To effectively manage these risks, institutions must:

- Maintain liquidity reserves to mitigate funding and operational risks,
- Monitor reputational risks through public sentiment analysis and stakeholder engagement.

Regular reporting of the KRIs to the management board is essential to highlight the impending risks and draw attention to them. By integrating real-time monitoring, risk mitigation strategies, and proactive interventions, deposit insurance funds can enhance resilience, minimise disruptions, and maintain long-term stability.

Possible Risk Mitigation Strategies

1. Diversified Asset Management: The DGS should maintain a diversified and balanced portfolio that includes highly liquid and secure investments. This ensures quick access to funds during payout events and minimises the risk of loss due to over-concentration in specific asset types or sectors.

2. Accurate Portfolio Valuation and Monitoring: The DGS should regularly assess the market value of its asset holdings, ensuring that financial statements reflect up-to-date valuations. Continuous credit risk assessment of investment counterparts is critical to identifying emerging vulnerabilities early.

3. Alternative Funding Mechanisms: To enhance its funding flexibility, the DGS should arrange for standby credit lines and establish bridge financing options. These mechanisms provide emergency liquidity in cases where payout demands exceed immediately available resources. Statutory or contractual arrangements should ensure enforceability of the alternative funding mechanisms.

4. Stress Testing: The DGS should conduct regular stress testing to evaluate its resilience under adverse conditions. Scenarios should simulate severe liquidity stresses, market shocks, and systemic bank failures to ensure preparedness.

5. Market Risk Hedging: Where appropriate, the DGS should employ hedging strategies to manage exposure to market volatility:

- **Interest rate hedging** to protect against fluctuating rates that could impact asset returns,
- **Currency hedging** to minimise the impact of exchange rate fluctuations on the value of foreign-denominated investments.

Risk Control Instruments

1. Portfolio Monitoring and Reporting: The DGS should implement robust liquidity monitoring practices, producing regular liquidity reports to confirm that resources are sufficient to cover potential depositor claims. Key market risk indicators—such as interest rate shifts, currency trends, and market volatility—should be monitored continuously.

2. Stress Testing and Scenario Analysis: The DGS should perform periodic scenario analyses that simulate extreme yet plausible crisis events, such as multiple bank failures, economic downturns, or sovereign defaults. Results should be used to refine recovery and contingency plans that identify steps for securing additional funding when needed.

3. Risk Limits and Tolerances: The DGS should establish and enforce specific investment limits and risk tolerances:

- **Concentration limits** to avoid excessive exposure to any single institution, asset class, or sector,
- **Credit quality thresholds** requiring investments to be made primarily in secure and highly creditworthy instruments, including but not limited to government bonds.

Key Considerations for Financial Risk Management

When designing its financial risk framework, a DGS must account for:

- **Country-specific characteristics** including legal environment, financial market depth, and supervisory practices,
- **Dependence on commodities** if the national economy is influenced heavily by commodity prices,
- **Currency risk** particularly if funds are invested or potentially needed in multiple currencies,
- **Macroeconomic tendencies**, such as inflation rates and GDP growth patterns, which impact liquidity and asset value,
- **Sources of Liquid Resources** including government agreements, domestic market loans, and international loan facilities,
- **Premium Structures**, ensuring that ongoing contributions from member institutions are sufficient and sustainable to meet target fund levels.

II.2 Third-Party Risk Management

Third-Party Risk refers to the potential adverse effects that come from relying on external vendors, suppliers, or partners for critical services.

DGSs, like other financial sector entities, increasingly rely on third-party service providers for critical functions such as IT services, data processing, asset management services, legal and compliance support, and crisis communication. While outsourcing can enhance operational capacity, it also exposes the DGS to a range of risks including operational, data security and privacy, regulatory, financial, and reputational that must be managed through a structured Third-Party Management (TPRM) framework.

This section outlines the framework applied to TPRM, inspired by principles reflected in the EBA Guidelines on outsourcing arrangements[4], while remaining tailored to the DGS environment.

Vendor and service provider risk assessment

All third-party vendors should be systematically identified and documented within a centralised register. Each relationship is classified based on the criticality of the services provided, their contribution to core DGS functions, and the level of risk exposure they carry. Particular attention is paid to providers supporting the compensation process, information systems, or communication with the public.

Prior to establishing a contractual relationship, the DGS must perform a documented risk assessment to evaluate the potential operational, financial, and reputational impacts in case of service disruption. This includes an analysis of data sensitivity, legal exposure, and the provider's role in the continuity of essential activities. Vendors are then categorised according to their risk level, which determines the level of scrutiny and control applied throughout the lifecycle of the engagement.

Due diligence must be conducted to assess the provider's financial health, information security posture, regulatory compliance record, and the maturity of its business continuity and incident response capabilities. Further, an analysis (where possible) of the concentration risk that the provider presents should be completed and factored into alternative recovery strategies where relevant. This evaluation must be conducted not only at onboarding but also reviewed on a regular basis to reflect any material changes in the risk profile.

Contractual Obligations and Risk Mitigation

All third-party relationships must be governed by formal contracts. These agreements must include detailed service descriptions, performance expectations, and service level agreements (SLAs), confidentiality clauses, data protection requirements, audit rights, exit clause and clearly defined exit strategies. Contractual terms must ensure that the DGS can maintain control and continuity in

[4] EBA/GL/2019/02

the event of non-performance or termination.

Consideration of Environmental, Social and Governance (ESG) matters is a vital consideration in the execution of effective third-party vendor management. Whilst these are not currently a decisive factor for all DGS', ESG matters provide intelligence which is useful in the wider risk management landscape.

Monitoring and contingency planning for outsourced services

Once a provider is engaged, its performance and risk exposure must be continuously monitored. This includes periodic reviews of service levels, operational performance, security posture, and compliance with contractual obligations. Providers deemed high-risk should be monitored more frequently and be subject to enhanced supervision and reporting requirements.

Third parties must also be fully integrated into the DGS's crisis management and incident response procedures. This includes participation in simulations, alignment of escalation protocols, and real-time communication channels in the event of major disruptions. Providers must be able to notify the DGS as soon as possible in the event of a breach, outage, or security incident, and support coordinated recovery efforts.

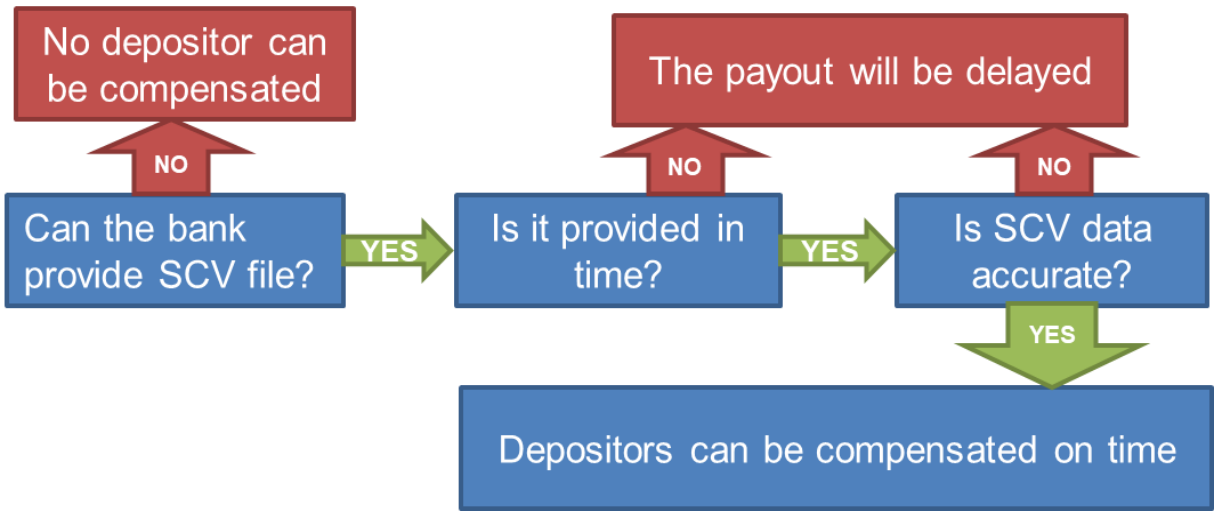
Finally, the DGS must establish and maintain a contingency and response plan to address third-party failures or breaches. The objective is to ensure that the DGS can maintain its critical operations and fulfil its mandate. In line with the EBA's expectations, contingency planning must be in place to ensure that, in the event of provider failure or contract termination, the DGS can maintain continuity of operations by, for instance, activating temporary internal reallocation of the concerned processes, or activate the exit plan (alternative providers).

Third-party risk is a complex but essential dimension of a DGS's overall risk management framework. By implementing a structured approach to assessment, contracting, and supervision, DGSs can reduce their exposure to third-party failures and improve operational and reputational resilience.

II.3 Managing SCV Data Quality Risk

SCV files are computer files in a defined, portable format containing a full set of information for each depositor that allows unequivocal identification of the depositor and accurate computation of the compensation amount.

Figure 1: Use of SCV in case of a pay-out



Source: Risk Management Working Group Members

Disclaimer: the use of SCV files will vary depending on other variables, i.e., type of DGS, dependencies from external sources, delays in the process and so on.

In case of bank failure followed by depositors' pay out, SCV files are the key for timely & accurate compensation.

Credit institutions are responsible for having in place adequate systems (including ICT systems that allow them to always have full and accurate records of data on depositors.

The quality SCV data is critical to the operational success of a DGS especially during payout events. Poor SCV file quality can lead to delayed payouts, regulatory penalties, operational inefficiencies, and reputational damage. Therefore, robust processes for **data validation, reconciliation, and secure transfer** must be in place to ensure that SCV files are reliable, accurate, and readily usable in crisis situations.

According to the EBA Guidelines on DGS Stress Tests (EBA/GL/2021/10), DGSs should perform regular tests of SCV-files of member institutions. These tests are considered a core element of DGSs' stress testing and contingency planning, and aim to assess the quality and reliability of SCV-files, including the completeness and accuracy of depositor data.

Good quality SCV data must meet the following criteria:

- **Real**: Data must be supported by verifiable documents and facts,
- **Correct**: Information in the member institution's databases must align with depositor IDs, application forms, contracts, and other official records,
- **Complete**: All eligible depositors must be included,
- **Consistent**: Mandatory database fields must be properly populated, with no mismatches or field confusion,
- **Secure**: Data must be protected through secured communication channels and/or encryption mechanisms,
- **Timely**: SCV files must reflect up-to-date information and be provided within

the legal deadlines.

When one or more of these qualities is lacking, the risk of operational failure during a payout event significantly increases. Moreover, all parties involved in the handling of SCV data must ensure full compliance with the General Data Protection Regulation (GDPR).

Depositor Identification

Accurate depositor identification is fundamental to efficient payout processing. To facilitate this, each depositor should have a **unique identifier** enabling quick validation and calculation of the insured amount. In a cross-border context, due to differences in national laws and practices regarding customer identification, the DGS may need to adopt additional measures to ensure that unique depositor identification is possible.

At minimum, the DGS should verify the uniqueness of the depositor identifier and promptly investigate any exceptions. Where permitted by national legislation and practice, the use of a national personal identification number is recommended, as it often includes validation algorithms that enhance reliability. However, unique identifiers may not always be available in SCV files from foreign DGSs, which should be taken into account.

Compensation Amount

Ensuring the **accurate and timely identification of all eligible account balances** is crucial. Banks must be able to:

- Accurately report the balances of all eligible accounts for each depositor,
- Identify and deduct any amounts in accordance with applicable law, such as outstanding loan instalments, commissions, or secured obligations,
- Highlight accounts under specific conditions (e.g., pledged accounts, unsettled transactions).

Safe and Swift Transfer of SCV Files

The secure and timely transfer of SCV files from a failed institution or its liquidator to the DGS is critical to ensure operational continuity. The transfer process must protect data from corruption, unauthorised disclosure, and loss. Appropriate IT and cybersecurity controls must be employed.
Failure to maintain secure and timely SCV file transmission can significantly hinder the DGS's ability to respond to crises.

Remediation Measures for Data Inconsistencies

To mitigate SCV data risks, a comprehensive set of regulatory, operational, and technical measures must be implemented:

- **Depositor Identification**: Establish a clear legal framework obliging credit institutions to maintain and provide SCV files on demand. The DGS should be empowered to conduct on-site and off-site inspections to test SCV file compliance and mandate timely and permanent corrections,

- **Compensation Amount**: Develop structured cooperation between banks and the DGS during non-crisis periods to pre-emptively address potential complications in identifying eligible versus non-eligible deposits, handling deductible amounts, and managing pledged or unsettled transactions. The DGS should also assess bank procedures regarding depositor eligibility and compensation calculations,
- **Safe Transfer of SCV Files**: Require the use of secure communication channels and/or encryption for SCV file transmission to protect sensitive depositor information,
- **Timely Availability**: Regularly monitor the quality of SCV files through sample-based fire drills and inspections. Periodic fire drills not only test operational readiness but also encourage banks to maintain accurate, up-to-date SCV data.

In cross-border payout cases, it must be noted that the host DGS does not have direct control over the quality of the SCV file data, and therefore the home DGS bears responsibility for data accuracy and integrity.
By instituting these measures, the DGS strengthens its operational resilience, minimises risks associated with SCV data, and ensures depositor protection even under stressful conditions.

II.4 Reputational Risk Management

Communication plays a critical role in the overall risk management of any DGS or institution involved in financial stability safety net. It is both a strategic tool and a potential vulnerability, especially in situations where public trust and institutional credibility are at stake.

International standards such as COSO Enterprise Risk Management (ERM) and ISO 31000 stress that organisation must proactively manage communication as a transversal, embedded dimension of risk. The COSO ERM framework views reputational risk not as a standalone category, but as a consequence of events related to other risks (operational, compliance, governance). It emphasises the importance of managing communication within each risk scenario, given its amplifying effect. The ISO 31000 standard defines risk as the "*effect of uncertainty on objectives*" and incorporates reputational aspects into enterprise-wide risk analysis. It promotes anticipation, coordination and resilience, with communication being essential to informed decision-making and confidence.

Reputational risk is transversal. It encompasses both internal and external factors and is highly sensitive to how the DGS communicates, especially in times of uncertainty or crisis. Miscommunication, poor coordination or inadequate preparedness can seriously damage public trust, even if operational mechanisms are working effectively. A communication strategy is typically built around two core dimensions:

1. Dual communication modes: "Peacetime" and "Crisis"

DGSs operate in two distinct communication modes:

- In "**Peacetime**", the objective is to proactively inform, educate, and reinforce public confidence in the guarantee scheme and the broader financial safety net. This includes regular public awareness, media visibility, actions carried out in collaboration with financial institutions involving communication, training, coordination and crisis preparedness,
- In "**Crisis**" mode, communication must become strategic, responsive, and tightly coordinated. Messaging must be timely, accurate, and consistent across all channels to preserve public trust and support operational responses such as deposit reimbursement or emergency interventions.

This dual approach ensures that communication is not reactive by default but integrated into preparedness planning and risk mitigation.

2. Communication as a strategic risk function

Communication is not a secondary or supportive activity. It is a core component of reputational and operational resilience. Mismanaged communication can escalate minor incidents into crises, or worsen the public impact of operational disruptions. Effective communication risk management requires:

- Clear internal validation processes,
- Pre-crisis planning and scenario-based communication assets,
- Reliable and well-coordinated external partners, and
- Continuous alignment with operational and strategic functions.

Risks affecting DGS reputation

Several factors may compromise the ability of a DGS to manage communication effectively, particularly during crisis situations. These risks can generally be grouped into two main categories: internal incapacity and communication channel disruption.

- Internal incapacity to manage communication
  - Failures in communication tools and systems: Malfunctioning or unavailable internal platforms (e.g., compensation system, websites, crisis dashboards, mailing systems) may stop timely and coordinated dissemination of key messages;
  - Inadequate spokesperson communication: Inaccurate, inconsistent, or poorly phrased public statements from authorised representatives may generate confusion, anxiety or even panic among stakeholders,
  - Spread of defamatory or misleading information: Unverified or harmful content can rapidly circulate, damaging public confidence and the reputation of the DGS if not addressed swiftly and transparently,
  - Disruptions in the compensation communication process: Ineffective communication regarding reimbursement procedures can leave depositors uninformed or misinformed, amplifying dissatisfaction and eroding trust in the DGS.

- Inability or failure of communication channels
  - Contact centre malfunctions or underperformance: Insufficient capacity, lack of trained personnel, or total unavailability of helplines during a crisis may lead to significant reputational damage and reduced public confidence,
  - Website and digital platform outages: If public-facing digital channels become unavailable or fail to relay, in real-time, an accurate information, the risk of misinformation spreads fast and panic escalates,
  - Disruptions in press and social media operations: Unresponsiveness from external media partners or internal teams responsible for media management may result in loss of narrative control, enabling speculative or inaccurate narratives to dominate the public discourse.

These factors can individually or collectively damage an institution's reputation even when the operational side (such as deposit reimbursement) is functioning correctly.

Crisis communication and stakeholder management

Reputation is most vulnerable during crises, where expectations for transparency, speed, and clarity are crucial. A DGS must be able to switch quickly into crisis communication mode, with all components (internal and external) aligned and ready.

Recommended approaches include maintaining a dual communication structure that distinguishes between peacetime and crisis modes. In peacetime, communication should be proactive and educative, aimed at strengthening public understanding and reinforcing confidence in the scheme. In contrast, during a crisis, communication becomes reactive, strategic, and must be fully integrated with the operational response, such as deposit reimbursement. To support this, DGSs should ensure consistency of messaging across all platforms, including websites, media, call centres, and social channels. Rapid and accurate dissemination of information relies on the presence of clearly defined internal processes. One key element is the establishment of a dedicated internal crisis communication unit, referred to as a Rapid Response Team, composed of representatives from legal, IT, communications, and operational departments. This team should be specifically trained and prepared to act swiftly in crisis situations. It must operate under a clear mandate, with well-defined activation procedures and access to pre-approved communication scenarios tailored to various incident types. Regular involvement of the team in crisis simulations enhances coordinated and timely responses, reducing the risk of internal miscommunication and delays in public messaging.

Managing these elements effectively helps mitigate the reputational impact of crises and reinforces stakeholder confidence in the institution’s credibility.

Preventive measures and response strategies

Reputation management requires not only the ability to communicate effectively, but also the existence of tested systems, trusted partners, and robust technical foundations. The following measures aim to strengthen both prevention and response capacities across all communication channels and providers. To this end, DGSs may consider implementing the following control framework.

External partner oversight plays a central role in this strategy. All service

providers involved in communication including call centres, press agencies, and digital service partners should operate under formal agreements that clearly define performance expectations, crisis protocols, and business continuity requirements. These agreements must be backed by a structured control framework, combining first-level controls (contractual and operational supervision) with second-level oversight that may include financial monitoring and thematic assessments to challenge the robustness of providers' crisis preparedness. The goal is to ensure that all partners remain operationally resilient and financially viable. Each year, providers should perform availability checks, sizing assessments, and dedicated operational testing in addition to their participation in crisis simulations to evaluate their readiness and coordination within the communication chain.

The following sections provide a more targeted view of the main communication-related service providers. While all are subject to the same common framework in terms of preparedness and oversight, each category involves specific operational requirements and risk considerations that must be addressed individually.

The **contact centre** must be supported by a business continuity plan that includes redundant sites and critical resources. Call centre agents should be regularly trained to handle high-stakes especially during compensation events. Annual tests should verify the centre's availability, capacity, and functionality. The contact centre should be fully integrated into crisis simulations.

Website hosting and digital platforms require special attention due to their critical visibility and public accessibility, especially during crisis events. Public-facing platforms must be designed with a high level of technical and operational resilience to ensure continuous access, reliable content delivery and protection against external threats.

To achieve this, platforms should be supported by both internal and external backup systems and incorporate redundancy at all levels, including servers and DNS. Resilience must be tested through regular technical exercises, such as load tests, penetration tests, and both technical and organisational audits. These evaluations should cover, among other things, performance, capacity, backup activation capability, and readiness under simulated conditions such as platform stress, cyberattacks or public misinformation events.

Finally, **press relations and social media** must be supported by agencies capable of scaling quickly and delivering messages across all channels in a timely and coordinated way.

The incorporation of these preventive and crisis-response mechanisms into a DGS's risk management approach enhances its resilience and strengthens its ability to preserve public confidence and institutional integrity.

II.5 Managing ICT Risk in a DGS

Information and Communication Technology (ICT) risk represents a critical and complex area of operational risk for any modern organisation and this is especially true for a DGS. As a financial backstop designed to protect depositors and ensure

financial stability, a DGS relies heavily on its ICT infrastructure to perform its core functions, including data management, claims processing, payout simulations, crisis response, and secure communications with member institutions and stakeholders.

ICT risk can manifest through various channels, such as system failures, cyberattacks, data breaches, or disruptions in third-party services. These events can compromise not only operational continuity but also the reputation and legal standing of the DGS. As such, managing ICT risk is not only a technical necessity but a strategic imperative for the DGS's long-term resilience.

To effectively build and operate secure, reliable, and scalable IT systems, a DGS can align itself with internationally recognised frameworks and standards. One such widely accepted standard is ISO/IEC 27001, which offers a structured and risk-based approach to establishing, implementing, maintaining, and continually improving an Information Security Management System. **In addition, domestic regulations, financial supervisory guidelines, and central bank expectations may provide further requirements or best practices tailored to the local context.**

Therefore, the controls and practices described in the following chapters should be interpreted as recommendations or guiding options rather than rigid requirements. Each DGS is encouraged to assess its own environment and tailor its ICT risk management strategy, accordingly, taking into account both local regulatory obligations and international best practices.

Ultimately, the goal is to ensure that ICT risks are identified, assessed, and mitigated in a manner proportionate to the DGS's role, resources, and risk exposure—so that it remains ready and capable of fulfilling its critical mission, even under stress or crisis scenarios.

Having in mind the complexity of ICT risks and the good practices shared, the following areas can be included in the risk management practices and considering them a source of risks.

Access Control and Identity Management

This chapter details how the DGS can regulate access to its systems, networks, and digital resources to prevent unauthorised use and support secure operations.

- **Password Policy**
  The DGS should enforce a strict password policy requiring strong, complex passwords across all systems. Passwords should be changed regularly, and repeated failed login attempts should trigger temporary account lockouts to prevent brute-force attacks. Multi-factor authentication should be implemented wherever possible,
- **VPN Policy**
  The DGS can permit remote access to internal systems only via secure Virtual Private Network (VPN) connections, especially where remote work is available. These connections should be authenticated using multi-factor protocols and restricted to approved, managed devices. VPN usage logs should be reviewed regularly to detect anomalies,
- **Asset Management**
  The DGS should maintain an up-to-date asset inventory, linking each IT device

to a specific user. Access rights should be assigned based on job roles and promptly revoked upon changes in employment status. Asset audits should be conducted periodically to ensure alignment with internal controls.

Supplier and Vendor Risk Management
While evaluating third party risk management, it is critical to assess ICT type risks especially data-sharing related risks. Please refer to the TPRM part for further details.

The DGS should conduct **annual testing of its Business Continuity Plan** (BCP) **and Disaster Recovery Plan** (DRP). These exercises should simulate realistic disruptions and evaluate the DGS's ability to maintain critical operations, restore systems, and communicate with stakeholders. Test results should be documented and used to improve future preparedness.

Incident Response
The DGS should maintain an Incident Response Plan to promptly address ICT incidents such as cyberattacks, data breaches, or system failures. The plan must define roles, escalation procedures, and communication channels. Regular staff training and periodic testing of the plan are required. All incidents should be documented, reviewed for lessons learned, and, where necessary, reported to authorities and stakeholders.

Physical Controls
This control outlines the physical security measures that a DGS should implement to safeguard infrastructure, systems, and sensitive data. These controls form part of the broader internal risk management framework and support the DGS's mandate to operate with security, transparency, and resilience.

- **Office Physical Controls**
  To protect critical premises and sensitive operational areas, the DGS should implement layered and reliable office security infrastructure:
  - **Proximity Card-Based Access and Alarm Systems**
    The DGS can use electronic entry systems based on proximity cards to control access to offices and critical areas. These systems should be integrated with alarm features that trigger alerts in case of unauthorised attempts. Entry and exit logs should be maintained for audit purposes,
  - **CCTV Surveillance**
    The DGS can install CCTV camera systems in strategic internal and external office locations, including building entrances, server rooms, and document storage areas. These cameras should operate continuously, with video recordings retained in line with data protection regulations and used for post-incident reviews,
  - **Motion Detectors and Door/Window Sensors**
    To enhance physical security, the DGS can install motion detectors and door/window sensors in sensitive areas. These systems should be linked to the central alarm system to ensure prompt detection and response to any unusual activity, especially outside working hours,
  - **Biometric Access to Server Rooms**
    Access to the DGS's rooms containing sensitive documents or assets can be restricted using biometric systems (e.g., fingerprint or facial recognition). Only authorised personnel should have entry, and all access events should be logged and reviewed periodically to ensure compliance with access policies.
- **HR-Related Physical Controls**

These measures ensure that the DGS's employees manage physical security risks during their daily operations and interactions with sensitive data.

- **Segregation of Entry Rights**
  The DGS should implement role-based physical access controls. Employees should only have access to the specific zones necessary for their duties. Entry permissions should be reviewed regularly and promptly updated in the case of role changes or departures,
- **Working in Secure Areas**
  When DGS employees handle sensitive data, such as depositor records or financial system credentials, they should work exclusively in secure, access-controlled areas. These areas should be monitored and logged to prevent unauthorised access and to maintain the confidentiality of critical information,
- **Clear Desk and Clear Screen Policy**
  The DGS can enforce a clear desk and clear screen policy across all departments. Employees should store physical documents securely when not in use and lock their computer screens when stepping away from their desks. Periodic reminders and spot checks can support compliance with this policy.

- **Operational Physical Controls**
  This section covers how the DGS can manage and protect its assets, both on and off premises, throughout their lifecycle:
  - **Security of Off-Premises Assets**
    The DGS should ensure that any laptops or devices used remotely by employees are encrypted, password-protected, and monitored. Staff working offsite should adhere to strict security protocols, including connecting through VPN and using organisation-approved devices only,
  - **Usage of Storage Media**
    The DGS can prohibit the use of unauthorised mobile storage devices (e.g., USBs, external drives). Where mobile media is necessary, usage should be pre-approved, encrypted, and centrally tracked to prevent data leakage or loss,
  - **Equipment Maintenance**
    The DGS should ensure that all IT and operational equipment is maintained on a regular schedule. Maintenance should be performed by authorised technicians only, and all servicing activities should be logged for traceability and oversight,
  - **Secure Disposal of IT Equipment**
    When IT assets are no longer in use, the DGS should dispose of them through certified secure disposal processes. This includes physical destruction or certified data wiping of storage devices to eliminate the risk of data recovery. Documentation should be maintained for each disposal activity.

Technical and Operational Controls

This chapter defines the technical control mechanisms a DGS should implement to secure its IT environment, systems, applications, and network infrastructure. These measures are critical for ensuring service continuity, protecting sensitive data, and maintaining the integrity of internal operations.

- **Central Operation-Related Controls**
  The DGS should maintain a robust, centrally managed IT security infrastructure that proactively identifies, prevents, and responds to potential cyber threats:
  - **Endpoint Protection and Anti-Malware**
    The DGS should deploy a centrally managed endpoint protection system

across all user devices and servers. The system should provide real-time protection against malware, viruses, ransomware, and other forms of malicious software. Updates and threat definitions should be automatically deployed,

- **Firewall Operations, Web and Email Filtering**
  To control inbound and outbound traffic, the DGS can maintain enterprise-grade firewalls. Web access and email communications should be filtered to block malicious content, phishing attempts, and access to non-compliant or high-risk websites. Email attachments should be scanned for threats before delivery,
- **Security Event Management and Log Collection**
  The DGS should implement continuous monitoring of critical ICT systems and networks to detect anomalies and security threats in real time. Automated alerts help to ensure timely response to suspicious activities. The process should also collect, store, and analyse logs from critical systems. Monitoring processes should be periodically assessed and updated and reports should be reviewed regularly to address evolving risks,
- **Change and Configuration Management**
  The DGS should implement strict change management procedures for IT systems. All system changes, including patches, updates, and configuration changes, should be documented, tested, approved, and monitored to prevent disruptions or vulnerabilities,
- **Backup Management and Disaster Recovery (DR) Mirroring**
  Regular data backups should be performed by the DGS, with copies stored both onsite and offsite. A DR mirroring system should ensure that critical systems can be restored rapidly in the event of an outage or data loss. Backup restoration procedures should be tested periodically.

- **Network-Related Controls**
  To ensure a secure and reliable network environment, the DGS can implement layered network security protocols:
  - **Network Security and Protection of Network Services**
    The DGS should enforce strong controls over internal and external network connections. All network services should be secured through firewalls, intrusion detection/prevention systems (IDS/IPS), and encryption. Access to internal resources should be granted based on business needs only,
  - **Network Segregation (LAN and WiFi)**
    The DGS should segregate its networks by function and access level. Local Area Networks (LAN) used for sensitive internal operations are advised to be separated from guest or public WiFi networks. Administrative access should be further restricted and monitored.
- **Development-Related Controls**
  When developing or procuring custom applications or systems, the DGS can follow secure development standards to ensure resilience against software-related risks:
  - **Secure Development Lifecycle**
    The DGS should adopt a secure software development lifecycle, incorporating security requirements from the design stage through to deployment and maintenance. Developers and vendors should be required to follow secure coding practices,
  - **Testing in Development and Acceptance Phases**
    The DGS should conduct thorough security testing during development and prior to deployment. This includes code reviews, vulnerability scans, and user

acceptance testing. If development is outsourced, contracts must include strict security obligations. Development, test, and production environments must remain logically and physically separate to avoid data contamination and risk exposure,

- **Penetration Testing and Code Reviews**
  The DGS should commission regular penetration tests and stress tests to identify vulnerabilities in applications and systems. Independent code reviews should be performed for critical applications. All results should be documented and remediated before go-live approval.

Risk Management in HR Processes from ICT perspective
These suggestions outline the human resource-related risk controls a DGS can implement to minimise internal threats, ensure responsible hiring, and promote an organisational culture of risk awareness and compliance:

- **Preliminary Risk Profiling Before Onboarding**
  Before onboarding new employees, the DGS should conduct thorough risk assessments. This includes requesting criminal background check and requiring candidates the acceptance of the adopted code of ethics regarding their prior disciplinary issues and conflicts of interest., in compliance with the GDPR and applicable national regulations, as well as a declaration of acceptance of the DGS's code of ethics. These steps help mitigate reputational and operational risks,
- **Protection of Personal Data**
  The DGS should protect all personally identifiable information of its employees and affiliated individuals in accordance with applicable data protection laws. This includes securing digital and paper-based records, restricting access to authorised personnel, and using encryption where applicable. Regular data protection audits and staff training should reinforce compliance,
- **Development of IT Security Awareness Among Employees**
  To minimise human-factor vulnerabilities, the DGS should ensure all staff receive regular cybersecurity awareness training. This includes mandatory yearly testing and education sessions. Monthly newsletters should be distributed to keep employees informed about evolving threats such as phishing, ransomware, and social engineering tactics.

III. Governance, Risk Monitoring and Reporting

Effective risk monitoring and reporting are essential components of a robust Risk Management Framework within a DGS. Ongoing surveillance of risks and transparent reporting mechanisms enable early identification of emerging threats, ensure compliance with internal and external requirements, and support informed decision-making.
Risk monitoring must be continuous, structured, and tailored to the nature, scale, and complexity of the DGS's operations. The objective is not only to detect deviations from expected risk levels but also to ensure that risk exposures remain within the defined risk appetite and tolerance limits.

Risk Monitoring Activities

The DGS shall implement a systematic and proactive approach to monitor risk

exposures across all relevant areas, including but not limited to ICT risks, funding risks, operational risks, and SCV data quality risks. Monitoring activities should include:

- Regular collection and analysis of risk data from both internal operations and external developments (e.g., financial market movements, regulatory changes, technological advancements),
- Tracking of key risk indicators (KRIs) and performance against predefined thresholds, enabling the timely identification of emerging risks or deterioration of risk profiles,
- Periodic reassessment of risk exposure to ensure alignment with the DGS's risk appetite and to capture new or evolving risks,
- Continuous surveillance of control effectiveness, ensuring that risk mitigation measures are operational and effective,
- Incident and near-miss reporting to capture and analyse operational failures or disruptions that could inform future risk management actions,

Monitoring activities must be integrated into daily operations, supported by appropriate tools and systems, and adapted dynamically as risks evolve.

Risk Reporting Framework

Risk reporting ensures that the DGS's leadership, governance bodies, and relevant stakeholders have timely, accurate, and comprehensive information about the organisation's risk profile. The DGS shall establish a structured reporting framework that includes:

- Periodic Risk Reports: Regular reports to management and the Board summarising key risk exposures, incidents, control deficiencies, risk mitigation progress, and trends in risk indicators,
- Early Warning Alerts: Immediate notifications of significant risk events or breaches of critical risk thresholds to appropriate decision-makers,
- Thematic Risk Reviews: In-depth reports on specific risk categories or emerging risk areas (e.g., cybersecurity threats, liquidity stresses, operational vulnerabilities),
- Compliance and Regulatory Reporting: Fulfilment of all mandatory risk-related reporting requirements toward national or international supervisory authorities.

All reports must be accurate, objective, and actionable, and should provide both quantitative and qualitative analyses of the risk environment.

Responsibilities and Governance

- The Risk Management Function is responsible for the design, operation, and continuous improvement of the risk monitoring and reporting processes,
- The Executive Management must review risk reports regularly, challenge assumptions, and take appropriate corrective actions when necessary,
- The Board of Directors or equivalent governing body shall exercise oversight over the overall risk management process, ensure that risk monitoring is adequate, and that reporting enables strategic risk-informed decisions.

The DGS should also foster a risk-aware culture, encouraging all employees to participate in risk identification, escalation, and mitigation as part of their routine activities.

Through diligent risk monitoring and transparent reporting, the DGS strengthens its resilience, ensures compliance, protects its stakeholders, and maintains the credibility and trust essential to its mission.

IV. Key Risk Indicators

In order to have in place a performant risk management system, DGSs need to close the loop by establishing a risk monitoring and reporting framework.

Key Risk Indicators for DGS help assess the financial health, effectiveness, and potential vulnerabilities of the system that protects depositors in case of a bank failure.
To manage risks effectively, DGS must have KRIs across its activities. To ensure proactive risk management, it is important to define early warning and critical warning levels.

Annex 1. contains a proposed catalogue for keeping the KRIs up to date with clear roles and responsibilities.

Annex 2. contains a list of proposed indicators. **Each DGS should adapt its indicators to its own risk tolerance. The proposed limits can be used as benchmarks Moreover, the list of the KRIs provided are examples and the list is not exhaustive.**

V. Policy Review and Updates

In order to ensure the continued relevance, effectiveness, and compliance of the Risk Management Policy, the following framework governs its review and update process:

Frequency of Policy Review

The Risk Management Policy shall be formally reviewed at least once every 12 months. In addition, interim reviews may be initiated in the event of:

- Regulatory or legal changes affecting DGS or risk governance,
- Any initiative by a DGS to enhance or update the policy, including but not limited to developments arising from newly identified risks, lessons learned from banking crises, stress testing outcomes, or evolutions in risk management methodologies or practices.

Governance of policy amendments

All amendments to this policy must adhere to EFDI's governance principles:

- Proposed changes shall be prepared by members of the Risk Management Working Group,
- A preliminary review and validation shall be carried out by the Risk Management Working Group,
- Final approval shall be given by the EFDI Board Members.

Documentation and version control

Each version of the Risk Management Policy shall:

- Be assigned a unique version number and effective date,
- Be stored in the EFDI Risk Management Working Group media centre and made accessible to all relevant stakeholders.

A version control table shall be maintained within the document to record all revisions and corresponding validation dates.

*****

VI. References

- European Union's Directive 2014/49/EU on Deposit Guarantee Schemes (DGSD2),
- EBA Revised Guidelines on DGS Stress Tests (EBA/GL/2021/10),
- EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02),
- European Union Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),
- International Journal of Learning & Development ISSN 2164-4063 2013, Vol. 3, No. 3, Available: https://www.academia.edu/download/31621665/Ideololgy__Purpose__Core_Values_and_Leadership-_How_they_Influence_the_Vision_of_an_Organization.pdf
- ISO 31000:2018 – Risk management — Guidelines. ISO.org. International Organization for Standardization,
- ISO/IEC 27001:2022 International Information Security Standard, Guidelines. ISO.org. International Organization for Standardization,
- Compliance Risk Management: Applying The COSO ERM Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), November 2020,
- 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 (2024), available: https://www.efdi.eu/storage/2617371/download?refresh_at=1727778588

VII. Annexes

Annex 1: Key Risk Indicators Catalogue Template

Annex 2: Key Risk Indicators Examples