EFDI. EUROPEAN FORUM OF DEPOSIT INSURERS

Annex 2: Sample Key Risk Indicators for deposit insurance funds

This annex provides a selection of examples of Key Risk Indicators (KRIs) that DGSs may use to monitor and manage exposure to specific risks. The KRIs listed here serve as illustrative examples and are not intended to be exhaustive. Each organization should tailor its KRIs to reflect its unique risk profile, operational context, and strategic objectives. The indicators included highlight common metrics across the five risk categories to support proactive risk identification and informed decision-making.

Proposed financial risk indicators

Interest Sensitivity GAP. This indicator measures the mismatch between interest-sensitive assets and liabilities, reflecting the institution's exposure to interest rate fluctuations. A large gap can lead to earnings volatility and funding instability. As an Early Warning Threshold, we accepted 5% of capital ratio. If in the first stage, the gap increases above the 5% of the capital, mitigation action should be Implementing swap agreements to hedge against interest rate risks. The Critical Threshold is accepted to be the 7% of capital (in terms of available financial funds). In this Critical Stage, mitigation procedure can be utilizing public financial sources and internal financial statements to reassess exposures. Considering the effect of this ratio, it is recommended to be monitored at least monthly by the Risk - Finance team.

Currency Position. Evaluates the difference between foreign currency-denominated assets and liabilities to manage foreign exchange risk. Significant currency mismatches can lead to financial losses due to exchange rate fluctuations. The Early Warning Threshold is 5% of the capital (in terms of available financial funds). This means if the currency gap between liabilities and assets exceeds the 5% of the capital, swaps and forward contracts need to be employed in order to hedge against currency risk. The critical threshold is 7% of the capital. The critical stage mitigation policy involves adjusting currency exposure using internal financial reports and public financial sources. Consequently, this KRI should be monitored at least monthly, overseen by Risk – Finance departments.

Volatility of investment assets. Measures fluctuations in asset values, indicating potential financial losses due to market instability. If the change in the fair value of assets is more than 70-80% of the interest income of the portfolio, this indicates an *Early Warning Stage*, diversifying assets and prolonging investment maturities. If this value outbounds the critical threshold of 80-90% of interest income, then it is recommended to reasses the risk exposure using public financial sources and internal assessments. So, daily monitoring task should be assigned to the Risk team.

Value at Risk (VaR). Estimates the maximum potential loss in asset values over a given period, with a definied confidence level - typically between 95% and 99% - due to market volatility. A high VaR indicates increased exposure to financial losses. At an early warning stage, when this indicator is above 0.5-1% of the total asset value, it is expected to diversify assets and extend investment maturities. If this indicator is greater than 1% of the total asset value, utilize public financial data sources and internal statements to adjust strategies. Weekly to monthly monitoring should be held by the Risk team.

Current Ratio. Measures an institution's ability to meet short-term liabilities with available current assets. A declining current ratio signals a liquidity stress. When this liquidity KRI falls below 1.5, the institution should start strengthening cash reserves and optimizing working capital. At a critical stage, when this ratio is down to even 1.2 level, it is expected securing emergency funding and renegotiating short-term liabilities. To avoid

delays in the response of crisis time, a strict monthly tracking should be managed by Risk & Treasury teams together.

Contract Provision Risks. Assesses the adequacy of contract provisions in agreements with third parties, suppliers, and service providers. Poorly defined contract terms may expose the institution to financial and legal risks. Increased contract disputes or delays in service delivery could be a warning indicator. Strengthening contract review processes, ensuring alignment with regulatory requirements are essential in this step. In a more serious stage, legal action or financial penalties arise from contract failures, legal intervention, renegotiation of unfavorable contract terms could be applied. Quarterly reviews are conducted by the Legal & Compliance teams and reported to the Risk team.

Proposed third party risk indicators

- **Percentage of Critical Services Dependent on a Single Party (%)** – Measures concentration risk in IT, data processing, or payouts.
- **Number of Alternative Providers Available for Critical Functions** – Assesses diversification in vendor sourcing.
- **Service Level Agreement (SLA) Compliance Rate (%)** – Percentage of third parties meeting agreed performance levels (e.g., system uptime, payout processing times).
- **Average Downtime of Third-Party Services (Hours/Days per Incident)** – Tracks system outages or performance failures affecting the DGS.
- **Number of Data Breaches Linked to Third Parties** – Tracks unauthorized access, hacking attempts, or data leaks at vendors.

Proposed SCV Quality risk indicators

To monitor data quality and consistency, the DGS should track risk indicators such as:

- Non-standardized Data Format Rate
- Duplicate Customer Record Rate
- Percentage of Missing or Incomplete Records
- Error Rate in Depositor Name Matching
- Mismatch Rate Between SCV Files and Core Banking Systems
- Incorrect Account Balance Rate
- Errors in Deposit Insurance Calculations
- Inconsistent Data Across Multiple SCV Submissions

By monitoring these indicators, the DGS can proactively identify deficiencies and work with banks to remediate issues before a payout situation arises.

Key risk indicators for monitoring secure transfer include:

- Number of Unauthorized Access Attempts on SCV Data
- Percentage of Files with Encryption Errors
- Audit Trail Completeness
- Data Corruption Issues
- SCV File Submission Compliance Rate
- Time to Generate and Submit SCV Files
- Percentage of Files Rejected Due to Errors
- Time Taken to Correct and Resubmit SCV Files

Proposed reputational risk indicators on Communication & Public Confidence

Reputational Risks. Measures public perception and reputation through customer feedback, complaints, and social or public media sentiment analysis. A surge in negative feedback can damage trust and brand value. Increasing volume of negative feedback or complaints could be a warning sign to address customer concerns proactively, enhance communication strategies. Without consistent prevention methods, significant reputational damage and loss of customer confidence could emerge. Mitigation strategies in this stage are launching damage control campaigns, engaging in public relations efforts, and regulatory reporting if required. Real-time monitoring, managed by the Public Relations & Customer Service teams, is essential. Additionally, regular reporting should be implemented for the Risk team.

A lack of clear **public awareness and stakeholder communication** can lead to panic, misinterpretations, or inefficiencies.

- **Public Awareness Level (%)** – The percentage of depositors aware of the DGS coverage and rules (measured through surveys).
- **Customer Complaint Rate (%)** – Tracks complaints from depositors regarding payout delays, errors, or unclear processes as a *percentage of total depositors serviced*.
- **Accuracy of Public Information (%)** – Ensures that official communications (website, brochures, etc.) provide up-to-date and correct information.
  Possible inputs:
  - *Number of outdated or incorrect references remaining (or corrected) compared to outdated or incorrect references previously identified.*
  - *Total brochures (or means of communication in general) with outdate or incorrect info compared to total brochures (or means…) reviewed.*
- **Number of False News or Misinformation Cases** – Measures incidents where inaccurate information about the DGS causes public confusion or panic.

Proposed ICT risk indicators

Number of Cyber Threats. Tracks the frequency and severity of cybersecurity incidents, including phishing attacks, malware intrusions, and data breaches. An increasing number of cyber threats indicates vulnerabilities in IT infrastructure. Early warning indicators are a noticeable increase in the number of threats. Prevention methods include enhancing cybersecurity protocols and increasing employee awareness training. In a more critical stage, in case of successful breaches or operational disruptions, an immediate incident response, system-wide security upgrades, and regulatory reporting are required. Continuous monitoring should be conducted by the IT Security team and reported to the Risk & Compliance Teams.

- **Number of Data Breaches or Cybersecurity Incidents** – Tracks hacking attempts, ransomware, or unauthorized access to sensitive depositor data.
- **System Recovery Time After Cyber Incident (Hours/Days)** – The time needed to restore systems after a cybersecurity breach or IT failure.
- **Backup System Reliability (%)** – The effectiveness of data backup and recovery processes.

  Possible inputs:

  - *Number of cases where data recovery was unsuccessful in relation to the total number of cases where data recovery was required (in real life or during tests)*
  - *Percentage of users that consider data backup and recovery processes are ineffective (through surveys).*

- **Number of Ticket Issued** – Daily operational distress