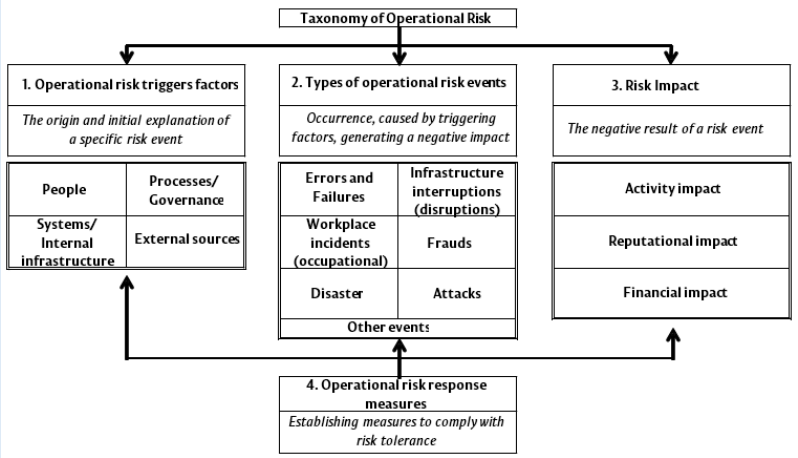
Extract - Unofficial translation

OPERATIONAL RISK MANAGEMENT IN THE NATIONAL BANK OF MOLDOVA

Operational risk	It is part of the range of non-financial risks faced by a central bank. Specifically, issues related to human factors, information integrity, physical security, and business continuity fall under the broad topic of operational risk management. Considering the need for continuous improvement in risk management in general and operational risks (OpR) in particular, the central bank is committed to enhancing its own capabilities and implementing a robust operational risk management framework.
Operational risk management framework within the NBM (Framework ORM)	it is developed as the main internal regulation for organizing and establishing the process of identifying, assessing, addressing, monitoring, and reporting operational risks (OpR), as well as for setting up and maintaining the operational risk management system (ORMS) within the National Bank of Moldova (NBM).
Terms and definitions	
Operational risk	is a potential financial, activity and/or reputation impact on the bank, arising from or conditioned by inadequate or failed internal governance activities, business processes, people, systems, infrastructure, legislation, communication, or changes in the external environment
Coordinator of the operational risk management system	Strategy, Organization and Human Resources Department through the Internal Methodology and Risks Division.
Operational Risk Management	a continuous and systematic process, with defined responsibilities, for identifying, assessing/measuring, monitoring, and taking actions to control or mitigate risk exposure, as well as reporting the outcomes of these activities to the Executive Board and the Supervisory Board.
Governing bodies of the NBM	Supervisory Board, Executive Board of the NBM
The purpose of the Framework	to establish a coherent system of policies and procedures at the NBM level for a unified understanding of the operational risk management process. This includes providing a common language and a clear definition of operational risk, setting principles, and outlining how operational risks should be identified, assessed, controlled/mitigated, monitored, and reported, as well as defining the respective lines of responsibility
The basic objective of the Framework	to develop an effective operational risk management system applicable for identifying and controlling risks, quantifying and managing their impact, with the aim of ensuring the optimal execution of NBM processes, as well as achieving the mission and strategic objectives of the NBM
The field of application	all hierarchical levels and business processes of the NBM.
Basic elements of the operation, monitoring and continuous improvement of the ORMS	• taxonomy of operational risk • risk matrix • risk appetite • risk tolerance • risk profile

Taxonomy of operational risk

based on three interdependent components: *fundamental causes* (risk trigger factors), *risk events* and *the impact of risk*



Risk matrix

a well-structured tabular tool used by each subdivision during the self-assessment of operational risks (OpRisks) related to processes. It serves to document, manage, and report OpRisks, specifying triggering factors and the type of risk event, describing the impact on objectives, control measures, and the levels of inherent/residual/forecasted risk (risk category)

Risk appetite

the maximum amount and type of risk that the bank is prepared or able to assume, accept or tolerate in achieving the bank's fundamental objective (mission) and core functions.

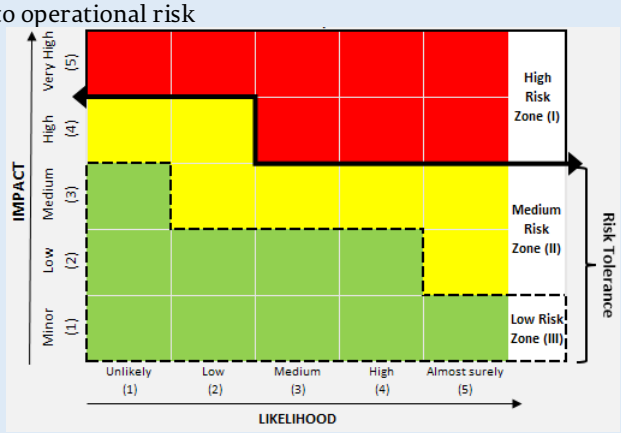
Risk tolerance

the amount or level of residual operational risk (the "quantity") which the bank is willing to bear or to be exposed (the degree of variation accepted) at any time **after the inherent risk treatment**, in order to achieve the objectives. In the NBM risk profile

Risk tolerance = Appetite for risk

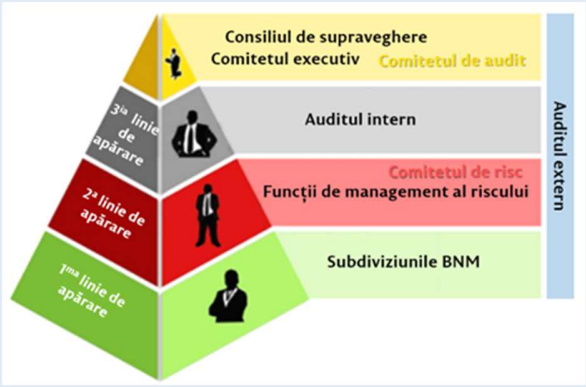
Risk profile

a *"heatmap of risk"*, it is a chart that translates the prioritized qualitative assessment of the specific risks of the bank's activities into quantitative terms and presents a ranking of exposures to operational risk



Zone I high risk severity *(red zone)*. Includes high risks, which are above the bank's risk tolerance and require immediate decisions, with treatment measures developed by the risk owner subdivision, approved by the Executive Board. In the absence of effective risk treatment measures, the Executive Board accepts by decision, based on a solid justification, or rejects the risk.

Zone II ← medium risk severity *(yellow zone)*. Includes medium risks, requiring additional treatment or monitoring measures, developed by the risk owner subdivision, approved at the Risk Committee level. In this zone, active monitoring of both risks and their treatments is required.

	Zone III ◄— low risk severity *(green zone)*. Low risks do not require additional risk treatment measures and are considered to be accepted by default. A key risk area, where only periodic monitoring of risks and the effectiveness of their treatments is required
Governance of the OpR	is based on the classic model *"three lines of defense"* in risk management, where each of the lines plays a distinct role in the governance of the NBM  **The first line of defense** is *the line managers, the NBM subdivisions*, who are the "owners" of the risks. They are responsible for identifying and managing operational risks inherent in the business processes. **The second line of defense** is represented by the structures dedicated to *operational risk management: the Risk Committee*, support functions – the *risk management function* (the ORMS Coordinator) and the business continuity and information security management function. Each of these functions is independent of line managers, is responsible for ensuring the OpR management framework, organizing the process, independent supervision and reporting of OpR management activities at the level of the entire bank. **The third line of defense** *provides independent assurance* and is represented by *internal audit*. Internal audit provides for management and line managers an independent, reasonable assurance as to the adequacy and effectiveness of governance, risk management and internal controls, including how the first and second line of defense achieve the risk management objectives.
	The external audit provides independent reasonable assurance that the financial statements present fairly the position and the financial performance according to the generally accepted field standards, assesses the internal control system for conducting audit procedures, but without expressing an opinion on its effectiveness. The external audit is carried out in accordance with the requirements of the Law on the NBM **The governing bodies** of the NBM implement the model of the three lines of defense and ensure that it reflects the risk management process and internal control of the bank.
The ORMS governance model in the NBM	*is a distributed one*, where each structural subdivision is responsible for identifying and managing the risks specific to its activity, and the ORMS Coordinator provides methodological support, monitors the application of regulations and report at consolidated level on self-evaluation result OpR.
Roles and responsibilities within the NBM ORMS	**Supervisory Board** • establishes ORM standards in the NBM by adopting this Framework; • defines and approves the bank's tolerance for operational risk; • promotes and monitors the development, maintenance, review of the Framework; • oversees the functioning of ORMS in the NBM, compliance with the approved level of tolerance to risk; • examines and approves the risk profile determination methodology and the annual operational risk management report; • ensures the resources required for effective OpR management; • promotes the development of an active risk management culture at all levels within the NBM

Executive Board

- ensures the implementation of the Framework and related procedures of ORMS and adopts decisions related to ORM;
- examines and approves the risk profile with the overall risk matrix and significant changes in risk levels, new risk zones;
- examines and approves the risk management measures in the red zone submitted by line managers as soon after identifying the risk;
- approves acceptance of risks in the red and yellow zone and related conditions;
- ensures the resources, training and tools required for effective OpR management within the approved NBM Budget;
- develops and promotes risk management culture with ethical values and integrity of personnel;
- ensures the management of the risk for the major projects carried out in NBM

Audit Committee

In the context of the ORM system, in accordance with the powers laid down in Article 28 of the Law on the National Bank of Moldova, and the provisions of the Regulation on the functioning of the Audit Committee of the National Bank of Moldova (DSB no.15 of 22.12.2016), the AC's role consists in:

- the efficiency supervision of the operational risk management system;
- the overall supervision of the effectiveness and adequacy of the ORM framework at NBM level;
- the adequacy and opportunity supervision of procedures adopted for monitoring and controlling exposures to OpR in general;
- the implementation supervision of recommendations made by the external/internal audit related to high risk findings;
- making recommendations to the NBM governing bodies, as appropriate, supporting an environment that promotes integrity and control

Risk Committee

- monitors and ensures the effectiveness of the regulatory framework of ORM in the NBM, including the tools, methodologies, procedures and reports required to operate the framework, and assesses the need to update them (no more than once every three years), considering the suggestions made by the ORMS Coordinator and the evolution of the methodologies applied in ORM;
- discusses and agrees on policy proposals on ORM, which should be presented to the NBM governing bodies;
- endorses the risk profile for submission to the Executive Board for approval;
- approves the proposed treatment measures for the response to the risks in the yellow zone;
- assesses and notes through the minutes:
  - *as soon* as they are reported - the risks in the red zone, and
  - *quarterly* – by the risk profile, developed and presented by the ORMS Coordinator;
- assesses the annual report on ORM in the NBM developed by the ORMS Coordinator and gives an opinion to be submitted through the Executive Board to the Supervisory Board.

The NBM's subdivisions (with line managers)

- identify, assess and report **annually** (in coordination with the Executive Board member patron of subdivision) to the ORMS Coordinator the operational risks related to the business processes, in the annual **risk self-assessment exercise** or, if necessary , more often, by filling in the associated risk matrices or informing about the lack of change;
- determine the ex-ante response to OpR in the yellow and red zones, in coordination with the Executive Board member patron of subdivision; accepts the risks in the green zone;
- **immediately report the high risk** (red zone) identified and formulate measures to treat to treat them to the Executive Board for approval, informing Coordinator ORMS;
- continuously monitor the risks in the three risk zones of the managed processes, maintain effective internal controls, performs risk control procedures on a daily basis and proactively considers the consequences of risk events;
- report by EDMS **quarterly**:
  - to the ORMS Coordinator status and changes in OpR level in the red zone;
  - the implemented red and yellow risks treatment measures - through the process of quarterly planning and reporting of subdivision activity.
- report and manage incidents according to internal regulations and considers the information resulting from the review of the OpR self-evaluation;
- ensure the regulation of the control measures applied for the management of the OpR specific to its activity by including them in the internal regulations related to the relevant business processes.

The responsible for OpR within structural subdivisions

- planning and organizing the self-assessment process;
- understanding and transfer of knowledge related to the ORM methodology within the subdivision;
- establishing and collecting, together with the process manager, the KRI for the processes, the owner of which is their subdivision and annual reporting to the ORMS Coordinator in coordination with the line manager;

	• communication with the ORMS Coordinator on all aspects related to the responsibilities of ORM subdivision **The ORMS Coordinator** • facilitates and coordinates the ORM process in NBM, develops and manages ORMS, based on the NBM process management system; • ensures the establishment and development of the OpR management; • establishes and develops the (self) assessment methodology (procedures) of OpR on business processes; • facilitates OpR self-assessment procedure, performs the analysis and coordination of the risk matrices completed by the structural subdivisions, cooperate and assist in their completion; • reports immediately to RC the risks materialized in the red zone, communicated by subdivisions; • collects and analyzes quarterly risks and their evolution from the red zone and the new high risk zones identified by subdivisions and, report with the same frequency the results and risk profile to the Risk Committee; • submit to the Risk Committee for approval treatment measures, established by subdivisions for the risks detected in the yellow zone, at the next quarterly meeting, from reporting to ORMS Coordinator; • develops the bank's risk profile and dashboard • elaborates the annual report of ORM in NBM and performs the consolidated annual report on the OpR of the NBM, with the risk profile of the bank and the dashboard, to the EB, subsequently submitted to the SBC for examination and approval, shall forward to the internal audit for information the annual ORM report; • performs the monitoring and control of the risk response established by the subdivision and adopted at that level for the risks in the yellow and red zones, taking over the measures from the quarterly activity plans of the subdivisions; • monitors incidents (including those avoided), reports consolidated annually to the EB and quarterly to RC, information about incidents with high and very high impact, on processes; **The Business Continuity Management and Information Security** • the elaboration and implementation of standards, policies and response plans for incidents that disrupt or threaten any operational function within the NBM and the resumption of essential operational functions within the pre-established deadlines; • organizes and facilitates the process of risk assessment of process continuity, IT and information security by business process owners; • performs the analysis and coordination of continuity matrices completed by subdivisions, cooperates and assists the subdivisions in completing them; • communicates to the ORMS Coordinator the results of the continuity, IT, and information security evaluation; • quarterly and yearly collects information related to the continuity, IT and information security risk management from NBM subdivisions, analyzes changes in risk levels and new risk zones identified during the year and communicates to the ORMS Coordinator to adjust the risk profile; • maintains database of incidents and monitors the incidents management process; • manages major incidents and exceptional situations of continuity and security of information, products and avoided **Internal Audit** • analyzes and evaluates ORMS; • reports to the Audit Committee and Supervisory Board of the NBM the results of the assessment of the ORMS.
The main stages of the operational risk management process	*Identification of risks;* *Risk assessment* *Response to risk* *Monitoring* *Risk reporting* The ORM process is preceded by a description of the business processes carried out by SOHRD in accordance with the *General Framework on the activity process management system within the National Bank of Moldova*.
The risk self-assessment procedure	consists of the identification of OpR and the assessment by the process owner subdivision together with the participants in the process, where appropriate , the likelihood and impact of inherent OpR, the effectiveness of existing control measures (regulatory framework, control procedures), the residual risk assessment and the establishment of additional risk management / prevention measures for their management up to the residual risk according to the established tolerance.

Risk identification	is carried out by the NBM subdivisions in the self-assessment procedure. When identifying, the NBM subdivisions take into account both the type of the event and the internal factors (such as the bank structure, the nature of the bank's activities, the quality of human resources, the organizational changes, the fluctuation rate of staff, etc.) and external factors (such as changes economic, political, technological advances, etc.), which could affect the achievement of the objectives. Usually, the risks are identified and defined in relation to the objectives that may be affected.
Risk assessment	NBM subdivisions identify and assess risks for each process that contribute directly or indirectly to the bank's performance and /or achievement of strategic objectives. The NBM subdivisions perform the risk assessment in the risk matrix in terms of likelihood and severity of impact. The evaluation consists of the following steps: - assessing the likelihood of materialization of the identified risk; - assessing the impact if the risk materializes; - assessing risk exposure as a combination of likelihood and impact (risk level determination). Operational risks are divided into three groups in terms of **impact type**: *Impact of Activity* – affecting strategic objectives, projects, processes, operations, including related to human resources, information, systems, infrastructure and legal operations. *Reputational Impact* – impairment of public confidence in the bank's performance, negative reaction of the media, third parties, customers; *Financial Impact* – affecting the effectiveness of process objectives with/or generating financial losses: costs of changing/revising activities or correcting damages, penalties, interruption of processes etc. In order to assess the likelihood and impact of risk, the NBM uses a scale of five levels *(Annex),* as follows. *Probability* of the risk event: 5 – almost certain; 4 - high; 3 - medium; 2 - low; 1 - unlikely. *Impact* of risk: 5 – very high, 4 - high, 3 - medium, 2 - low, 1 – very low.
Risk response	After identifying and evaluating the inherent risks, it is necessary to determine by subdivision the residual risk response for each OpR. The risk response is set to reduce the deviation exposure to risk to the risk tolerance through one or more of *the risk response strategies (options)*: ➢ *avoid the risk/refusal* – eliminating activities (circumstances) that generates risks; ➢ *risk mitigation* – procedures to mitigate the risk; ➢ *transfer (outsourcing) risk* – the use by the bank of an external supplier to carry out activities on a contractual basis in order to achieve the bank's objectives. The bank remains responsible for managing OpR of outsourced activities; The outsourcing of the risk and, implicitly, of the activity is approved at the level of the Executive Board through the draft estimate of expenditure and/or investment allowances, submitted for approval to the Supervisory Board. ➢ *risk acceptanc*e – intervenes when the risks are assumed or when a risk response strategy is not possible; ➢ *risk follow-up/monitoring* – is the risk acceptance condition of maintaining ongoing supervision. Follow-up involves a delay in taking control measures until the circumstances increase the probability of materializing the OpR underlying this treatment and changing the response strategy

Monitoring	risk monitoring is carried out by the NBM subdivisions, for: - reflecting changing circumstances that favors the emergence of risks, maintaining the current risk profile; - obtaining assurance on the effectiveness of ORM and identifying the need for further measures; - identifying new OpR zones or events in a timely manner. Annually, under the self-assessment procedure, subdivisions review in risk matrices: risks grouped by triggering factor, event type, impact and probability, risk category, response to risks as well as response strategies with additional control measures, depending on the zone. Revision of OpR through self-evaluation is performed on every significant change in the process or occurrence of a high and very high impact. For risks in the *red zone*, their review is performed *quarterly*. The monitoring process will be completed with a reporting activity to the Risk Committee and the Executive Board, depending on the residual risk level. After the implementation of the risk treatment measure, the assessment procedure will be repeated by subdivision immediately (in case of residual risks in the red zone) or to the periodic assessment of risks in the yellow and green zones.
Reporting	*The purpose* of risk reporting is to ensure that all levels of management (from the governing bodies of the NBM to the Heads of Subdivisions) are informed of the: - fficiency and stage of the risk management process - respecting the bank's risk tolerance - main risks and proposed response actions - significant risks materialized - changes in the risk profile The ORMS Coordinator groups the identified and assessed risks of subdivisions on business processes, according to risk exposure and forms the bank's risk profile. *The object* of the reporting process is the risks in the yellow and red zones of the risk profile and all incidents with a high and very high impact, with priority for urgent and high resolution The results and data for: i) the self-assessment, ii) the information reported by subdivisions on the occurrence, preservation or modification of the OpR status in the red zone, iii) the incidents with high and very high impact, registered in EDMS, and iv) rapid scan of OpR, are consolidated by the ROpMS Coordinator in the General Risk Matrix, risk profile and dashboard for further reporting to the Risk Committee, Executive Board and the Supervisory Board, with new/improved control proposals if deemed necessary. The risk profile is reported quarterly to the Risk Committee, the dashboard - annually to Risk Committee, Executive Board and Supervisory Board *Annually*, the ORMS Coordinator will present to the Executive Board the annual report of ORM in NBM – the dashboard and the risk profile, which will be subsequently submitted to Audit Committee for information (via IAD) and Supervisory Board for approval. *The general communication* on how to manage operational risks in the NBM will be made through the annual reports of the NBM, published on the official website of NBM
Development and transfer of knowledge	is a continuous process that takes place during all phases of the ORM process. The Bank keep up with the evolution of best practice in OpR management through contacts with central banks, financial institutions, and profile literature. The NBM is a member of the International Operational Risk Working Group, capitalizing on the

	knowledge distributed through it. At the same time, the NBM contributes to its work by developing and conducting studies, participating in the research of other central banks and expert groups for organizing the annual IORWG conferences. SOHRD performs the *transfer of knowledge* during the working sessions with the operational risk officers of the NBM subdivisions. It also exchanges knowledge of line managers on risk management initiatives within subdivisions. Knowledge transfer sessions are mandatory.
ORMS maturity	reflects the degree of development (complexity, efficiency, performance) of the methods and means applied in operational risk management in the institution and is measured by comparison with the maturity *model of the operational risk management system.* Maturity assessment is performed on *five categories:* 1) Risk culture: values, norms and behaviors shared by all members of the institution, especially members of the governing bodies. 2) Organization: structure of ORM governance. 3) Risk reporting: the content and frequency of risk reports and beneficiaries. 4) OpR management process: ORM framework, from goal setting to continuous OpR monitoring. 5) Application domain (scope) of ORM and results: the link between risks and decision-making, especially in business units (subdivisions). Determining the maturity level of the ORMS within the bank it occurs by aggregating individual indicators obtained from the evaluation of those 5 categories. The model distinguishes **five maturity levels** of operational risk management: 1. *Initial* *2. Basic* *3. Defined/Managed/Developing* *4. Advanced* *5. Mature* The ORMS Coordinator applies the maturity score set by the IORWG (annual) to assess the current maturity level of ORMS, but also to define its development objectives. The results of the assessment are included in the annual report on ORM presented to Risk Committee, Executive Board and Supervisory Board.

Annex. OpR assessment based on probability and impact

LIKELIHOOD [1]*		IMPACT[2]**	Impact on business objectives ** *Effectiveness*: *the ratio between the result obtained and the planned target*		Reputational Impact **					Financial Impact** *Efficiency*: *the ratio between the result obtained and the resources used*
Likelihood level Criteria	Frequency of events		Ability to perform the basic tasks of the NBM and / or strategic objectives	Market reaction (triggered by NBM)	Duration of impact on public confidence	Source credibility and severity of opinion	Media coverage (duration, geography, character)	Subject to criticism	Visibility (importance) of targeted persons	Financial losses, direct or indirect
1p	2p	1	2a)	2b)	3 a)	3 b)	3 c)	3 d)	3 e)	4
Almost certain (5)	Every year or more often	Very high (5)	● Failure to fulfill basic duties	● Undesirable side effects of the market with significant movements exceeding the 1-week period	● Credibility affected long-term (> 3 years)	● Series of information and / or very negative opinions, from credible, verified sources.	● More than 1 month. ● International media coverage including press, TV and radio	● Basic tasks of NBM	● Governing Bodies (Multiple Members)	● Exceeding 1,000,000 lei
High (4)	Once every 1-2 years	High (4)	● Partial failure to achieve basic or ● Total failure to achieve strategic goals	● Undesirable side effects of the market with significant movements over the 1 day - 1 week period	● Credibility affected in the medium term (1-3 years)	● Negative information and / or opinions from credible sources	● 1 week to 1 month ● Media coverage in the press, TV and radio with national coverage, and media coverage in most internationally recognized newspapers	● Published Strategies	● One of the members of the governing bodies	● In the range of 100,000 to 1,000,000 lei inclusive
Medium (3)	Once every 2-5 years	Medium (3)	● Unsatisfactory quality or significant delays in fulfilling basic tasks or partial fulfillment of strategic objectives	● Market irritation and undesirable market movements over a day	● Credibility affected in the short term (3 months-1 year)	● Negative information and / or opinions	● 3 to 6 days ● Media coverage in the press, TV and radio with national coverage.	●Governance and support functions	● Superior Management (subdivision heads) of the NBM	● Framed within the limits of 10,000[3]*** to 100,000 lei inclusive

[1] * In the past, observable events in your organization or elsewhere, if applicable to your organization.

[2] ** The evaluation should consider whether a risk event is repetitive and therefore leads to a cumulative impact.

[3] *** For amounts higher than MDL 10,000, in agreement with the BFAD, the draft of the DEB on the change in the statement of expenditure for the current financial year.

Low (2)	Once every 5-10 years		**Low (2)**	● Basic attributions and strategic objectives can be further achieved, however the internal expectations of the NBM are not met due to a delay in delivery or quality deterioration	● Temporary market irritation and undesirable limited market movements over a day	● Credibility affected between 1 week and 3 months	● Ad-hoc negative statements / statements	● 1 to 2 days ● Media coverage in one or several nationally recognized newspapers	● Issues related to NBM litigation / issues / to some NBM employees	● Focus on the NBM	● Framed within the limits of 1,000 to 10,000 lei inclusive
Unlikely (1)	More rarely once every 10 years		**Very low (1)**	● Operational objectives, affected business processes, however, basic tasks or strategic objectives are not affected	● No significant market reaction	● Credibility affected for less than 1 week	●Unconfirmed rumors, affirmations and / or opinions	● A negative and unfounded report in the media	● Vague or in error problems related to NBM employees	● Any worry / concern expressed internally	● Up to 1,000 lei inclusive