INTERNAL AUDIT IN BANKS: CHALLENGES FROM THE RUSSIAN/UKRAINIAN CRISIS

THOUGHT PAPER

MARCH 2022

INDEX

1. Purpose of the document

The current crisis is posing difficult challenges to the Banking System, which is requested to rapidly adapt and cope with fast moving regulations and market developments.

A Banking Group risk profile can potentially be impacted on a wide range of drivers: business, regulatory, country, credit, liquidity and financial risk, operational/continuity (among which IT and cybersecurity, physical safety), fraud risk and reputational risk.

The purpose of this document is to define what role should be played by Internal Audit (IA) in the current situation to meet the expectations of its stakeholders, including Board members, Top Management and Regulators, as a third line independent control function and how this role must be carried out.

We start from some general remarks about IA role in these circumstances:

- IA should strengthen and focus its assurance and advice role of independent internal advisory during the crisis, helping the bank to build up, as soon as possible, the internal framework allowing a proper management of the crisis

- IA should be adaptive to the circumstances and quickly responding to adjust the audit plan, in case deemed necessary

- IA must be involved in the process of dealing with the crisis from the very beginning and at all relevant organizational levels. Only in this way it will be possible for IA to give its independent assurance, in an effective and timely way, that all relevant information is properly collected and reported

- IA should be ready to frequently report to its stakeholders: Board, Top Management and Regulators about the effective management of the crisis, on timely resolution of problems and proper escalation

- IA should verify in due time (ex post) the implementation of the internal framework defined by the Bank to manage the crisis in order to provide independent assurance to the Board

In the next section, IA contribution will be discussed along with a synthetic overview of the steps that a diversified Banking Group must take to manage the crisis effectively.

2. Crisis Management Steps and Internal Audit Contribution

2.1 Activation of Group Crisis Management and assessment of the Group direct involvement – operational Risk Exposure

First step for the Group should be an assessment of its physical direct involvement in the crisis.

This assessment should be made with reference to the geopolitical extension of the Group, considering the existence of subsidiaries and/or branches inside the country mostly impacted by the crisis (Ukraine and Russian Federation, the surrounding countries, etc.).

Key Risks: Business Continuity, People Safety, IT and Cyber-security

Main Actions and IA contribution

Operational resilience Crisis Management should be activated. Business Continuity Unit must quickly prepare a complete picture of Group **physical presence** in the countries involved in the crisis, with the support of Human Resources, IT and Logical/Physical Security structures. It should contain the perimeter exposed, a list of assets, the type of risk and the actions taken/in launch, with any other business related (points of attention, possible consequences).

Regarding **people safety**, is extremely important to evaluate and provide economic (salary paid in advance for example) and logistic support (moving, repatriation, emergency communication channels) to employees located in countries impacted by the war.

Appropriate actions should be put in place to ensure the operational effectiveness of the Business Continuity (disaster & recovery) of local HQ and branches: i) Offices and ATMs closure (also partially), ii) remote working adoption, iii) data center backup and data archiving in a secure place, iv) identification of key local staff to manage the crisis.

Quick actions should be activated also on **cyber** topics. First, it is necessary to evaluate whether to isolate local information systems from Head Office and from other countries, in order to limit the surface of a possible attack. Security Team must increase cyber alert, threat monitoring and other protection countermeasures (mail traffic, for example). Banks should also map their communication networks to make sure that, where they are routed via the conflict impacted region, alternative routes with sufficient capacity are available. Further, if any data is travelling unencrypted through conflict impacted regions this should be addressed as a matter of urgency. The importance of "Knowing your employee", including their access rights, also increases in importance, as there may be various attempts to target and influence employees (particularly the ones having roots in the countries involved in the war) resulting in cyber security misconduct.

Finally, organizations with direct links to Russia and Ukraine and impacted countries may also face significant **supply chain risks** due to material shortages, capacity constraints and business continuity, especially in IT providers (e.g. technical, network and cloud services). Several Companies based in Ukraine and Russia have ceased or suspended their production. The dedicated functions should consider how supply chain risks will affect the Company ability to deliver or receive ICT services (third parties' risk). For example, IT or cloud providers should consider the adoption of their backup and recovery

solutions, in order to deliver the services from systems or countries not impacted by the war.

IA must follow and check the correct activation of these actions, ensuring the tracking of all events and the existence of recovery procedures to be triggered when possible.

2.2 Clear picture of all sanctions and restrictions Groupwide – Sanctions and Reputational Risk exposure

A clear and complete up to date picture of sanctions and restrictions for each of the relevant jurisdictions and business in which the Group is active must be prepared. Clear internal rules to comply with the new sanctions must be issued. The picture is also an input to the evaluation of business risk (see next).

Key Risks: Sanctions, Compliance and Reputational

Main Actions and IA contribution

Internal rules should be prepared under the responsibility of the relevant internal functions (Compliance/AML, supported by Legal) and kept updated. A picture, containing a clear description of the nature of the **sanctions** and their implications for the bank, as a lender and as a regulated intermediary providing different kinds of financial services, should be made available as soon as possible to all interested functions, and kept updated. All significant update must be properly circulated.

Rules should be explained in clear operational instructions. Often it is worth organizing training sessions for the staff. An advisory technical team should be created to deal with possible interpretations of different regulatory frameworks arising from the operational network.

Reputational exposure depends on many variables (see also under). Failing to comply with rules issued by authorities exposes the Group to sanctions risk and to reputational risk.

IA should monitor/audit that fast-changing rules are properly managed and implemented in the Group monitoring framework, with clear roles and an effective internal control framework.

2.3 Assessment of the Group business exposure – Business and Country Risk Exposure

All relevant **business units impacted** by sanctions/restrictions or correlated with the countries involved in the war should be identified. For each of them, key **exposures** and **flow data** must be clearly identified and reported.

In typical large diversified Group main, impacted business units are:

Lending, Proprietary Investments, Client Investment Management, Transactions Services.

Key Risks: Business, Country, Credit and Legal

Main Actions and IA contribution

For each business lines complete information must be available on existing exposure and flow of business. For both, clear instructions must be provided. Operational task force and communication channel must be opened to solve special cases and escalating main issues (see also par. 2.5). **IA** must verify if blocks and rules are properly applied and controlled. **IA** should monitor

that actions decided are put in place in a timely manner, supported by guidance to business lines.

Lending

A thorough assessment of the credit lines towards customers based in countries impacted by the crisis must be prepared (e.g. Russian Companies and Counterparties controlled by Russian entities: **'direct' credit risk**), including undrawn amount of committed lines.

A list of due amounts from these clients must be available and regularly updated. Regulations about payments must be carefully analyzed and consequent approach evaluated by competent functions. Legal advice (internal vs external) could be necessary to manage specific cases.

A re-assessment of credit exposures based on updated ratings should be implemented and then, in a following phase, an evaluation of any additional **provisioning**.

Credit assessment should concern also the clients with high import/export relationship with Russia and Ukraine and correlated areas (**'indirect' credit risk**) to discuss possible problems in the supply chain and, more in general, in the rising of prices in energy and raw materials. Commodities supply shortages (grain, energy products, etc.) and increased prices may cause significant challenges to companies operating in specific industry. This situation can be managed by a proactive action to assess potential impact in manufacturing and financial cycle of the clients.

Proprietary Investments and Capital Markets activity

Clear instructions and a strict monitoring of **financial investments** on securities issued by crisis correlated entities should be given. OTC derivatives activity with crisis correlated counterparties must be carefully overseen and regulated. Settlement risk must also be assessed, especially with reference to the currency involved in the crisis.

Client Investment Management

Accounts related to **sanctioned** names must be promptly identified and controls put in place on the respect of blocking measures.

New guidelines should be given about investment policies and deposits, considering emerging risks on issuer related to the crisis.

Transactions Services

Bans posed to transaction services (payments and trade finance services) should be followed with detailed operating instructions to assure that the activity is conducted in strict compliance with internal rules and operational instructions.

2.4 Group Reputational issues – Reputational Risk Exposure

Communications related to the conflict, e.g. compliance issues and managerial actions, may expose the Group to significative reputational risk. Tone at the Top is important.

Key Risks: Reputational

Main Actions and IA contribution

Social media and **information channels** should be monitored to intercept possible threat to Group reputation, being ready to fast reaction to minimize potential damages and enforce related internal conduct code.

Humanitarian initiatives (donations, fundraise, collections etc.) must be conducted in compliance with internal rules and properly coordinated and authorized.

Reputational consequences connected to **lending** and **investment businesses** (for example operation with countries impacted by the war, companies operating in defense/military sector) must be carefully assessed and regulated, also considering the ESG profile of the Group.

IA should help to mitigate reputational risks, providing assurance on the adequateness of the internal rules and control framework and promoting attention towards these aspects. It should be also important to assess the quality of the internal process put in place in order to determine data and information to insert in the communication eventually provided to Markets/Regulators.

2.5 Set up of specific governance mechanisms and monitoring tools

The Group should organize itself to collect firsthand information on the evolution of risk and facilitate the flow of information among Group structures and decisional processes. Flow of information towards the Board and Top Management must be frequent and complete. Decisions must be quickly and correctly executed.

Key Risks: Operational (with reference to correct collection and circulation of all relevant information to support proper decisional mechanism)

Main Actions and IA contribution

Group **Crisis Management** Unit should promptly trigger the creation and coordination of extraordinary task forces and coordination mechanism dedicated to follow and manage the crisis. All relevant business and control functions must be involved.

A Unit crisis to advise on critical business decisions and rule interpretations may be activated, as a distinct and high-level body, kept separated from day to day operational task force.

A clear **monitoring dashboard** should be implemented. Each of the business lines impacted should be included in the dashboard, showing current exposures in terms of credit lines, equity stakes, volumes of business and other meaningful data.

For each relevant business, an estimation of crisis impact must be provided, together with actions to be taken in order to comply with regulation and managerial options to mitigate emerging risks.

IA, in an observer and challenger role must attend the meetings of the Crisis Management Unit in order to collect relevant information, provide insight and discuss possible anomalies, assure that information and decisional process work properly. IA must not be involved in business decisions.

2.6 Continuous monitoring and management of the crisis impact on regulatory and RAF limits and other key Risk Indicators. Evaluations on P&C assumptions

Impacts of the developments of the crisis on all risk indicators (**Liquidity**, **Credit**, **Market** and **Counterparty,** etc.) must be strictly monitored. **Regulatory** and **RAF** limits indicators must be updated as soon as feasible. In a second phase, short-term and medium-term impacts on budget and planning assumptions should be assessed.

Key Risks: Operational (with reference to correct update of indicators, proper activation of governance on risk exposures decisions at relevant Board and management levels) and Compliance

Main Actions and IA contribution

Key risk figures must be updated promptly and preferably in operational dash boards at Group level and for each relevant Subsidiary/Entity. Possible **RAF/limit breaches** must be adequately managed and authorized at proper level. Clear comprehensive picture must be available to Board and Top management. In due time, budget and planning hypothesis must be checked considering the impacts of the Crisis.

IA should monitor the correct evaluation of risk indicators and the activation of consequent actions and verify if budget and planning assumptions have been checked.

3. Conclusion

Internal Audit has a key role as an independent function with regard to the development of the crisis. Main objectives should aim to provide independent assurance and insight to

- ensure that Top Management and the Board are given a complete and correct picture of the areas impacted by the crisis, in terms of compliance and regulatory risk (implementation of sanctions and restrictions), credit risk (rating downgrade and change of business perspective arising from the crisis), liquidity and market risk, operational risk (Cyber risk and Business Continuity), including the effects on people and physical assets.

- evaluate if the crisis management teams are composed of all the interested functions and participated by people with adequate level of empowerment and responsibilities. Main points and decisions taken should be traced and adequately disseminated with dedicated processes

- ensure that the decisions making process and the flow of news is properly devised, with adequate escalating and cascading arrangements (clear instructions are available, channels to collect questions and give answers about possible interpretations, proper escalating procedures)

- ensure that as soon as feasible the new rules that are time by time approved to regulate the Group activity during the crisis are properly applied and controlled by first level and second level control function

Internal Audit must be prepared to review its own planning and priorities, adjusting quickly and accordingly in order to follow adequately the development of the Crisis as above descripted.

Specific audit engagements should be foreseen to verify the correct implementation of new rules and procedures adopted and to assure the effectiveness of the **Internal Control System** along the different phases through which the crisis develops.

Following the above interpretation of its role, Internal Audit has an **important role to play**, together and in coordination with the other Group Functions, to help the organization to safely go through the current crisis minimizing the significative risks that it poses.

About ECIIA

The ECIIA is the voice of internal audit in Europe. Our role is to enhance corporate governance through the promotion of the professional practice of internal auditing. Our members comprise 34 national institutes of internal auditing from countries that fall within the wider European region, representing 48 500 members. The ECIIA mission is to further the development of good Corporate Governance and Internal Audit at the European level, through knowledge sharing, developing key relationships, and impacting the regulatory environment, by dealing with the European Union, its Parliament and any other European regulators and associations representing key stakeholders.

The **ECIIA Banking Committee** is representing the voice of internal auditors from the Banking Sector in Europe and made of representatives from big European Banks.

We would like to thank all the people involved in this thought paper, in particular, Claudio Testa, CAE at Intesa Sanpaolo, and the Executive Directors at ISP Audit Department at Intesa Sanpaolo: Paolo Nasi, Mauro Zanni, and Tortelotti Stefano.

We would also like to thank the ECIIA Banking Committee members for reviewing this publication.