A response by the Federation of Latin American Banks – FELABAN to the Basel Committee on Banking Supervision's consultative document on:

Principles for operational resilience

Dear Basel Committee on Banking Supervision members:

The Federation of Latin American Banks (hereinafter *FELABAN*) acknowledges the Basel Committee on Banking Supervision (hereinafter *the Committee)* for the opportunity to discuss the proposals included in the consultative document "*Principles for Operational Resilience*", published on 6th August 2020.

Even though risk management processes in the banking sector (particularly those related to operational risk management) have significantly improved over the last years across jurisdictions in emerging markets, it is worth noting that affairs related to operational resilience are in a nascent stage. The present circumstances worldwide have shown that no scenario, no matter how extreme it is, can be labelled as "unlikely" in future risk analysis exercises. Thus, we welcome the Committee's proposal included in this consultative document.

FELABAN analyzed and discussed its content with the Banking Associations we represent, as well as with our Latin American Committee on Risks, and the outcome is this document, which highlights our comments and views on this initiative. We firmly believe it will be a useful feedback to the development of an operational resilience framework, from the point of view of the Latin American banking sector.

***

General Comments on the Operational resilience principles

An evolving operational risk landscape. We agree on the dynamic nature of the risk landscape in the banking sector: new business opportunities imply potential new risk sources, and risk management must keep an eye in this ever evolving and fast-paced environment. Given the speed of implementation of new technologies, as well as the constant change in threat scenarios, we consider an operational resilience framework should consider guidelines on periodical assessments (once a year) on the evolution of emerging risks, in order to update resilience plans and/or including them in the banks' strategic business plans.

Similarly, an operational resilience approach should also be considered and implemented by third parties, not only banks (i.e. through legally binding contracts), as third-party risk management is becoming more and more relevant nowadays.

Essential elements of operational resilience. In this regard, we consider continuous identification of potential risks associated to disruptions on information and/or application systems as a key consideration. Furthermore, we deem as necessary for bank to articulate operational risk management to BCPs (Business Continuity Plans) and Resilience plans along the key stakeholders in this process (business areas, tech areas, senior managers and board of directors).

Definition of operational resilience. We highlight the need for a resilience plan to be articulated to the bank's risk appetite, risk tolerance and risk capacity, keeping in mind these threats impact the whole financial system (instead of a single financial entity). The consultative document focuses on operational risk management on affairs such as nature, size, complexity and risk profile of bank's activities; however, some domestic regulatory frameworks seem not to consider these affairs as a whole, rather, as "tick boxes" that must be complied with, which does not enforce an operational resilience framework in the financial system.

Q1. Has the Committee appropriately captured the necessary requirements of an effective operational resilience approach for banks? Are there any aspects that the Committee could consider further?

In general terms, we consider the factors defined by the Committee for an effective management of operational resilience (Corporate Governance, Operational Risk Management, Business continuity test, Interconnections and interdependencies of critical operations, Third-party risks, Management of technological incidents and cybersecurity) are the right ones, and include accurate recommendations for banks when it comes to identifying the operational risks banks are currently facing. However, we consider this consultative document might benefit if some additional aspects are included from the point of view of the Latin American banking sector, which we summarize below:

- Set specific requirements in terms of the Committee expectations on operational resilience, involve business resilience and its importance and proper communication to the Board of Directors.
- Propose specific metrics to monitor and quantify operational resilience risk.
- Define a set of preventive actions to keep in mind in order to prevent materialization of risks associated to disruptive events, so that a determined business maturity stage is enforced.
- Highlight the importance of proper and timely communication between the Board, senior management and the banks' human capital, since the success of the execution of the processes and the measures adopted in a disruptive scenario, aiming to keep running a bank's critical operations, largely depends on the people who run them. This success, therefore, will not depend on producing highly technical and specialized documents on best operational resilience practices.
- Define the "optimal" maturity stage expected in terms of operational resilience, so that requirements aiming to achieve it can be developed and implemented. This could also be extrapolated to identification of systemic risks.
- Another aspect to emphasize is the human factor, that is, the safety of employees in the development and implementation response and recovery plans.

- Resilience should not be exclusively linked to operational risk. Credit and market risk areas, for example, can also play a key role should a systemic risk event materializes.
- The principles should be differentiated for internationally active banks, in order to measure the application of these principles at large scales.
- Risk management and risk quantification methodologies might benefit from a deeper revision in terms of frequency and probability of occurrence. As an example, the worldwide situation we are currently facing had a low probability of occurrence, but its outcome involved a high severity. Thus, when creating protocols and operational risk resilience plans, it is important to consider extreme events associated to severe disruption of business continuity, so that banks can be better prepared for future events of similar severity.
- Consider a principle for reputational risk. Even though having an incident communication plan is mentioned, improving the frame of reference to be followed during a crisis, will help beyond operational risk recovery, in addition to improving the level of positioning with clients in the case of an event that could materialize this risk.
- It is necessary to focus on longer interruptions of business activities, as the interruption length is an important measure to define how critical a disruption is - from a BCP point of view. Considering longer interruptions would allow banks to create better contingency scenarios, as well to prevent significant impacts compromising banks business continuity operations.
- The role and responsibilities of the three lines of defense should be kept in mind, so that the execution of any operational resilience plan is not compromised.
- Both regulators and supervisors play a key role in developing operational resilience plans, as any regulatory change can impact a bank's risk profile and risk appetite – not only in terms of expectations on operational resilience, but also on the way they can support bank's business operations from their role in the financial market.
- It is important to clarify the variables and parameters to keep in mind in order to estimate the Committee's operational resilience expectations across banks.

Q2. Do you have any comments on the individual principles and supporting commentary?

We observe that, in the Committee's view, third-party risk management is becoming more and more relevant, something we positively ponder. Arrangements with vendors and suppliers not only should become stricter, but also consider operational risks and BCP criteria.

Similarly, the Committee should consider the relationships prevailing in financial conglomerates (parent-subsidiary companies), as risk analysis might evidence irrelevant risks when evaluated at individual level, but might become relevant at a conglomerate level.

Moreover, we consider as important for the Committee to include risk appetite and risk tolerance metrics when defining capital requirements, as this proves to be key in challenging economic times – such as the one we are currently facing. Thus, specific metrics could be proposed by the Committee in order to individually monitor each of the risk factors that make up the 7 proposed principles and in addition to a comprehensive methodology allowing to quantify the total level of operational resilience risk.

Governance. We suggest the Committee to include guidelines regarding the Board of Directors' responsibility of incorporating operational risks and operational resilience in the bank's short, medium and long-term strategic plans.

Separately, on paragraph 17, the Committee should consider including a reference to the accountability that the Board of Directors should have in ensuring that lessons learned from disruptive events are analyzed and improvements, where applicable, are reflected in the response strategies.

Operational risk management. Paragraph 21 suggests that the responsibility for the Bank's "Senior Management" or "Bank's Functions" to manage and address risks is an exclusive responsibility of Operational Risk areas. Instead, it should be transversally address by several areas along the organization.

Additionally, the Committee should consider adding another sentence on paragraph 22, stating that assessments of controls should be reflected through the tools used by the Bank to manage its operational risk profile.

Business continuity planning and testing. Proper testing on a variety of severe scenarios is challenging for banks, as it demands significant investments in terms of implementation.

Furthermore, we suggest this principle not only accounts for critical operations but also critical vendors, as some vendors (such as tech ones) provide their services to two or more entities, or can even be the only providers in a given geography.

Mapping interconnections and interdependencies / Third-party dependency management. As these principles refer to the relationship between critical processes with internal and external processes provided by third parties, we suggest to unify both of them. This, given the importance to discard any potential ambiguity or confusion between them.

Third-party dependency management. Even though we deem it as important and relevant, we consider more clarification is needed in terms of the Committee's supervisory expectations on third-party operational resilience.

Q3. Are there any specific lessons resulting from the Covid-19 pandemic, including relevant containment measures, that the proposed principles for operational resilience should reflect?

Regarding Business Continuity Plans, we suggest:

- To include the (estimated) probability of occurrence of extreme events even if they had not materialized before, and set strategies allowing flexibility in terms of processes enforcement while preserving safety levels and BCP's regulatory compliance.
- To analyze processes' interruption periods in order to consider unusual/outlier events, as well as determining the criticality on those processes that initially did not trigger alerts under conservative scenarios.
- To rethink current business continuity frameworks according to predefined crisis or disruption scenarios. As an example, contingency support offices may be rethought, as the pandemic proved that working from home is a viable scenario.
- To analyze BCPs as a whole, not only from a technology point of view, but also from a business point of view (in terms of front/middle/back offices).

- As working from home could be maintained as an option for most of employees in the financial sector, the current contingency scenarios and the continuity strategies / plans must be updated to this situation.
- To provide more emphasis to the fact that resilience plans should also focus on ensuring adaptable processes and services to continue satisfying customer needs and protecting employees in the short term. Future frameworks on operational resilience should consider insisting on the importance of having the appropriate governance mechanism to oversee non-financial risks while contingency lasts.
- To review network configuration to allow a faster access without jeopardizing the security, segregating the bandwidth usage (*split tunnel*s) for bank's applications from internet, e-mail, etc.

On the other hand, it is important to better explain what critical operations entail, as a more explicit definition may be of relevance for several stakeholders (clients, shareholders, supervisors, amongst others). Similarly, it would be appropriate to set guidelines on which are the critical processes to keep in mind during a systemic failure, as COVID-19 proved as priority the immediate need of available resources on several customer service channels, and later, some other needs were identified in terms of outstanding payments and financing, and none of them were considered in most of banks' BCPs.

In fact, it is important that business continuity plans be rethought, not only focusing on the critical operations, but also on the entire operation of the organization, such as the current pandemic situation. Therefore, duration of contingencies should also be recognized and be kept in mind.

Separately, resilience should address commercial and sales strategies restructuring processes, given the rapid change in financial customers needs, market volatility and adjustments on financial services provided during the pandemic.

With regard to Human Resources, we suggest the Committee to consider:

- To address, in a more granular way, human resources management and their involvement in defining the measures to be adopted to face the pandemic effects, particularly in terms of physical, emotional and psychosocial affairs (amongst others).

- To monitor, on a regular basis, every party involved in the Crisis and Emergency Committees, given the importance of building a formal program both for key personnel and backup personnel.
- To include guidelines to strengthen and foster work-from-home policies.
- Within the Governance Principle or the Operational Risk Management Principle, critical personnel training in psychosocial risk management issues to mitigate negative psychological and social damage could be considered as a reinforcing measure. Thus, stress and mental exhaustion in key personnel should be considered, which can occur in people when they are subjected to crisis situations.

Likewise, we note the pandemic induced a systemic impact in which the response by banks was aimed not only to maintain the availability of their operational systems, but also the need of controlling side-effects in terms of risk management (particularly credit and market risk).

Similarly, the pandemic proved the need of considering joint (instead of isolated) extreme scenarios in the future, such as pandemic and natural disasters, natural disasters and cyberattacks, cyberattacks and international wars, etc.

Last, but not least, the pandemic demonstrated the need of easing some restrictive controls faced by financial sector entities, preventing them from operate their core business in places different to the ones where their normal operation functions in.

Q4. Do you see merit in further consolidation of the Committee's relevant principles on operational risk and resilience?

We consider as important to keep the aspects below in mind:

- Consider a more dynamic and collaborative approach with regard to information management. Real-time experience feedback both of entities and markets would be ideal.
- It is important to clarify that operational resilience will be effective as long as key stakeholders are aligned within the bank, and corporate governance affairs are strengthened through that process. Operational resilience should not be an exclusive responsibility of risk management areas.

- Before further consolidation, the Committee should take into account further principles that may properly describe operational resilience challenges for banks.
- To analyze what has happened in other geographies, so that best practices can be identified and, eventually, extrapolated to other jurisdictions.
- Given that this consultative document focuses on recovery and adaptation to operational contingencies, mostly due to operational risk events, we consider it worth further developing.

Q5. What kind of metrics does your organization find useful for measuring operational resilience? What data are used to produce these metrics?

When identifying and measuring operational resilience, it would be ideal to do so with parameters and indicators enforceable to all entities, as risk materialization events tend to be of a systemic nature (instead of failures impacting an isolated entity). Therefore, the next step would be to define the same critical processes or threat scenarios for every entity, thus facilitating resilience plans' evaluation and testing. The outcome results from these scenarios might be useful to create indicators aimed to evaluate whether an entity is prepared to face them, as well a designing tests aimed to evidence the overall financial system resilience. Such approach can be extended to critical processes both in domestic and overseas scenarios.

Currently, Latin American Banks use some form of the indicators described below:

- Key risk indicators (KRI) to monitor risk factors (Business continuity, Information integrity, Incident management, Third-party risks, Physical and technological security, etc.) that make up operational resilience.
- Indicators to measure compliance with recovery time objectives and other metrics and BCP enhancements. These indicators are based on target definitions and measured against actual observations.
- Implementation of alerts for any operational and technological incident.
- Technology and cybersecurity risk appetite metrics (Obsolescence, vulnerabilities, phishing, Independent Security Score, Security Information and Event Management integration). The data used for these purposes comes from independent monitoring of the systems.

- Portfolio growth / maintenance.
- Post-crisis self-assessment questionnaires in the aftermath of the crisis
- Compliance with internal and external regulations (reports, audits, questionnaires, evaluations)
- Effective communication with stakeholders and stockholders.
- Comparison of individual key performance indicators with systemic key performance indicators, as well as compliance with tolerance levels. It is suggested that operational information is taken into account.
- Information about the materialized incidents to design and implement new risk indicators, work plans and, if necessary, open new risks to monitor the development of the response plan and prevent future events with the same characteristics.

All in all, derived from the pandemic impact in the real economy, we consider the next elements can prove as useful when measuring operational resilience:

- Consolidating criteria, in order to determine the overall entity's operational resilience level from separate indicators.
- Continuous monitoring of continuity plans, identifying the ratio of satisfactory tests as a proportion of the overall tests.
- Continuous monitoring of critical vendors, as well as the associated legal contracts.
- Metrics related to adherence to business continuity plans when responding to disruptive situations.
- Metrics related to the time span business areas need to return to the same transactional amounts as before the disruption, from the lowest point reached in the crisis.
- Metrics related to third-party providers: how many of them have business continuity plans, the number of core services that it is possible to source from an alternative provider in the market, how much time is needed to establish commercial relations with alternative providers.
- Metrics related to operational management: proportion of activities undertaken by each employee, properly documented.
- Metrics related to incident management: number of recommendations made by the second line of defense, and permanently adopted by the first line of defense.

- Metrics related to information and communication technology: proportion of technological made redundant, information and communication technology availability index, and proportion of activities that can be carried out from remote locations.
- According to the changes related to the contingency and the operational resilience, a bank has made some new measurements from infection indicators by means of internal surveys, level of infections in contact centers through the properties department and the way they measure stressed operational losses. Data used for metrics for measuring operational resilience came from IT, available VPNs data, critical vendors' inventory, available IT infrastructure, among others. The relevant metrics may also come from heat maps developed from branches indicators, risk and controls original repository against the ones developed for the contingency and from stabilization review of the resilience process.
- Regarding critical processes:
    - Identifying the processes required for the entities' adequate functioning in a given time span
    - To carry out tests and interpret the outcomes
    - To define metrics related to the entity's capacity to respond to events, measured as RTO (Recovery Time Objective) and RPO (Recovery Point Objective), whenever possible
    - To develop critical applications backed up in alternate data centers
- Financial indicators: Liquidity and solvency in order to assure smooth banks' proper operation; and materialization of economic losses due to disruption events.
- To determine a ponderation including maturity measures or completion percentages for each principle.
- Limits on risk appetite.
- Regarding transactions: Continuous transactions monitoring in a given day in order to analyze service capacity; and understand whether customers' transactional behavior is changing and, thus, regulatory adjustment might be needed.
- From operational risk materialization events, signals on risk classification, service channels and geographies can be determined, allowing banks to perform analysis and preventive measures. It might be possible to considering monitoring: number

of lost customers due to unmet service demands; number of technical or operational errors; security incidents; and so on.

- Metrics that identify the extent to which operational capacity recovers in relation to the capacity existing prior to a severe operational contingency (for example, the volume of operations or transactions, level of sales, income, in the current post-contingency state).
- Remote data queries in order to get feedback on key risk indicators monitoring, so that continuous operations tracking may lead to determine whether certain risk exposures can turn into disrupting business events.
- Periodical reporting of risk behavior to a central crisis committee.
- Given that operational risks are quantified, as is the loss due to not operating critical processes, the latter in the BIA, it would be necessary to implement a scheme that helps to compare both measurements. A bank would assess different scenarios from those already contemplated, these being of greater complexity. With the above, a bank would quantify the materialization of not operating a process and that at the same time there was a serious deviation in it. With these indicators, a bank could compare the outcomes with the institution's risk appetite, and obtain thresholds of loss amounts. It is also possible to carry out this assessment for incidents and vulnerabilities.
- Some banks are in the process of reinforcing these indicators, with a view to developing a comprehensive methodology that will allow us to jointly quantify the level of operational resilience risk.
- Defining a management model of prevention, action and return to operation, to ensure stability operational and financial entity is paramount. Thus, the definition of these 7 principles of operational resilience is appropriate for all corporate governance to implement in its business administration.
- Regarding online transactions monitoring, even though potential changes will not yield immediate results, it has been necessary to implement prompt application guidelines due to the observed massive attacks to digital channels, which evidenced a spike use during the pandemic. The focus here should not be metrics, rather, quick developers that make possible both scenario setting and new controls or business guidelines required to mitigate arising risks derived from lack of customers' financial

education. **To achieve a more comprehensive strategy, industry-level efforts and collaboration with public authorities becomes more relevant than just sharing information and data**. Fraud-related affairs are a common industry problem, and financial sector entities should not compete between each other on this regard. This should become a new line of defense, transcending individual entities, and strengthening the work both of supervisors and banking associations.

***

FELABAN wishes to thank the Committee for considering the above comments, and hope they enrich the development of the operational resilience framework. Should any clarification arise regarding our comments to this consultative document, we look forward to discussing them further.

Sincerely,

GIORGIO TRETTENERO CASTRO

Secretary General

FELABAN – FEDERATION OF LATIN AMERICAN BANKS