6 November 2020

EBF response to Basel Committee consultation on principles for operational risk and operational resilience

Introduction

The ever accelerating pace in which technology has advanced in the recent years, in combination with the outbreak of the Covid-19 pandemic have amplified the risks and threats to the operation of financial institutions, highlighting the need for firms to continue to build on their operational resilience.

The EBF welcomes the Basel Committee initiative to review, update and improve the principles for operational risk and operational resilience for banks. We would note that in the EU context, there are a number of regulatory developments in the context of "resilience", albeit with a different focus than the BCBS proposals. It is likely that some of these proposals, including the proposed EU Act on digital operational resilience for financial services (DORA) will contribute in part to an operational resilience and operational risk financial ecosystem of which Europe is such an important part.
The overarching view of our members is that in the context of an operational resilience framework, it is important to establish a regime that is appropriately principles based and outcome driven. Globally, financial sector firms have different business models and organizational structures and therefore a flexible approach is necessary to best support global consistency. BCBS should continue to work closely with industry, regulators other global standard setters to encourage a common approach to operational resilience in order to reduce the risk of conflicting approaches. In this respect, we would encourage the establishment of a joint public-private forum at the global level which could provide guidance, define key terms, and drive alignment on significant resiliency concepts. One of the subjects of this forum should be that regulators and industry should not strive for a zero-incident environment. This is neither feasible nor desirable. Once accepted, firms could collaborate with authorities on the national level to define the right processes to manage incidents. Given the nature of the Principles, we also encourage ongoing collaboration between the public and private sectors to allow for an iterative process for implementation and remediation, and a harmonized roll-out across jurisdictions.
In the following two chapters, the EBF is addressing key issues identified in each of the two sets of principles. While this response covers both consultation documents, our members, at this stage, are of the view that the BCBS proposals should be seen as two distinct, but related exercises. As such, our members support the documents being drafted

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

separately. Of course, this should be done keeping in mind the interconnections between the two documents. To that end the two documents should be drafted in a way that ensures consistency in definitions and concepts, as well as giving sufficient clarity as to how those documents are related.

Section I

Principles for operational resilience

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?

Good operational resilience frameworks bring together already-familiar good management disciplines with proven industry best practice to build more resilient firms and hence more robust financial ecosystems. Concepts like operational risk management, outsourcing and vendor management, business continuity, and regular firm and sector desk top exercising can be found at the core of the most resilient firms. Whereas management and regulators have traditionally taken a bottom-up approach to operational resilience planning, the evolving, interconnected and complex nature of contemporary operational resilience challenges now requires a more strategic approach. As the Principles suggest top-down, board-centric planning should be at the heart of any firms' approach to operational resilience, with boards themselves taking responsibility for setting their firm's strategy and risk appetite, and holding executives accountable for planning and execution. So we support the BCBS's approach in requiring operational resilience regulatory regimes to require firms to meet these expectations.

In determining a firm's approach to operational resilience, the BCBS establishes that operational resilience expectations are to be set with reference to the bank's critical operations. In one jurisdiction, policy makers have alighted on "important business services" as the mechanism by which this should be implemented. While it is understood that the intentions of individual regulators are in principle aligned with the BCBS on this point, it would be helpful for there to be greater alignment in the lexicon of terms such as "important business services", "critical operations" and "critical functions". This is important when further consideration is given to how jurisdictions and firms would implement the BCBS's requirements. Firms interpreting the BCBS proposals through the lens of recovery and resolution will, as a first step, be required to establish which of their operations are critical in line with the FSB's RRP guidance, and then to expand the list of critical functions to include activities, processes, services and their relevant supporting assets, the disruption of which would be material to the continued operation of the bank or its role in the financial system. In that light, it will ultimately also be essential to have more clarity on the extent if the alignment and harmonisation between RRP and operational resilience. For example, we would need more information how harmonization is expected to be achieved for example if a critical operation is identified for operational resilience but not for resolution planning purposes.

We support further clarification and consistent definitions of certain concepts to avoid potential misunderstanding across jurisdictions or entities[1]. Clarity and consistency would help to tackle this, and should specifically address how these may differ, if applicable, in the context of operational resilience and the read-across / alignment with related topics and regulatory guidance. Examples include:

i. Critical Operations, and degree of cross reference to RRP terminology
ii. Risk Appetite and Risk Tolerance
iii. Risk and Impact Tolerance
iv. Definition of Criticality, e.g. critical v. important

In addition, we welcome paragraph 13 in the consultative document, in which the Committee explains that, whether a particular operation is "critical" depends on the nature of the bank and its role in the financial system. This approach helpfully puts the concept of proportionality at the heart of any operational resilience regulatory regime, and provides for firms to assess their relative importance to their wider market stakeholders (which includes their customers). This also entails that banks should have the flexibility to decide what are ultimately included within those functions that are deemed as critical. In this respect, we would emphasise that in order to achieve an effective operational resilience approach, BCBS should pursue a principles-based and outcomes-focused approach where firms have the flexibility to determine their own operational resilience programs in a way that is relevant and proportionate to their business and risk profile. This could include leveraging existing broader risk management frameworks, along with other firm specific considerations.

While a firm's incident prevention controls will reduce the likelihood of disruptions, good operational resilience frameworks should also assume that disruptions are inevitable - it is a case of not if, but when. Incident management procedures must manage the incident, ensure there is no spike in fraud risk, and minimise any other fallout, but it is neither realistic nor reasonable to strive for a zero-incident environment. Instead, firms, working collaboratively with relevant authorities and government agencies should make all reasonable efforts to prevent an incident occurring. But when they do, firms must have sound crisis management processes in place that put the customer's interests first. This will help promote processes that will minimise wider market disruption, and secure a smoother return to BAU. Finally, firms should be required to regularly identify any vulnerabilities and promptly take account of them in their decision making and risk mitigation processes.

Finally, the issue operational incident reporting could benefit from further international elaboration. Common and well-understood approaches to the reporting of operational incidents – whether to regulators, the public or both - are inconsistent across jurisdictions, and we believe would benefit from BCBS guidance as to what constitutes best practice. Cyber incidents, an increasingly common cause of operational disruption, would in particularly benefit from a consistent reporting framework across jurisdictions, especially as the actors in these events regularly operate from beyond national borders. We ask that the BCBS consider what else could be done in this space.

[1] Please see also our response to question 4 of the consultation document on the principles for operational resilience.

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

Considerations of core requirements can be built on the seven suitable principles identified by the Basel Committee:

Principle 1 on Governance

We support the BCBS's placing responsibility for setting a firm's operational resilience strategies firmly with boards. As the draft BCBS principles establish however, responsibility for executing these strategies will remain in the hands of senior management. We believe that the BCBS principles should recommend that regulatory authorities engage with industry to develop a better understanding on how to operationalise senior management responsibility and accountability. In particular, for multinational banks reporting/board oversight can span multiple legal entities and governance structures. Firms should be allowed to make decisions, in particular operational ones, at a lower management level.

One concept introduced in the consultation document is "risk tolerance for disruption considering the bank's risk appetite, risk capacity and risk profile" however it is unclear how this "risk tolerance" should be set and measured. Indeed should it be similar to risk appetite and thus description the bank "willing to accept, or to avoid a risk, in order to achieve its business objectives" or is it more toward risk capacity stating the maximum level of risk the bank can assume before breaching its constraints (regulatory capital and liquidity needs).

Principle 3 on Business continuity planning and testing

The EBF agrees with the need for banks to have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption. EBF members have developed internal policies and procedures to support their organisation's business continuity (including their response to and recovery from cyber security and operational incidents), which are described in the Business Continuity Plan and Disaster Recovery Plans of each financial entity.

While we support prudent scenario testing, the policy design needs to be proportionate to the nature scale and complexity of the firm and the risk it poses to wider financial system stability. We view that scenario testing is important but recognize that it has limitations and may not capture the dynamic capabilities required to respond in crisis. Therefore, we consider that scenario testing should be considered alongside the banks' crisis management capabilities. Some firms may face challenges in their capacity to test against multiple scenarios, and then to introduce the necessary changes within operations. This is important when setting expectations around how frequently firms must undertake such testing. The time and expertise that is required to design, agree and then execute meaningful scenario exercises for each important business service on an annual basis should not be underestimated.

Greater clarity on when the testing should be paper-based vs simulation vs live systems would be welcome. Given, as noted above, that the resources required to execute each type of testing can be significant, a judgement will be required to determine which approach is best, while also ensuring a "do no harm" approach to testing. We also believe that the BCBS needs to draw a distinction between existing cyber exercises and operational resilience testing. As the resource demand internally will have significant overlap and with the number of tests related to cyber resilience growing, it is essential that authorities coordinate between the two regimes. It is key that there is a clear delineation between

operational resilience testing and cyber exercises, which are only a subset of operational resilience testing. Otherwise, the operational resilience framework may become inefficient due to overlaps between its different parts.

In addition, as stated above, operational resilience is a multifaceted concept that includes but is not limited to cyber risk or cybercrime. A variety of exercises and tests should be used to identify potential weaknesses in a bank's internal control systems, crisis management processes, 3rd party vulnerabilities, or governance frameworks. To test all of these effectively, a range of scenarios and tests must be used. Penetration testing and red team exercises for example are effective methods for firms to test their cyber capabilities. By simulating real-time attacks, they test the organisation's resilience and identify areas of improvement. Tests should be performed periodically and should test business continuity plans and evaluate the ability of those plans to managing complex events. They should also include more operational simulations, both related to business continuity solutions and to red teaming, so as to evaluate technological responses.

Principle 4 on Mapping interconnections and interdependencies

The EBF supports the principle that firms should be required to undertake resource mapping which is key to highlighting areas of operational resilience vulnerability. However, the EBF does believe that the process of resource mapping is likely to be one of the most resource intensive elements even where it is possible to leverage from existing work. Therefore, the BCBS should only require the resource mapping for the most critical functions. In addition, there are a number of areas where further detail would be welcome:

- Keeping maps up to date, especially across large multi-jurisdictional entities, will be challenging and costly. Technology solutions will need to be developed to address this however the BCBS should explicitly acknowledge that even an incomplete picture, which enables effective prioritisation and timely action, is valuable. The BCBS should encourage regulators to avoid arbitrary time periods, focussing instead on the need to capture changes in risks and operating processes.

- We agree that the approach and level of granularity of mapping should be sufficient for banks to identify vulnerabilities and to support testing of their ability to stay within their stated risk appetite, risk capacity and risk. It is important that firms are allowed to retain this flexibility, and that jurisdictions avoid arbitrary determinations about granularity of mapping.

- Where a firm operates across multiple jurisdictions, it is likely that elements of their critical operations will be geographically dispersed and/or spread across different legal entities. When mapping these interconnections, we believe that the level of mapping required should be proportionate to the level necessary to manage the dependency

Principle 5 on Third-party dependency management

The EBF agrees with the need to manage the dependencies on third parties for the delivery of critical operations, in line with applicable regulation and supervisory requirements addressing outsourcing by financial institutions. However, banks already operate under an extensive supervisory framework to which a significant number of regulations and Guidance has been added in recent years, for instance the EBA Guidelines on Outsourcing of February 2019. We therefore encourage policy makers to allow time for these

regulations to come into force before further adding to the regulatory rule book in this area.

Some jurisdictions, such as the EU, are now considering direct oversight regimes for third party IT providers deemed critical to the financial sector. It is important that any such oversight regimes are globally consistent and where possible coordinated to ensure the financial services market is not fragmented. Inconsistent application of such oversight between jurisdictions could result in market uncertainty for both providers and financial institutions and may even result in increased operational risk if firms are forced to operate supply chains that are designed for compliance rather than resilience. To give an example from the EU: Even when looking at the EU exclusively, it will be necessary to align the current framework (as set out in the EBA Guidelines on Outsourcing Arrangements) with the newly proposed DORA, and to unify concepts and requirements. The key principles proposed in DORA should be developed with sufficient detail to avoid divergences in its implementation, and building on the existing guidelines from the ESAs. We need to have a unique set of rules for all financial institutions on how to manage outsourcing risks from ICT providers. This demonstrates the challenges that exist and why it is important to tackle them to harmonize the different regimes.

Where the BIS's principle 5 is explicitly referring to intra-group entities, we would like to emphasise existing oversight mechanisms. We believe the principle for dependency management for intra-group outsourcing is already sufficiently reflected in the existing EU regulatory framework for financial institutions. Any new regulation for third party or supply chain management that include inter-affiliate operations should explicitly recognise the heightened control that an entity may be able to exercise over other entities in its cooperate group as compared to that of a truly external third party.

We welcome the considerations laid out in Principle 5 para. 32, 33 and 34. EU Financial institutions already uphold this guidance by complying with supervisory requirements which – in turn – reflect the EBA Guidelines on outsourcing. We would like to stress the importance of a risk-based approach by financial institutions and competent authorities when applying the considerations under Principle 5 para. 34 on business continuity and contingency planning.

Where para. 33 highlights the importance of written agreements, we strongly support the relevance of standard contractual clauses for cloud use, providing an appropriate tool to safeguard the proportionate implementation of requirements regarding cloud. We welcome the European Commission's respective work on a voluntary set of clauses.

Principle 6 on Incident management

The EBF agrees that banks should develop and implement response and recovery plans to manage incidents and mitigate their disruption of the delivery of critical operations. To this end, the development of a toolkit of effective practices would be helpful for providing guidance to banks' response to incidents, like the one developed by the FSB, which only concerns cyber security. Another example are more advanced Early Warning systems that can also contribute to gain early knowledge of incidents exceeding relevant thresholds or patterns (not limited to only IT-metrics) and enable timely mitigation before incidents become widespread failures causing systemic disruptions of critical processes. Such a toolkit should further encourage authorities to adopt more uniform practices by making reference to existing and well-established mechanisms and best practices. During attack phases and through the lifecycle of a cyber-attack, gathering intelligence and sharing it with peers and the industry is also very important.

One area that the BCBS principles do not address is communications. Fast and effective internal and external communication strategies are critical when managing an operational

incident, and firms should be required to have these in place. Plans should address how to contact key individuals, operational staff, suppliers and regulators. The principles should also address the role of regulators and require them to specify how they will coordinate communications relating to cross-firm/ systemic disruptions.

Furthermore, the BCBS should consider encouraging the use of standardized templates for incident reporting. As stated earlier in our response, the EBF believes that cyber incident reporting is particularly important for effective operational resilience. Currently, European banks face a fragmented cyber incident reporting framework, both in Europe and globally, as a result of a range of different incident reporting requirements. To address this challenge, the EBF recommends harmonising reporting thresholds and creating a common taxonomy for cyber security incidents. Public-private real-time collaboration and involving national CERTs in information flow should be strongly encouraged and regular bi-directional information flow between regulators/supervisors and the industry after analysing and anonymising the incident reports should be introduced. The EBF also supports the centralisation of incident reporting and coordination by establishing a single central hub that could work as a one-stop reporting mechanism through which all incidents, including sector-specific ones, can be reported.

Lastly, we would like to highlight that the BCBS should also emphasize the distinct characteristics of each incident management and crisis management, and to provide a sufficiently clear distinction between the two areas. After all, a crisis is not an elevated incident management approach but is a more strategic oversight to manage the impacts/consequences of an incident and to lead the strategic response.

Crisis management is seen as the responsibility of the entity/function accountable for the critical operations in scope of the disruption. It would be very welcomed if the BCBS could add a distinct definition of crisis management to clarify this point.

Principle 7 on ICT including cyber security

The EBF considers cyber security fundamental for the operational resilience of banks. In addition to the ICT-related issues raised under the previous principles, we consider that the principles should account for the importance of cyber threat information sharing schemes that allow, on a voluntary basis, the communication of incidents, threats, vulnerabilities, and lessons learned in a secure and trusted environment, which is vital for enabling banks to achieve high levels of cybersecurity resilience. This would entail better identification of cyber threats and improve the prevention of cyber incidents. However, any principle should equally emphasize that information must be voluntary and that when when mandated it loses its utility and creates risks by encouraging the sharing of information outside of trusted circles.

Another effective way to further enhance cybersecurity is the promotion of certification schemes for ICT providers servicing the financial sector. The consideration of a certification scheme should take note of existing industry initiatives and standards commonly established in the market.

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?

We would draw the following lessons from the Covid-19 crisis which have implications on the management of operational resilience:

- As regards cyber operational resilience, some useful lessons have been learned during the COVID-19 pandemic, such as the importance of enhancing of security controls on existing digital services (e.g. VPN infrastructure), implementing new security devices on new digital services made available so that firms can support households and businesses impacted by the COVID-19 emergency and strengthening customer awareness initiatives on cyber risks related to the emergency.
- Because of Covid-19, bank have put extra focus on the increased key controls in place for detecting and preventing fraudulent activities and human errors.
- Complying with health regulations to ensure the well-being of employees has proven to be a vital action during the COVID-19 pandemic. Any bank should act responsibly towards its employees when they are unexpectedly faced with a prolonged period of not being able to work from their office. This includes, but is not limited to, efforts to foster communication and collaboration among employees.

More generally, EBF members are of the view that the Covid-19 pandemic has had a limited impact on the provision of financial services due to the increased digitalisation of financial services, the fact that a pandemic was a known high priority risk and the fact that it was a market wide event that has occurred over a duration that afforded firms sufficient time to pivot to alternative infrastructure. The pandemic has, however revealed the interconnectedness of markets, firms, utilities, local and national governments. This highlights that coordination among multiple stakeholders, as well as convening power by the official sector, is critical to supporting operational resilience of the sector. The pandemic has also highlighted the need for development of global standards such as those proposed by the Basel Committee and/or a global framework, so that industry has a common framework to guide it rather than separate jurisdictional frameworks.

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

Our members are of the view that it its useful and appropriate for the operational risk management principles to be issued on a standalone basis. However, we think more clarity should be provided by the BCBS on the interconnections between the two different consultations, since there is a significant overlap regarding some items (appetite, taxonomy, business continuity, tolerance thresholds, etc). These concepts should be defined in the same way to avoid different interpretations or implementations. For instance, a different disruption tolerance under PSMOR may be required than in case of the operational resilience principles.

In order to achieve consistency between both set of principles, we would suggest some principles to be simplified in favor of others, including a clear cross reference between them instead of references that are only done via a footnote. Whether a principle, for example, ICT is considered to be primarily linked to operational resilience, this principle should be defined under the set of principles for operational resilience. For example, whenever there is a reference to ICT in the operational risk principles, this should be done as an explicit cross reference to the principles for operational resilience linking its content with the operational resilience principle, and vice versa. This would avoid defining the same concept in two sets of principles in different ways or to different extents.

Ultimately, it will be extremely important to have sufficient clarity as to how both sets of principles relate to each other. This important to avoid any ambiguity in the interpretation of both sets of principles.

Lastly, at this stage, we should aim for ensuring consistency and clarity between the operational resilience and operational risk principles. A consolidation between the two could be discussed at a later stage, also factoring in the experiences and lessons learned from the implementation of the operational resilience principles. At this moment, we consider a consolidation to be too premature.

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

Since these principles are high level, we consider we should await until they are defined in a lower, operational level in order to propose adequate metrics to ensure operational resilience. If the Committee intends to create industry-wide metrics, we encourage it to consult in detail beforehand.

Section II

Revisions to the principles for the sound management of operational risk

Q1) Has the Committee incorporated the appropriate revisions to the Principles? Do you have any specific comments on the revisions to the Principles and supporting paragraphs?

We support maintaining the 3rd LoD involvement, under the assurance function, in the oversight of the ORM framework which are firm-wide. However, it is not clear how the 2nd line of defense is defined (paragraph 5, page 3) in particular in respect to the apparent exclusion of the Compliance Function. Both, the Compliance function and the risk management function (including CORF) are broadly considered as 2nd line of defence functions. We agree that many firms will have a CORF but other may rely on their central compliance function to undertake this role. The Principles should leave the precise organisation of 2nd line of defence to the firm. We also agree that the 3rd line of defence should be entirely independent of the first and second lines of defence and should provide independent assurance to the board about the firm's ORMF.[2]

Principle 1:

The scope of principle 1 is not fully aligned with the content. Despite this being a general principle for the sound management of operational risk, paragraph 14 refers specifically to conduct risk. We suggest removing this paragraph as it does not relate to risk

[2] In the context of the discussion on the 3 Lines of Defence model, we would like to point out that there are also currently discussions ongoing, i.e. the comments of the Institute of Internal auditors and their "Three lines model", https://na.theiia.org/news/press-releases/Pages/IIA-Issues-Important-Update-to-Three-Lines-Model.aspx

management culture, which is the focus of Principle 1, although we recognise that conduct risk may arise from a poor culture.

Furthermore, EBF members request clarification on the new concepts of "Senior ethics Committee"/ "board level committee" introduced under Paragraph 14 and on their expected oversight of the implementation of the code of conduct / ethics policy (the latter to be made publicly available).

Principle 2:

- Paragraph 22.b: We would suggest to insert 'CORF' before 'procedures'. All Operational Risk Management Policies can be referenced, but not all Procedures can be referenced in the ORMF, since they are too many– Those of CORF, however, can be referenced.
- Paragraph 22.d: We would suggest to make the following change: After 'Describe' insert 'or reference'. Larger Banks have separate risk appetite statements etc.
- Principle 2 includes conduct risk as part of legal risks (paragraph 22.j). We consider both separately, so we would need more clarity on the definition of conduct risk.

Principle 3:

Principle 3 states:

- The Board of Directors should oversee material operational risks and the effectiveness of key controls: We assume the "Board of Directors" scope is drawn to include its subcommittees, such as the risk and/or audit committees. We view that the previous version of the principle outlining the BoD responsibilities around establishing, approving and reviewing the framework remains valid and should be integrated with the new responsibilities of the current draft.
- The board of directors should ensure that senior management implements the policies, processes and systems of the ORMF effectively decision. Perhaps an alternative wording to "ensure" could be "satisfy itself".

Principle 4:

This principle has introduced the obligation for BoD to periodically review a risk appetite and tolerance statement for operational risk. We assume that it is for the board to determine when a review is required, based *inter alia* on changes in operational processes, business structure and risk appetite

Principle 6:

Paragraph 34 lists examples of tools used for identifying and assessing operational risk, it seems to be very prescriptive. We assume these are cited as examples rather than an exhaustive list so we suggest that these examples should be moved to an appendix.

We are concerned about how supervisors could interpret this indicative list perhaps expecting a firm to deploy all those tools/reports and examine their use during the inspections. This would not be appropriate or proportionate. Firms should deploy operational risk management tools that are most suitable for their particular circumstances.

We would also welcome the provision of more details on the "risk register" referred to under Paragraph 34 b).

Paragraph 35.b indicates "banks should ensure that the operational risk assessment tools' outputs are: … Adequately taken into account in the internal pricing and performance measurement mechanisms as well as for business opportunities assessments". It is not sufficiently clear what "adequately taken into account in the internal pricing" means.

Principle 7:

Principle 7 seems to be too prescriptive.

Paragraph 37.b indicates that "the 2nd line of defence should challenge the operational risk and control assessment of 1st line of defence..." We understand that the term "challenge" in this context means that the 2nd line of defence should ensure that the implemented controls are working effectively. We view that control assessment should include both design and effectiveness.

Regarding paragraph 40, we propose to delete this requirement "Banks should maintain a central record of their products and services to the extent possible (including the outsourced ones) to facilitate the monitoring of changes." Indeed, the possibility to have a central record would depend on banks organization, IT architecture or merge & acquisitions track record. Not all banks can have a central record, all the more when implemented in different countries or running very diversified business and products. The most important is that banks should have procedures on where the products and services are recorded.

Principle 8: Monitoring and Reporting

We consider more clarity is needed when paragraph 41 indicates "Banks should continuously improve quality of operational risk reporting". We would appreciate further details regarding the expectations of the BCBS as to how an improvement could be measured.

The reference in paragraph 42 to producing reports in both normal and stressed market conditions may be understood linked to RDA principles. As mentioned before, this consultation needs to be viewed in connection with other relevant initiatives and existing regulatory frameworks, so reference to existing framework should be included in order to create a consistent and harmonized framework in the operational risk financial ecosystem.

Paragraph 43 refers to "compliance indicators". It is not clear what is meant, and we would appreciate further clarification.

Principle 9 (Control and mitigation)

Although paragraph 46 lists examples of "principle elements of a policy compliance assessment may include", it seems to be very prescriptive. We suggest to reword the paragraph to clarify the examples are not an exhaustive list.

We would ask for clarity on paragraph 48 when refers to "dual control". It is not clear if this paragraph proposes to establish controls on both levels, first and second line of defense.

Paragraph 48 which is entitled 'internal controls' covers much more than controls of norms, targets or limits. We propose hence to reword this paragraph changing the word "controls" to "mitigants".

Paragraph 50 refers to technology. We would appreciate a clearer definition of the term technology to ensure that apps which do not perform controls do not fall under technology risk, but process risk.

There is another reference to strategic risk when it is out of scope of operational risk as defined in the operational risk definition provided in page 2, paragraph 3. We would ask for consistent and harmonized definition across the consultative document.

Principle 10 on Information and communication technology

We agree on this principle. However, it looks like ICT was a complement, but different, to the operational risk framework. We propose that the BCBS makes it clear that ICT is fully embedded in the operational risk framework (definitions, methodologies ….). We propose an amendment on principle 10 to start with "As part of the operational risk management framework…".

The EBF believes that the principle should combine clarity with a degree of flexibility, so as to accommodate internal organisation variations within financial institutions and avoid being too prescriptive (e.g. as to the content of the three lines of defence). Taking a proportionate risk-based approach is of great importance when defining principles for the management of ICT operational risk.

Additionally, harmonising regulatory requirements at the international level by facilitating compliance and avoiding duplication and overlap is crucial for banks, therefore the principle should be linked with other already existing European and international practices and standards, such as the EBA Guidelines on ICT and security risk management.

Principle 11 (Business Continuity Planning)

It looks like BCP was a complement, but different, to the operational risk framework. We propose that the BCBS makes clear that BCP is fully embedded in the operational risk framework (definitions, methodologies ….). We propose an amendment on principle 11 to start with "As part of the operational risk management framework…".

The Committee could also consider to actively link the business continuity principle with "resilience" and "disaster recovery".

Principle 12 (disclosure)

We consider any disclosure requirements on operational risk should be aligned within Pillar 3 disclosures to ensure the comparability between different entities, being at the same time respectful with competitive and proprietary information. Disclosed information becomes more effective and meaningful when it is comparable avoiding inconsistent information across banks that may mislead users of information.

Alignment with Pillar 3 should also be sought in order to avoid that data is disclosed which is considered to be confidential. For example, a novelty of the consultative document is that "significant operational loss events" should be disclosed. Since there is confidential information related to the loss events, we would urge caution in developing this requirement. Generally, the notes accompanying financial statements already contain relevant information, i.e. in the legal risk section.

Q2) Are there any aspects that the Committee should consider further?

Regarding establishing new products and services, the option of deploying a sandbox environment to test such new products/services is missing. The proportionality principle should apply to basic (security) controls around sandboxes and these should not limit the exploratory process.

Moreover, we would like to remark the following: In the explanation of principle 9, the paragraph 51 is dedicated to third party and outsourcing risk. Considering the relevance of this risks (as shown by the Guidelines on this subject already published, for example by EBA), perhaps a specific principle could be dedicated to third party/outsourcing risk, rather than developed within the control and mitigation principle.

Regarding the overall principles we would remark that the BCBS could also consider a principle on "operational risk incident handling". The principle on operational risk handling could contain the following elements:

- A general definition, for example: Operational Risk incident[3] handling is defined as the process of identifying, analysing, remedying and learning from an incident as well as preventing recurrence and/or mitigating the impact if it reoccurs. This includes the continuous availability/exchange of information throughout the incident handling process to stakeholders, as necessary.
- Banks must ensure that provisions exist in the CORFs for the establishment of an effective operational risk incident management process, adequately reflected in operational risk policies and procedures. Necessary escalation processes must also be established based on the materiality of the operational risk incidents so as to facilitate adequate supervision and management response.

Some more specific comments which we would like share are as follows:

- In section 3 titled "Operational risk management", the first paragraph gives a definition of operational risk which excludes reputation risk. We suggest this exclusion is removed to allow banks more flexibility on where to locate and to deal with reputational risk, e.g. as a consequence of various types of risk or as a separate risk type. It is nevertheless, worth to mention that Reputation quantitative impacts are difficult to assess and measure and should not be embedded in operational risk loss data collections nor scenario analysis.
- In section 3, paragraph 9.d: We would suggest to replace the word "providing" with "ensuring the provision". Not all CORFs have the ability to provide training. Sometimes, HR has such capabilities or an external provider is used.
- Section 3, paragraph 10: We would suggest that in "corporate control groups (e.g. compliance, Legal, Finance and IT)", "and IT" should be removed so as to avoid confusion. As per note 10 at the bottom of the page, 1.5 line of defense functions may exist depending on the complexity and nature of the bank, for quality assurance purposes under the supervision of the 2nd line of defence function.

[3] provide also a common definition for operational risk incidents, for example:
'an occurrence or a series of current or past events or a change in a particular set of circumstances which has or may create a direct (i.e. monetary & person hours lost) or indirect (e.g. liability, reputation detriment, loss of business, disruption of services) loss to the Bank, due to inadequate or failed internal processes, people and systems or from external events, i.e. being an operational risk which materialized. Incidents can be 'Near Misses' or create 'Potential Losses' or generate 'Actual Losses' (request for amendment in point 2 below relates)

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:
Lukas Bornemann
Policy Adviser – Prudential Policy and Supervision
l.bornemann@ebf.eu
+32 2 313 32 73

Dimos Karalis
Policy Adviser – Cybersecurity & Innovation
d.karalis@ebf.eu
+32 2 508 37 11