November 6, 2020

Pablo Hernández de Cos, Chairman
Carolyn Rogers, Secretary General
Basel Committee on Banking Supervision
Centralbahnplatz 2
4051 Basel
Switzerland
Via Electronic Mail

RE: Basel Committee on Banking Supervision Consultative Document 'Principles for operational resilience'

Dear Mr. Hernández de Cos and Ms. Rogers:

On behalf of the Institute of International Finance (IIF) and the Global Financial Markets Association (GFMA) ("the Associations"), we are very encouraged that the Basel Committee on Banking Supervision (BCBS) has proposed global principles for the operational resilience of financial institutions ("Consultative Document").[1] By way of background, on June 5, 2020, the Associations submitted a letter to the BCBS and other global standard-setters asking for the development of such principles given that operational resilience has been of high importance for both public sector authorities and financial institutions and has more recently come into even greater focus due to the impact of the COVID-19 pandemic.[2]

Operational resilience is extremely important for the public and private sectors to maintain confidence in the financial industry and to support financial stability and economic growth. The Associations and our global membership acknowledge the importance of operational resilience for individual institutions, and across the financial sector, in support of customers, markets and the communities and broader economies they support nationally and globally. As BCBS members and the standard-setting bodies consider the suggested principles, we encourage ongoing collaborative efforts to continuously improve and strengthen the level of operational resilience across the global financial system.

[1] BCBS 2020. "Consultative Document: Principles for operational resilience" August 6, 2020
[2] IIF and GFMA 2020. "IIF and GFMA letter to Global Standard Setting Bodies Advocating Development of Global Principles on Operational Resilience" June 5, 2020.

A key priority for our members is global coordination and alignment among policymakers and supervisors on the policy outcomes, terminology and supervisory approaches to operational resilience.[3] Global consistency was an overarching consideration in our development of five guiding principles that were published for discussion by the Associations' members on how to support the strengthening of operational resilience maturity in financial services.[4] The potential for fragmentation due to divergences in regulatory standards and supervisory oversight poses substantial risks and operational challenges for financial services firms that operate globally and, in turn, for the strength of the financial system. Approaches are currently being advanced by authorities in various jurisdictions, including Australia, Canada, the European Union, Japan, Singapore, the UK, and the U.S. As such, the industry appreciates that the BCBS has proposed global principles to strengthen operational resilience and is fostering the overall collaborative efforts between the public and private sectors on this important matter.

Our response proceeds with a summary of the overarching messages and thematic points from our feedback (pages 2-7) and detailed responses to the specific questions on the proposed principles in the Consultative Document (pages 7-15). Furthermore, we have also included an Appendix (pages 16-22) of relevant regulations and guidance that financial firms already comply with globally and that reflect the resilience capabilities firms have already developed over time.

Overarching messages:

- **Regulatory alignment and consistency** are needed, internationally and within jurisdictions, on the outcomes sought and is a key focus given that a financial firm's businesses and associated processes may span multiple geographies.

- Operational resilience should focus on the **alignment of outcomes** that promote financial and market stability as well as firm safety and soundness by protecting and resuming key services during operational disruptions, enabling firms to continue serving the needs of their clients.

- It is important to strive for a **principles-based, risk-based and outcomes-focused approach** where firms have the flexibility to determine the specifics of their own operational resilience programs in a way that is relevant and proportionate to their business and risk profile. Some of the proposed principles – e.g. business continuity planning, third party dependency management, incident mapping and ICT including cyber security – are relatively prescriptive and granular at times and would entail significant resources for implementation. Therefore, it is imperative the BCBS is sufficiently clear on what is being asked for that does not already exist in current risk management frameworks.

[3] To help facilitate these efforts, the Associations have hosted working Symposiums on operational resilience in both October 2019 and July 2020 to bring together leading members of the regulatory community (including representatives from the BCBS, CPMI, FSB and IOSCO, as well as authorities from several jurisdictions), key financial and capital market participants around the world and relevant industry trade association representatives. We also appreciate being invited to participate in similar events organized by the BCBS.

[4] IIF and GFMA 2019. "Discussion Draft Principles Supporting the Strengthening of Operational Resilience Maturity in Financial Services" October 7, 2019.

- Firms should be able to **leverage existing broader risk management frameworks**, if they choose, acknowledging that these may need to be augmented or supplemented, as necessary. If the desired outcome is achieved, firms should also not be *required* to leverage existing frameworks.

- **Continued public-private collaboration is important**, including beyond the consultation period: operational resilience maturity will be an iterative process and it will take time to embed what are some new and complex concepts with the objective of supporting regulatory consistency and comparability.

- Clarity is needed on **how the operational resilience and operational risk principles are interconnected** and related. Further clarity would help to avoid overlaps in different areas (e.g. risk appetite, taxonomy, business continuity, tolerance thresholds) and to prevent different interpretations.

- The industry needs a **thoughtful implementation timetable and overall flexibility** on how firms demonstrate resilience outcomes (i.e., principles-based, without prescribing specific metrics), allowing the necessary time for collaboration with a cross-border firm's supervisors in different jurisdictions.

- While direct oversight would be outside the scope of the BCBS, we think the final principles should recognize, the need for **sector-wide collaboration**, including financial market infrastructures (FMIs) and critical third parties, to most effectively ensure operational resilience across the financial sector.

Thematic points:

<u>Regulatory alignment and consistency are of utmost importance</u>

We recommend that the BCBS should aim to ensure:

- Alignment in approaches to demonstrate operational resilience, across firms and across jurisdictions, building on existing industry standards;
- Consistency and clarity of objectives and avoidance of duplication in relation to existing standards, regulations, and guidance of which there are many including, but not limited to, the Principles for Sound Management of Operational Risk (PSMOR) and the 2006 BCBS High-level principles for business continuity.; and,
- The BCBS should also consider with member authorities how any new terminology created as part of operational resilience policy development translates to terms that are used in existing regulatory standards, requirements, and guidelines, to the extent that they already exist. This could bring clarity while recognizing that different standard setters, regulators, and firms may use different terminology to manage to objectives sought.

We believe that aligned approaches between jurisdictions and across firms would:

- Provide a minimum agreed upon outcome objective for the definition and measurement of operational resilience, which would foster market confidence and global financial stability;
- Increase comparability across jurisdictions, enabling understanding and accurate communication;

- Minimize the impacts of cross-border disruptions and global firmwide disruptions; and,
- Result in better resilience outcomes, reduce risks, and create efficiencies for the industry and regulatory community alike.

As an example of inconsistency with other standards, under the proposed revisions to the PSMOR, the role of the board to approve and review the operational risk management framework has been removed (Principle 3), but that responsibility remains part of the Operational Resilience Principles (par. 17).

As an example of how operational resilience terminology currently differs between jurisdictions, the UK Authorities introduced the term "important business services," which is a building block in their approach.[5] The US Prudential Agencies, on the other hand, include a definition around "critical operations and core business lines," which originate from concepts used in recovery and resolution planning.[6] This is why agreeing to the same outcome objective for demonstrating operational resilience will facilitate banks with global processes to be compliant in multiple jurisdictions that use different terminology.

Principles-based, risk-based, and outcomes-focused approach

At its core, operational resilience should focus on outcomes that promote financial and market stability as well as firm safety and soundness by protecting and resuming key services during operational disruptions, enabling firms to continue serving the needs of their clients.

The proposed Principles should explain clearly what a good outcome should look like under each competence, and how that would help contribute to overall operational resilience. Clarity of expectations on how to demonstrate this would give firms a better understanding of what is novel about operational resilience expectations compared to the range of existing standards, regulations, and guidance. Given the varying degrees of granularity and resources that could be dedicated to achieving each Principle, the BCBS should give due consideration to costs vs. benefits.

Recognizing the value of the BCBS membership to provide alignment on the outcomes sought, we recommend that the final text should be principles-based, without any prescriptiveness, to support the ongoing maturity of operational resilience. Our member firms think that the proposed principles are currently too prescriptive and granular at times, and that the BCBS should focus on capabilities so that the principles remain dynamic. This applies to business continuity planning, third party dependency management, incident mapping and ICT including cyber security. The principles should focus on materiality to outcomes sought and provide institutions with the flexibility to tailor them to their respective organizations.

A principles-based and outcomes-focused approach to operational resilience should afford firms the flexibility to determine their own operational resilience approaches in a way that is relevant and proportionate to their business and risk profile. Prioritizing resources on an outcomes-focused approach would also help maintain a manageable scope of a firm's operational resilience processes and direct resource and investment to those integral to the safety and soundness of firms and financial stability.

[5] Bank of England, PRA, FCA 2018. "Discussion Paper: Building the UK financial sector's operational resilience." July 4, 2018. And 2019 package of consultation proposals from the same authorities.
[6] US Agencies 2020. "Sound Practices to Strengthen Operational Resilience." Oct. 30, 2020.

The Committee notes in the paper that it considers that previously issued guidance does not adequately capture all essential elements when considered on a standalone basis, but that it does advance operational resilience when considered collectively. Given individual jurisdictions will be measuring operational resilience in their own way, consistent regulatory outcome objectives will always be of particular importance.

Leveraging existing frameworks

Firms should be able to leverage existing broader risk management frameworks, if they choose, acknowledging that these may need to be augmented or supplemented, as necessary. As long as the desired outcome is achieved firms should also not be required to leverage existing frameworks.

In addition, while the Financial Stability Board's (FSB) Recovery and Resolution Planning (RRP) guidance is a useful frame of reference and is likely to align in many ways to a firm's operational resiliency efforts, firms should have the flexibility to decide the scope of any enhanced operational resilience measures. Firms should be able to retain significant flexibility in determining whether and how to leverage RRP processes and determinations for operational resilience purposes. We recommend that the final principles clarify that firms may consider, but are not required, to directly incorporate or replicate aspects of the RRP framework into their operational resilience approach.

See the Appendix for an indicative, non-exhaustive list of relevant regulations and guidance that financial firms already comply with globally and that reflect the resilience capabilities firms have already developed over time. These existing regimes are themselves somewhat different and fragmented across jurisdictions; to introduce further fragmentation through lack of consistent alignment on new operational resilience outcomes sought would only compound existing challenges for global firms and undermine the objective to strengthen operational resilience.

Scope and proportionality

The industry believes that a firm should be able to determine the specifics of their own operational resilience programs based on the services it delivers to customers, and proportionately to the firm's business and risk profile, including its role in the broader market. Some firms may choose to leverage their existing RRP or Enterprise Risk Management (ERM) governance structures to help identify these areas but should not be required to do so.

Scope and proportionality should be key pillars based on factors such as the firm's size, type and complexity of business operations, customers and counterparties, the markets in which they operate, and the products traded on those markets, as well as market interconnectedness.

In the areas of governance and (operational) decision-making, strategic decisions will usually be made at the board and senior level, but firms should have the flexibility to decide which decisions are taken at the appropriate level of management.

Third parties and resilience of the overall sector

The aim of operational resilience within the financial sector is ultimately to support financial stability and ensure proper functioning of markets to serve clients where they do business. The Consultative Document

focuses on individual firms but does not adequately address or recognize the challenge of systemic weaknesses across the industry where reliance is placed upon critical third parties and outsourced functions. The level of regulatory oversight between critical third parties and outsourced functions varies with some providers sitting outside of the regulatory perimeter. Critical third parties and outsourced functions should have, and some entities are already required by regulatory authorities, to demonstrate robust operational risk management and operational resilience approach to both the authorities and firms they support.[7] Please find additional feedback on third parties below (pages 10-11) regarding Principle 5.

Ongoing public/private collaboration

We encourage industry and policymaker collaboration to support sector-wide resilience at the global level. This collaboration can help to identify potential risks and gaps, given sector-wide interdependencies. This is of particular importance for cross-border products and services (e.g. wholesale payments) and firms that operate in multiple jurisdictions.

The practical application of the final BCBS principles will require further dialogue and interaction between firms and their supervisory authorities, and at the level of the global standard setting bodies given the interconnected nature of operational resilience. Given this, we recommend that the BCBS, jointly with FSB, International Association of Insurance Supervisors (IAIS), the International Organization of Securities Commissions (IOSCO) and Committee on Payments and Market Infrastructures (CPMI), regularly convene a cross-sectoral public/private working group to address ongoing interpretive issues with operational resilience. The group could serve to:

- Identify solutions to cross-border risks (e.g. lack of substitutes from a common industry utility used globally) and help promote consistency;
- Jointly assess financial stability impacts across the entire sector and share pertinent data while maintaining necessary security controls;
- Advise on key scenario exercises that would be useful and share lessons from any exercises conducted; and,
- Facilitate practical discussions on implementation (e.g. case studies and best practices.)

For sector-wide collaboration to succeed it should also include FMIs to enhance the collaboration that banks and authorities have been doing to date.

Implementation timeline

The industry views operational resilience maturity as an iterative process that will continue to evolve. Regulatory and supervisory expectations should allow for and encourage firms to consistently review and

[7] Outsourced functions are an arrangement of any form between a financial institution and a service provider by which that service provider performs a process, service, or activity that would otherwise be undertaken by the financial institution itself exclusive of the following:

- functions legally required to be performed by a service provider;
- clearing and settlement arrangements between clearing houses, central counterparties, and settlement institutions and their members;
- market information services (e.g., data provisioned for credit ratings and pricing);
- global network infrastructures (e.g., Visa);
- global financial messaging infrastructures that are subject to regulatory oversight; and
- correspondent banking services.

enhance their programs rather than focus on a static point in time for demonstrating operational resilience. Prioritizing efforts to achieve and demonstrate operational resilience should be done in collaboration with authorities on a cross-border basis to identify any current gaps where the timeline for the closure of such gaps should be based on the potential severity to both the firm and the sector rather than by a fixed date for all gaps and all firms. To address certain gaps, depending on their operational resilience maturity, some firms may need to make significant investments and major technological or organizational changes. Such changes would inevitably require a thoughtful implementation period to execute in parallel to maintaining ongoing resilience management and executing other business change programs, particularly for large firms and those operating cross-border. The BCBS should work with member jurisdictions to allow flexibility and the necessary time required for operational resilience policy approaches to stabilize rather than introducing any measures that are too prescriptive. As is true for other BCBS initiatives, it is also critical that jurisdictions are encouraged to align the implementation of their timelines, to avoid unnecessary fragmentation.

Lessons from COVID-19

As the ongoing COVID-19 crisis has highlighted, the private and public sectors must evolve from viewing risks and threats as being mostly business-specific or geography-specific to thinking about risk and infrastructure on a genuinely global and systemic basis. Banking systems globally entered this crisis having built up a high level of resilience and they have been able to maintain confidence through this highly uncertain period. In response to Question 3 of the Consultative Document, we offer some initial observations related to operational resilience during the COVID-19 crisis. We would like to emphasize that, while the COVID-19 experience is naturally top of authorities' and firms' minds at present, we think the BCBS Principles should be capabilities-driven and agnostic towards exact scenarios. No one can predict the next event, and flexibility is required to respond appropriately to a range of possible disruptions. As such, paragraph 41 of the Consultative Document is perhaps too specific by focusing on "remote access" and "remote user connections".

Responses to the specific questions in the Consultative Document:

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?

Yes, generally the proposed Principles (i) capture the necessary requirements, (ii) allow for flexibility in implementation, and (iii) are sufficiently forward-looking.

However, the BCBS should consider (i) areas of interpretive issues, (ii) resources required to reach a sufficient outcome, (iii) granularity of the information required (e.g. mapping), and (iv) clearly articulating in what way these principles are different from, or leverage, existing guidance to explain what outcomes are expected.

We think the BCBS principles should help firms to clearly evidence operational resilience as an outcome; we think how to demonstrate this could be more clearly specified under each Principle.

We support further explanation of certain concepts to avoid potential misunderstanding across authorities or firms, including:

- Critical operations, and degree of cross reference to Recovery and Resolution Planning (RRP) terminology;
    - We need a clearer definition of “critical operations” as paragraph 13 says it is being expanded to include “critical functions”, whereas footnote 12 on that same page refers back to “critical operations” in existing RRP terminology;
- Risk appetite, risk capacity and risk tolerance; and,
- Definition of criticality, e.g. critical vs. important.

These definitional issues would require practical discussions around examples (e.g. risk tolerance and risk appetite have not generally been used in a resilience construct.)

Finally, harmonization and alignment with RRP is indeed relevant but it would be useful for firms to have flexibility to determine to what extent this harmonization should be done, and what to do in cases where a critical operation is identified for operational resilience, but not for resolution planning, given that the underlying policy drivers for each are based on different scenarios and assumptions.

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

Principle 1: Governance

The Associations are supportive of this principle as it was designed to ensure that operational resilience is integrated into the existing governance structure and normal operations across the firm. We agree that board-level oversight is crucial in the successful implementation of an operational resilience approach.

Due consideration should be given to multinational banks, at which reporting/board oversight span multiple legal entities and governance structures. As stated before, while strategic firm-wide decisions would ultimately be made at the board and senior level, firms should enjoy the flexibility to decide the appropriate level for decisions to be taken, for example around implementation decisions.

Efficient and effective data aggregation and reporting processes rely on a common and consistent taxonomy. It is challenging to aggregate data unless there is a globally consistent and firm-wide way of expressing the key features. This also aligns with points on metrics (below). Furthermore, paragraph 19 refers to a firm’s business units, not critical operations. The Associations seek clarity on whether this refers to existing management information or whether this data would need to be reframed at the operational resilience level.

While in the definition of Operational Resilience there is a clear mention of prevention and detection of potential failures, the governance focuses solely on the response and mitigation of an ongoing disruption.

The draft principles introduce "risk tolerance for disruption considering the firm’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 therefore the firm would be "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 firm can assume before breaching its constraints (regulatory capital and liquidity needs). Through the ongoing public/private collaboration this should be a focus of discussion once authorities agree the global outcomes being sought.

Principle 2: Operational Risk Management

In general, it is important that the BCBS clarifies the relationship between operational risk and operational resilience, and how to think about operational risk management in the context of resilience. Refer to response to Question 4 for more detail.

Further, more clarity is needed on how this Consultative Document is related to the BCBS Consultative Document "Revisions to the principles for the sound management of operational risk" since these two documents are overlapping on several items (e.g. risk appetite, taxonomy, business continuity, tolerance thresholds, etc.).[8] These definitions and functions should be defined in the same way to avoid different interpretations or implementations.

It would also be useful to explain in more detail the difference between operational risk scenarios and operational resilience scenarios. Further clarity is needed on how operational resilience links to the Risk Control Self-Assessment.

Principle 3: Business Continuity Planning and Testing

This is one of the areas where the proposed principles are relatively prescriptive. The Associations would appreciate clarity on what is being asked from firms here and how it is different from existing standards and requirements. Perhaps "Testing" can also be expanded to "Testing / Exercising" which is broader than only testing.

We also seek clarification on how Business Continuity Plans intersect with third-party recovery plans. Appropriate consideration should be given to what would lead to an outcome of operational resilience, whilst taking into account, as mentioned previously, that an individual firm would not have full visibility of all relevant risks to financial stability or critical points of failure across the industry.

Although not discussed in the Consultative Document, testing could be conducted both at the level of individual firms as well as at the level of the financial sector to support preparedness and identify interconnections and potential market dependencies. The industry believes scenarios should reflect the fact that incidents do not stop at borders and that there are interdependencies between financial sector participants and other important sectors. Eventually, scenario testing could be conducted with financial institutions' critical third parties and outsourced functions. This is another important reason for ongoing global collaboration and the necessity for alignment of outcomes sought.

Principle 4: Mapping interconnections and interdependencies

The expectation outlined in the Consultation is for firms to map out what is needed to deliver critical operations, and a process for keeping maps current. We would appreciate further clarification on the mapping of "information" and "interconnections" and what role firms play in that exercise. Mapping, the way it is currently presented in the draft BCBS principles could be resource-intensive for firms to develop, and maps for recovery and resolution planning could be of limited help as those were designed with financial resilience in mind. While it is helpful that recovery and resolution plans can be leveraged, they

[8] BCBS 2020. "Revisions to the principles for the sound management of operational risk" August 6, 2020.

are developed at a different level of granularity and focus (i.e., financial resilience) than what the BCBS seems to have in mind for operational resilience.

It is important to ensure that the level of granularity of mapping, as well as the resources needed to refresh and sustain the mapping itself, is commensurate with the outcome to be achieved.

In some cases, authorities are already doing this, and they have a better ability to connect the different organizations across the financial system. Firms would not be aware of whether other firms are dependent on the same third party. This is also true for determining concentration risk, which requires a broad view of the sector, and (as also discussed under Principle 5) would be better suited to be undertaken by the relevant regulators.

Principle 5: Third-party dependency management

This is another area where the proposed principles are relatively prescriptive. The Associations would appreciate clarity on what is being asked from firms here and how it is different from what already exists.

The Consultative Document focuses on individual firms but does not adequately address or recognize the challenge of systemic weaknesses across the industry where reliance is placed upon critical third parties and outsourced functions. The level of regulatory oversight between critical third parties and outsourced functions varies with some activities sitting outside of the regulatory perimeter. Critical third parties and outsourced functions should be encouraged, and typically are required, by their appropriate regulatory authorities to have a robust operational risk management and resilience approach that provides sufficient assurance to both the authorities and firms they support. Exposure to third parties that sit outside the regulatory perimeter requires policy makers and the industry to develop a solution.

Specifically, while some of the risks associated with the use of and reliance on unregulated third parties can be addressed through contractual negations, this solution is incomplete. The ability of firms to require transparency and impose operational resilience requirements in written agreements with third parties may be predicated upon choice in the marketplace, size of the financial institution, and level of service agreement. In some areas of critical third-party services, there is a limited set of vendors with market dominance who provide valuable services, which also limits firms in their ability to negotiate contractual terms.[9]

While firms recognize the importance of balancing concentration risk of third-parties, which can have a direct impact on overall stability, it would be incumbent on the respective authorities to determine this overall risk, as firms themselves would not have an accurate overview of which providers are being used by other firms across the industry. Recognizing these practical limitations, the regulatory perimeter needs to ensure outcome objectives agreed to by the BCBS for operational risk and operational resilience apply to financial institutions, and the providers of functions and services to the financial industry.

We recommend that the BCBS engages with the other global standard-setting bodies across the financial services sector to consider the interdependencies across the global financial system and establish common outcomes across sectors. While firms recognize the importance of avoiding concentration risk,

[9] GFMA Consultation Response: IOSCO Principles on Outsourcing (September 2020)

which can impact overall stability, it would be incumbent on the respective authorities to determine this risk, as firms themselves would not have an accurate overview of which providers other firms could be using. In the area of scenario testing, which will also be discussed in more detail below, it is also critical to include critical third parties and outsourced functions given their importance to the financial sector. Lastly, the level of regulatory oversight between critical third-party providers and outsourced functions varies with some activities sitting outside of the regulatory perimeter. Given this disparity, it is important that ongoing sector collaboration and public/private partnership continues to drive a consistent and effective operational resilience framework across these groups. We therefore recommend that the BCBS engage with the other global standard-setting bodies across the financial sector to consider the interdependencies across the global financial system and establish common outcomes across sectors.

Due consideration needs to be given to alignment and consistency with existing regulations, e.g. BCBS outsourcing guidance[10], as well as existing operational risk and technology risk guidelines. It is unclear how these principles differ from existing third-party management frameworks already being used by regulated entities, which already require third parties to have resilience planning in place.

For example, there is no definition of how "criticality" is determined although Paragraph 10 of the Consultative Document seems to suggest that Critical Operations could encompass those services which are outsourced, critical for recovery and resolution planning, as well as critical within the firm's own risk management framework.

In addition, in respect to paragraph 32 on respective functions performing risk management and due diligence, and taking into account Principle 2, the proposed language suggests that the risk assessment and due diligence should leverage a firm's existing framework for the management of operational risk to identify external and internal threats and vulnerabilities. However, it would be helpful to clarify how the risk assessment and due diligence expectations for operational resilience differ from or are additive to the existing guidance regarding the risk assessment and due diligence of third parties for regulated entities.

Further clarification would also be useful to understand the due diligence expectations for intra-group entities given that the ability to control or mitigate the risks are greater than those applicable to third parties. Intra-group outsourcing arrangements are already covered within existing guidance. Further guidance would be helpful to understand if this is intended to broaden beyond intra-group outsourcing or reliance upon intra-group entities for critical services as defined by Recovery and Resolution Planning.

Principle 6: Incident management

Existing frameworks in this area are robust, and firms should ensure they continue to test/exercise them against severe but plausible scenarios to build confidence of their effectiveness during real events.

Another area where clarity would be helpful is the connection between ICT and non-ICT risks, and what is the scope of the incidents being covered here. We would also appreciate additional guidance around the scope of BCBS incident reporting expectations given the many possible types of incidents and overlap with some existing reporting requirements. For example, FSB has just released its own final report on Effective Practices for Cyber Incident Response and Recovery.[11]

[10] BCBS 2005. "Outsourcing in Financial Services." Feb. 15, 2005.
[11] FSB 2020. "Effective Practices for Cyber Incident Response and Recovery: Final Report" Oct. 19, 2020. Please also see the FSB consultation responses by GFMA (July 20, 2020) and IIF (July 20, 2020.)

Further clarification would be helpful to distinguish incident management from crisis management. Crisis management 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: ICT including cyber security

It is not entirely clear why ICT including cyber security merits its own principle. There are other resources at firms, including facilities and staff management, that are also important but have not been afforded their own principles.

This principle should be flexible enough to capture risks arising from emerging technologies. Paragraph 41 is very specific to remote access (which seems to be targeted at a prolonged COVID-19 scenario and should be more agnostic) while other paragraphs are more generic. This comment also complements the last sentence in the response to Q3 below, which suggests keeping principles agnostic of scenarios. Perhaps the working of remote access could be merged with paragraphs 39 and 40 and made more generic to say that it is one of the considerations.

It would also be beneficial for the draft principles to reference common ICT capabilities that are of particular interest for operational resilience, including change management, capacity management, logical and physical security, backup management, environmental controls, etc.

***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?*

As the ongoing COVID-19 crisis has highlighted, the private and public sectors must evolve from viewing risks and threats as being mostly business-specific or geography-specific to thinking about risk and infrastructure on a genuinely global and systemic basis.

Banking systems globally entered this crisis having built up a high level of financial and operational resilience and they have been able to maintain confidence through this highly uncertain period. As remarked by the Bank for International Settlements: *"The pandemic was a tremendous shock that rocked financial markets. The good news is that the banking sector was not at the epicenter - banks proved to be resilient enough to be part of the solution this time around, rather than being part of the problem."*[12]

In a recent speech, Wayne Byres, Chair of the Australian Prudential Regulation Authority (APRA), also said that COVID-19 has been a "very real test of banks' operational resilience" and that over the past six months "there has been no significant degradation of services provided to customers."[13] He also identified

[12] BIS 2020. "Rebuilding better: Banks, central banks and governments in a Covid economy" Panel remarks by Agustín Carstens, General Manager, Bank for International Settlements, at the Santander International Banking Conference 2020. October 7, 2020.
[13] APRA 2020. "APRA Chair Wayne Byres - Remarks to the BCBS outreach meeting on operational resilience." Oct. 16, 2020.

a number of initial lessons learned, around: board oversight of risks exceeding risk tolerance levels; the robustness and breadth of business continuity plans; increased risks to information security; impact of change freezes and deferrals; reliance on third-party service providers; ability to test contingency arrangements; and, the human toll of an extreme environment.

Firms are also continuing to assess the lessons learned from the ongoing pandemic, and our members consider that the COVID-19 crisis has underscored the importance of further global consistency and coordination in the policies designed to enhance operational resilience effectiveness and on the intrinsic need for a cross-sectoral alignment on outcomes sought.

Some other initial observations around COVID-19 and operational resilience would include:

Importance of public/private collaboration: firms acknowledge on the importance during periods like this of increased public/private collaboration, including with government agencies and health experts, to elevate the quality and speed of the response.

Remote working arrangements: human capital was put to the test during COVID-19. The pandemic challenged a wide breadth of people (and therefore staffing) as well as people's working habits. From a very human and practical perspective, firms have had to consider the impacts resulting from differing family, health, and economic circumstances amongst its staff.

Acceleration of digital measures and protocols: changes to measures/protocols were required to enable work from home *en masse*. This accelerated digital solutions for tasks that were previously conducted in person, such as "wet signature" requirements.

Third-party dependencies: given the impact of COVID-19 is global and affected every sector, firms had to understand their dependencies on third parties. Firms have had to rely on third parties' recovery plans and assess the level of information they can be reasonably comfortable with.

Ability to scale technology: firms quickly had to scale technology to support staff and address logistical issues with equipment. Firms learned that Business Continuity Plans were useful, but that the planning assumptions could in some cases be incorrect as the technological challenges developed faster than many would have expected. This provided an effective test of their ability to respond and demonstrate what effective crisis response management would entail.

Cyber: cyber threats also emerged rapidly, with new threat vectors exploiting the healthcare element of the crisis. The cyber space is very fast-moving and opportunistic, and cyber adversaries were quick to take advantage of the pandemic and target customers from a social engineering standpoint. It was important to maintain heightened awareness and regular communication to staff warning them of the risks.

Nevertheless, even though the COVID-19 experience is naturally top of authorities' and firms' minds, we think the BCBS Principles should be capabilities-driven and agnostic towards exact scenarios as we cannot predict the next event. Additionally, flexibility is required to respond appropriately to a range of possible disruptions.

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

No, we would support keeping the relevant principles on operational risk and operational resilience separate given that they are distinct from reach other as separate discipline areas and usually also contained and considered in different parts of firms, especially at the operational levels.

However, we recognize the importance of the connections between the two documents, and they should be consistent and aligned where appropriate. The BCBS should also consider a simplification of some of the principles, including cross-references between both sets of principles avoiding duplication where possible to streamline and to emphasize where a principle reflects operational risk or operational resilience objectives. Such streamlining is helpful recognizing different standard setters, regulators and firms may use different terminology to manage to objectives sought. It is important for the BCBS to provide more clarity on how the two areas interact and where the demarcation lines are. Traditionally, operational risk is concerned with reducing risk through preventative measures. We understand that operational resilience, however, is an outcome and requires an approach that assumes that a given risk has crystallized, hence the focus on the ability to respond, recover and learn from disruptive events. Currently, the role of a firm's operational risk management in recovery measures is unclear and clarity is important as this has not traditionally sat within operational risk frameworks.

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

Metrics will ultimately be devised by standard-setters and regulators but from an industry perspective, and as indicated in the Consultative Document, more work is needed to assess the appropriate role of various metrics in the context of operational resilience. Both authorities and industry see the development of operational resilience as an iterative process; we would encourage future private/public sector forums to consider these issues and to discuss the value of metrics and how they can best be employed. If the BCBS intend to create industry-wide metrics, we would encourage it to consult in detail beforehand.

While there are several metrics used within the industry for the separate disciplines under the Principles, this is an area that requires very careful consideration not least due to several factors:

- The appropriateness and effectiveness of metrics vary for each discipline
- The purpose / quality / usefulness of metrics needs to be made clear and outcomes driven
- There could also be several metrics for thing being measured (e.g. end of life metrics)
- Metrics can also be split into those that are lagging (historic) and those that are leading (control effectiveness) indicators
- Metrics can represent and apply to either key controls or key risks. It is often difficult for metrics to reflect the aggregation of risks
- Metrics should not breach principles of competition.

The industry thinks it is crucial to maintain flexibility for individual firms to use and evolve metrics over time as part of their operational resilience programs. The industry thinks that prescriptiveness surrounding any mandatory metrics for regulatory or supervisory purposes should be avoided. The industry believes that regulators and supervisors should review evidence as to how firms are managing their own risk and not be prescriptive on metric design and definitions. Defining metrics would not allow

for the nuances across firms to be addressed, makes it more complex to make any in-flight changes during an incident, and any necessary changes to the metrics could be slow and bureaucratic. Providing firms with the necessary flexibility to account for the way different scenarios affect their most important business activities, clients, business and broader markets and financial stability is important rather than having an excessive focus on technical resumption decisions driven by certain metrics. The Associations and our members stand ready to work with standard-setters and regulators to formulate effective, repeatable, and globally applicable metrics.

Concluding remarks

The IIF and GFMA reiterate our members' support for advancing operational resilience in the global financial sector, and we hope our feedback is helpful in enhancing the conversation on operational resilience. It is widely recognized that strengthening operational resilience will be an iterative process that requires effective collaboration among financial institutions and regulators around the world on an ongoing basis. The focus must always be on delivering tangible, outcomes-focused results that achieve genuine resilience enhancements. Continuing this collaborative engagement with a focus on the outcomes for clients, markets and financial stability gives the highest chance of success.

As always, we are available to provide any necessary expansions and/or clarification on our comments, and we welcome future continued dialogue with the BCBS and your respective members on how supervisors and market participants may move forward most effectively to further support operational resilience across the financial sector.

Yours sincerely,

Allison Parent
Executive Director
Global Financial Markets Association (GFMA)
aparent@gfma.org

Martin Boer
Director, Regulatory Affairs
Institute of International Finance (IIF)
mboer@iif.com

APPENDIX

This appendix of financial regulations does not include the BCBS proposal, which is the subject of the main letter, but includes other relevant documents for context.

Financial Regulations and Resilience Capabilities by theme/functional area		
Functional Area	**Regulation/Guidance**	**Resilience Capabilities**
Operational resilience	Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) – Building Operational Resilience: Impact tolerances for important business services (December 2019)	• The proposals aim to improve the operational resilience of firms and protect the wider financial sector and UK economy from the impact of operational disruptions. • It addresses risks to operational resilience including those arising from the interconnectedness of the financial system, and the complex and dynamic environment in which firms operate. Proposals are relevant to credit institutions, insurers, certain investment firms and FMIs. • The PRA considers that there is a need for a proportionate minimum standard of operational resilience that incentivizes firms to prepare for disruptions and to invest where it is needed. • Expect firms and FMIs to identify "important business services" and set "impact tolerances" for each of these services.
	Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency - Sound Practices to Strengthen Operational Resilience (October 2020)	• The paper outlines practices to increase operational resilience that are drawn from existing regulations, guidance, statements, and common industry standards. • The practices are grounded in effective governance and risk management techniques, consider third-party risks, and include resilient information systems. The paper does not revise the agencies' existing rules or guidance. • The practices are for domestic banks with more than $250 billion in total consolidated assets or banks with more than $100 billion in total assets and other risk characteristics.
	Monetary Authority of Singapore (MAS) - Ensuring Safe Management and Operational Resilience of the Financial Sector (2020)	• Issue guidance and advisories to address operational, technology and cyber risks. • Focus our surveillance, supervision, and enforcement efforts on financial institutions' pandemic response as well as operational and cyber resilience. • Continue to monitor the impact of COVID-19 and put in place additional measures and advisories, as necessary.
	European Commission – Digital Operational resilience framework for financial services (December 2019)	• Propose targeted improvements of ICT and security risk management requirements. • Harmonize reporting of ICT incidents. • Develop a harmonized digital operational resilience testing framework. • Enhance oversight of critical third-party providers.
Risk Governance	Basel Committee on Banking Supervision (BCBS) – Corporate Governance Principles for banks (July 2015)	• Ensure sound and robust corporate governance by determining allocation of authority and responsibilities, including: i/ setting the banks strategy and objectives; ii/ selecting and overseeing personnel; iii/ operating the bank on a day-to-day; iv/ protecting recognized stakeholders; v/ aligning corporate culture; vi/ establishing control functions. • Reinforce the collective oversight and risk governance responsibilities of the board (e.g. risk governance, risk culture, risk appetite, risk capacity). • Evaluating and promoting a strong risk culture in organizations.

	Financial Conduct Authority (FCA) - The Senior Managers and Certification Regime (July 2019)	• Provide a robust framework for accountability and transparency. • Ensure accountability from the most senior individual responsible for managing the internal operations and technology of a firm.
	Federal Reserve Board (FRB) – 'Three Lines of Defense' Risk Management Model	• Ensure systemically important financial institutions (SIFIs) manage risk in a way that is prudent and consistent with their business strategy and risk tolerance. • Clarify the responsibility of the executive management team in managing the overall risk framework.
	The Office of the Comptroller of the Currency (OCC) - Heightened Standards for Large Financial Institutions (September 2014)	• Guidelines to strengthen the governance and risk management practices of large financial institutions. • The guidelines provide that covered institutions should establish and adhere to a written risk governance framework to manage and control its risk-taking activities. • The guidelines also provide minimum standards for the institutions' boards of directors to oversee the risk governance framework.
	IAIS – Application Paper on Proactive Supervision of Corporate Governance (February 2019)	• calls upon insurance supervisors to be forward-looking, identify issues early and to act quickly and constructively to address circumstances before they become critical or a violation of law or local requirements.
Risk Monitoring and Management	FSB – Principles for an effective risk appetite framework (November 2013)	• The FSB Principles set out key elements for: (i) an effective risk appetite framework, (ii) an effective risk appetite statement, (iii) risk limits, and (iv) defining the roles and responsibilities of the board of directors and senior management. • The Principles aim to enhance the supervision of systemically important financial institutions but are also relevant for the supervision of financial institutions and groups more generally, including insurers, securities firms, and other non-bank financial institutions.
	Basel Committee on Banking Supervision (BCBS) - Principles for the Sound Management of Operational Risk (June 2011)	• Ensure that financial institutions identify risks to the bank and measure exposures to those risks (where possible), and ensures that an effective capital planning and monitoring program is in place to monitor risk exposures and corresponding capital needs on an ongoing basis, take steps to control or mitigate risk exposures and report to senior management and the board on the bank's risk exposures and capital positions.
	Basel Committee on Banking Supervision (BCBS) - Revisions to the principles for the sound management of operational risk (August 2020)	• Review principles that have not been adequately implemented, and issue further guidance to facilitate implementation (e.g. risk identification and assessment tools, change management programs and processes, implementation of the three lines of defense, senior management oversight, articulation of operational risk appetite and tolerance statements, risk disclosure). • Capture additional important sources of operational risk, such as those arising from information and communication technology (ICT) risk, warranting the introduction of a specific principle on ICT risk management.
Busines Continuity Planning, Systems	The Joint Forum (BCBS, IOSCO, IAIS) – High-Level Principles for Business Continuity (August 2006)	• Ensure the development of recovery objectives that reflect the risk an event represents to the economy. • Require the conducting of periodic tests of business continuity plans to ensure the plans are effective.

Integrity and Third-Party Resilience	The Joint Forum (BCBS, IOSCO, IAIS) – Outsourcing in Financial Services (February 2005)	• Reduce potential for over-reliance on outsourced activities that are critical to the ongoing viability of a regulated entity (e.g. draw up comprehensive and clear outsourcing policies, establish effective risk management programs, require contingency planning by the outsourcing firm, negotiate appropriate outsourcing contracts, and analyze the financial and infrastructure resources of the service provide). • Mitigate concerns by ensuring that outsourcing is adequately considered in firm assessment whilst taking account of concentration risks in third party providers when considering systemic risk issues.
	IOSCO – Principles on Outsourcing: Consultation Report (May 2020)[14]	• Set out expectations for regulated entities that outsource tasks, along with guidance for implementation. • Seven fundamental principles covering issues such as the definition of outsourcing, assessment of materiality and criticality, affiliates, sub-contracting and outsourcing on a cross-border basis.
	Federal Financial Institutions Examination Council (FFIEC) –Business Continuity Guidelines	• Decrease the likelihood that disruptions will have a material and long-lasting impact on critical business services. • Require institutions to assess all business functions, identify the impact of business disruptions and estimate maximum allowable downtime and recovery time objectives.
	Federal Financial Institutions Examination Council (FFIEC) - Information Technology Examination Handbook: Business Continuity Management	• Describe principles and practices for IT and operations for safety and soundness, consumer financial protection, and compliance with applicable laws and regulations. • Focus on enterprise-wide, process-oriented approaches that consider technology, business operations, testing, and communication strategies critical to the continuity of the entire entity.
	Federal Reserve System, U.S. Treasury Office of the Comptroller of the Currency, and the Securities and exchange Commission (SEC) – Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (April 2003)	• Ensure rapid recovery and timely resumption of critical operations and staff following a wide-scale disruption for firms that play significant roles in critical financial markets. • Require firms a high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible.
	Monetary Authority of Singapore (MAS) - Business Continuity Guidelines (June 2003)	• Ensure BCM is a risk-based framework that addresses operational risk by developing clear policies, strategies, and accountabilities for the recovery of critical business functions.
	Monetary Authority of Singapore (MAS) – Proposed revisions to guidelines on Business Continuity Management (March 2019)	• Set expectations of how an FI's are to identify business functions that are critical and prioritize for recovery in disruption. • Place greater emphasis on the Board of directors and senior management to demonstrate leadership and commitment in building an organizational culture that embeds business continuity. • Expect FIs to have in place end-to-end business continuity plans for each service that is delivered to their customers.

[14] GFMA responded to the IOSCO consultation report on Principles for Outsourcing on September 30th, 2020. Please find the response here: https://www.gfma.org/wp-content/uploads/2020/09/gfma-response-iosco-principles_on_outsourcing_cp.pdf.

		• Continue to expect an FI to conduct different types of testing to gain the confidence that they will be able to continue to operate reliably, responsively, and efficiently as planned.
	Security Exchange Commission (SEC) – Regulation Systems Compliance and Integrity (Regulation SCI) (February 2015)	• Requires SCI entities (including registered clearing agencies) to establish written policies and procedures reasonably designed to ensure their systems have levels of capacity, integrity, resilience, availability, and security adequate to maintain their operational capability. • Require SCI entities to mandate participation by designated members or participants in scheduled testing of the operation of their BC/DR plans, including backup systems, and to coordinate such testing on an industry- or sector-wide basis with other SCI entities. • Require SCI entities to develop business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse to ensure next business day resumption of trading and two-hour resumption of clearance and settlement services following a wide-scale disruption.
	European Banking Authority (EBA) - Outsourcing Guidelines (February 2015)	• Set standards for the management of outsourcing risk. • Define requirements for competent authorities to effectively supervise financial institutions' outsourcing arrangements, including identifying and monitoring risk concentrations at individual service providers and assessing whether or not such concentrations could pose a risk to the stability of the financial system.
	European Securities Market Authority (ESMA) - Draft Guidelines on Outsourcing to Cloud Service Providers (June 2020)	• Develop guidance on outsourcing to cloud service providers. • Support firms identify, address, and monitor the risks that may arise from their cloud outsourcing arrangements.
	Prudential Regulatory Authority (PRA) – Outsourcing and third party risk management (December 2019)	• Complement proposals on operational resilience. • Facilitate greater resilience and adoption of the cloud and other new technologies. • Implement EBA 'Outsourcing Guidelines' with consideration to, proportionality, governance / record keeping, outsourcing arrangements, data security, access / audit / information rights, sub-outsourcing, business continuity / exit planning.
	EIOPA – Guidelines on Outsourcing Cloud Service Providers (February 2020)	• EIOPA Guidelines provide direction on cloud services and outsourcing, including the need for: a thorough pre-outsourcing analysis and risk assessment; a written outsourcing policy; notification to the supervisory authority of the outsourcing of critical or important operational functions and activities to Cloud Service Providers (CSPs); documentation requirements; due diligence and contractual considerations; exit strategies; access and audit rights; and data and system security.
Cyber Resilience and Risk Management	FSB – Cyber Lexicon (November 2018)	• Set of 50 core terms related to cyber security and cyber resilience. • Support the work of the FSB, standard-setting bodies, authorities, and private sector participants, to address financial sector cyber resilience.
	FSB – Effective Practices for Cyber Incident Response and Recovery (April 2020)	• Provide a toolkit of effective practices to assist financial institutions before, during and after a cyber incident. • Set 46 effective practices, structured across: i/ Governance; ii/ Preparation; iii/ Analysis; iv/ Mitigation; v/ Restoration; vi/ Improvement; vii/ Coordination and communication.
	G7 - Fundamental Elements of	• Require firms to identify functions, activities, products, and services — including interconnections, dependencies, and third parties —

	Cybersecurity for the Financial Sector (October 2016)	prioritize their relative importance and assess their respective cyber risks. • Require firms to identify and implement controls — including systems, policies, procedures, and training — to protect against and manage cyber risks within the tolerance set by the governing authority.
	G7 – Fundamental Elements for effective assessment of Cybersecurity in the Financial Sector (October 2017)	• Describe desirable outcomes for mature entities: i/ G7 fundamental elements are in place; ii/ cybersecurity influences organizational decision-making; iii/ understanding that disruption will occur, iv/ an adaptive cybersecurity approach is adopted; v/ there is a culture that drives secure behaviors. • Provide assessment components for assessors, to develop approach to assessing progress as entities build and enhance their cybersecurity: i/ establish clear assessment objectives; ii/ set and communicate methodology and expectations; iii/ maintain a diverse and process for toolkit selection; iv/ report clear findings and concrete remedial actions; v/ ensure assessments are reliable and fair.
	G7 – Fundamental Elements for threat-led penetration testing (October 2018)	• Provide guidance for the assessment of resilience against malicious cyber incidents through simulation and testing (Threat-Led Penetration Testing). • Enhance and assess cyber resilience of entities in the financial sector through guidance on: i) scoping and risk management; ii) resourcing; iii) threat intelligence; iv) penetration testing; v) close and remediation; vi) thematic data.
	Bank of England (BoE) CBEST (2016) European Central Bank (ECB) TIBER-EU (May 2018)	• Provide standard approaches for regulatory-driven penetration testing regimes.
	European Central Bank (ECB) Cyber Resilience Oversight Expectations for Financial Market Infrastructures (CROE) (December 2018)	• Set standards for the management of cybersecurity risks. • Provide FMIs with detailed steps on how to operationalize the guidance, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time. • Provide overseers with clear expectations to assess the FMIs for which they are responsible. • Provide the basis for a meaningful discussion between the FMIs and their respective overseers.
	IAIS – Application Paper on Supervision of Insurer Cybersecurity (November 2018)	• Provides 7 elements of insurer cybersecurity practices: a strategy and framework; governance; risk and control assessment; monitoring; response; recovery; information sharing and continuous learning. • The Application Paper also includes supervisory case studies of effective practices. It notes that cyber resilience must be achieved by all insurers, regardless of size, specialty, domicile, or geographic reach. Supervision of cyber resilience should be proportionate, and risk based.
Technology Risk Management	European Banking Authority (EBA) – Guidelines on ICT and security risk management (November 2019)	• Sets minimum standards for the management of Information and Communication Technology (ICT) and security risk management. • Sets expectations in relation to governance, the risk assessment process, information security requirements, ICT operational management, security in the change and development processes and business continuity management to mitigate ICT and security risks.
	Monetary Authority of Singapore (MAS) - Guidelines on Risk Management Practices –	• Guidance on the oversight of technology risk management, security practices and controls to address technology risks.

	Technology Risk (June 2013)	
	IAIS – Application Paper on the Use of Digital Technology in Inclusive Insurance (November 2018)	• Discusses digital technology applications in an inclusive insurance context and how the Insurance Core Principles can be applied in a proportionate manner in the supervision of the use of digital technologies in inclusive insurance. An Annex to the paper discusses the risks manifest in digital technology applications.
FMI Resilience	The International Organization of Securities Commissions (IOSCO) Principles for Financial Market Infrastructures (PFMI) (April 2012)	• Ensure the security of critical functions and, in the event of a disruption, recovery of operational capacity in a timely manner. • Require review of the entity's material risk exposure because of interdependencies with other entities. • Require identification of events that prevent an entity from providing its critical operations and services as a going concern.
	Committee on Payments and Market Infrastructures (CPMI) & International Organization of Securities Commissions (IOSCO) - Guidance on Cyber Resilience for Financial Market Infrastructures (June 2016)	• Supplemental details, on top of the Principles for Financial Market Infrastructures (PFMI) [see row above], related to the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities with the objective of limiting the escalating risks that cyber threats pose to financial stability. • Outlines 5 risk management categories that should be addressed across FMI's cyber resilience framework: governance; identification; protection; detection; and response and recovery. Also outlines 3 overarching components: testing; situational awareness; and learning and evolving.
Stress Testing	BCBS – Stress Testing Principles (October 2018)	• The principles are guidelines that focus on the core elements of stress testing frameworks. These include the objectives, governance, policies, processes, methodology, resources, and documentation that guide stress testing activities and facilitate the use, implementation, and oversight of stress testing frameworks.
	Bank of England - The Bank of England's approach to stress testing the UK banking system (October 2015)	• Stress tests therefore contribute to the Financial Policy Committee's statutory objective to protect and enhance the stability of the UK financial system, and, subject to that, support the economic policy of the Government. Equally, they contribute to the PRA's general objective to promote the safety and soundness of the banks it regulates, and its secondary objective to facilitate effective competition in the markets for services by the banks it regulates.
	Federal Review Board (FRB) - Comprehensive Capital Analysis and Review (CCAR)	• Ensures that banks have adequate capital to absorb losses and are able to lend to households and businesses even in a severe recession. • Ensures that the largest and most systemically important financial institutions are able to continue to operate under severe economic stress conditions. • Promotes financial resilience that indirectly supports operational resilience by ensuring necessary resources to support operational capacity.
	Federal Review Board (FRB) - Comprehensive Liquidity Analysis and Review (CLAR)	• Ensures the largest and most systemically important financial institutions' ability to continue to operate under severe liquidity stress. • Requires firms to assess the adequacy of their liquidity positions relative to their unique risks and tests the reliability of these institutions' approaches to managing liquidity risk. • Promotes financial resilience that indirectly supports operational resiliency by ensuring necessary resources to support operational capacity.

Recovery and Resolution	FSB - Guidance on Arrangements to Support Operational Continuity in Resolution (August 2016)	• Identify a number of arrangements including specific contractual provisions, access arrangements and governance structures that, if implemented appropriately, could support operational continuity in resolution.
	FSB - Key Attributes of Effective Resolution Regimes for Financial Institutions (October 2014)	• Set out core elements considered to be necessary for an effective resolution regime.
	FSB - Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services (July 2013)	• Provide basis for a strategic analysis that identifies firm's essential and systemically important (or "critical") functions. • Assist evaluation of firm's criticality of functions. • Promote common understanding of which functions and shared services are critical by providing shared definitions and evaluation criteria.
	European Commission - Bank Recovery and Resolution Directive (2014)	• Ensure continuity of banks and maintaining financial stability by: i/ requiring banks to prepare recovery plans to overcome financial distress; ii/ restoring viability of parts or all of the bank. • Grant national authorities powers to ensure an orderly resolution of failing banks with minimal costs for taxpayers.
	Bank of England (BoE) - Recovery and Resolution Planning (2013)	• Ensure continuity of banks and maintaining financial stability by: i/ requiring banks to prepare recovery plans to overcome financial distress; ii/ restoring viability of parts or all of the bank. • Grant national authorities powers to ensure an orderly resolution of failing banks with minimal costs for taxpayers.
	Federal Review Board (FRB) – Resolution Plan requirement under Regulation QQ (November 2011)	• Ensure the resilience and resolvability of globally systemic important banks (G-SIBs) without interruptions to the banks' critical operations and economic functions.... in a manner that substantially mitigates the risk that the failure of the bank would have serious adverse effects on financial stability
	IAIS – Application Paper on Recovery Planning (November 2019)	• Addresses governance, elements of a recovery plan and supervisory considerations, with an overarching focus on proportionality. The objective of a recovery plan should be to aid the insurer in understanding its own risks from a severe stress scenario and to be better prepared with an effective response and ensure timely activation and implementation of that response.
	FSB – Key Attributes Assessment Methodology for the Insurance Sector (August 2020)	• Provides a methodology for assessing the implementation of the Key Attributes of Effective Resolution Regimes for financial institutions in the insurance sector and applies to any insurer that could be systemically significant or critical if it fails (i.e. where the failure of the insurer could lead to a disruption of services critical for the functioning of the financial system or the real economy). • The methodology is intended to be used primarily in assessments performed by authorities of the existing resolution regimes in their jurisdictions, in peer reviews and in IMF and World Bank assessments, including through Financial Sector Assessment Programs.