July 20, 2020

By electronic submission to fsb@fsb.org

Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Re: FSB Consultative Document "Effective Practices for Cyber Incident Response and Recovery"

Dear Sir/Madam:

The Institute of International Finance (IIF) and its members welcome the opportunity to respond to the Financial Stability Board (FSB) Consultative Document "Effective Practices for Cyber Incident Response and Recovery".[1] We also appreciate the active engagement of the FSB in the ongoing discussions among regulators, market participants and industry groups on addressing financial sector cyber resilience, including the four regional stakeholder workshops organized by the FSB in the last few weeks to discuss this consultation in more detail.

The proposed FSB toolkit of effective practices for cyber incident response and recovery (CIRR) is welcome and important given the constant need to address the frequency and scope of cyber incidents and the increased sophistication of cyber-attacks. It is also timely given the increased focus of both authorities and the financial industry on building up resilience. While the financial industry has long been the sector most exposed to cyber-attacks, it is also often credited for having the most proactive policy, regulation and investment in risk management and governance practices with respect to IT.[2]

In responding to this Consultation, the IIF would like to elaborate on the following themes:

- The FSB CIRR toolkit complements the two previous FSB initiatives, which have helped to highlight and address market fragmentation across jurisdictions
- The FSB can help encourage jurisdictions to find common agreement on the definition of an "incident" and thresholds around "significance" and "materiality"
- The established practices can help strengthen the overall resilience of the financial system, especially for less mature firms on a proportional basis
- It is important that the practices are considered to be *voluntary* and *principles-based*, and that the wider financial ecosystem are also encouraged to consider using them
- The proposed practices could be more closely aligned with leading global practices and would thereby further help address regulatory and supervisory fragmentation
- There should be a coordinated approach to how regulators communicate with firms during a material incident

[1] See the FSB consultative document at: www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document/
[2] BIS 2020. "BIS Working Papers No 865: The drivers of cyber risk" May 2020.

The FSB CIRR toolkit complements the two previous FSB initiatives, which have helped to highlight and address market fragmentation across jurisdictions

This latest FSB initiative complements the two previous FSB initiatives focused on cyber risk, including taking stock of regulations, guidance and supervisory practices (2017), and producing a Cyber Lexicon (2018) of common terms and definitions. Both of those initiatives helped streamline public sector initiatives and private sector approaches to cyber resilience. The FSB "stocktake" on cyber security regulations, guidance and supervisory practices, published in October 2017, found a divergence of practices being introduced around the world.[3] Notably, the report concluded that the FSB's 25-member jurisdictions had 85 different schemes of regulation and guidance, and 35 different supervisory practices. The report also indicated that 72% of its member jurisdictions would plan to revise or introduce new cybersecurity frameworks in the following year. The FSB summary report underscored that there is a significant amount of diversity in approaches between the increasing amount of regulation being developed that is aimed at strengthening cyber resilience across the financial services industry.

Regulatory and supervisory fragmentation is a considerable concern to the financial services industry, especially for firms that operate in multiple jurisdictions. Complying with myriad regulations and guidelines is complex, costly and diverts resources away from other effective cybersecurity related activities. Importantly, rather than enhancing overall cyber-resilience, uncoordinated, duplicative and contradictory regulation can pose a risk to financial stability, especially when testing critical systems multiple times or creating unnecessary duplication of sensitive information. That is why the publication of the FSB cyber lexicon in November 2018 was also significant, because it provides common terms and definitions for industry and policymakers to use as they consider respective approaches to cyber risk management.[4]

The Lexicon was also a necessary first step towards reducing regulatory fragmentation by creating a common vernacular and thereby reducing the number of interpretations of terms. The cross-sectoral application of the Lexicon – from banks to insurers to financial market infrastructure – recognizes the similar impact of cyber events across the financial sector and sets forth a common framework that should help support the reduction of the number of similar, but not identical, industry cyber requirements. But given the speed of developments around cyber resilience, not all the relevant words in this toolkit would have previously been defined in the earlier Cyber Lexicon, which is now almost two years old. Therefore, the FSB could consider identifying a Lexicon owner responsible for its management and ensuring timely and consistent updates. This would also support the final CIRR toolkit, which would benefit from a glossary of terms, even if the Lexicon is not updated, to ensure that the effective practices are considered and undertaken in a consistent manner across jurisdictions.

The work undertaken by the FSB, such as the creation of the Cyber Lexicon, acknowledges the importance of language and its ability to affect positive change. Language helps link a wide swath of our shared cultures and values, and must evolve alongside these constructs – whether passively or actively.

Amidst increasing social awareness of inequality and racism pervasively present worldwide, positive change is needed to ensure we shape a better and fairer future than the present. Just as regulators and standard-setters consider potential impacts that new technologies may have on

[3] FSB 2017. "Summary Report on Financial Sector Cyber Security Regulations, Guidance and Supervisory Practices" October 2017.
[4] FSB 2018. "Cyber Lexicon" November 2018.

bias, discrimination and financial exclusion, so too should we explore how language within our industry shared cyber standards may implicitly support racially-insensitive stereotypes.

We welcome the FSB and its peers to join market participants in this effort, and to encourage the altering of any standards' language which may carry such negative connotations wherever identified. This includes terms such as "whitelisting" and "blacklisting", or "master" and "slave" servers, among others. Although the FSB itself has not employed any of these terms in neither this consultation nor the Lexicon, we would be grateful if you joined us in encouraging regulators and market participants to strive for more equitable language going forward.

The FSB can help encourage jurisdictions to find common agreement on the definition of an "incident" and thresholds around "significance" and "materiality"

More urgent is the active debate taking place across jurisdictions by policy-makers and industry about what constitutes an "incident", and to what extent such an event is "significant" or "material." Clear definitions and thresholds would greatly benefit both authorities and industry to prioritize what should be reported. In practice #46 "Cyber incident reporting", for example, the term "significant" is used but it is not very specific, hard to define, and should be refined given the meaning of "significant" will mean different things to different people.

Therefore, we strongly support the FSB's focus in the CIRR on "significant" cyber incidents for regulatory reporting purposes and encourage the FSB going forward to focus its efforts specifically in the area of incident reporting, including helping define what is an incident, and how relevant incidents can be reported consistently by firms across jurisdictions. Materiality thresholds should be risk-based and based on circumstances (e.g. disruption or threat to confidentiality, integrity or availability of information assets, potential client or market impacts), rather than set on fixed, specific criteria (e.g. nature, extent and magnitude), so that it can be applied to firms of various types and sizes, based on the firms' risk framework, in order to capture only significant security incidents.

By working together with its membership and other global standard-setters, the FSB can encourage agreement on key definitions and how to establish a scalable "materiality" threshold which best captures relevant incidents in the financial system. It will be increasingly important that relevant authorities have accurate and comparable data on significant cyber incidents, also given the growing range of market participants involved in the provision of financial services and products. Incident Reporting is also an area that the IIF will be focusing on this year and we would like to support the FSB in this area later this year with key recommendations and to help coordinate industry viewpoints and expertise.

The established practices can help strengthen the overall resilience of the financial system, especially for less mature firms on a proportional basis

The proposed FSB toolkit of 46 effective practices for CIRR provides additional opportunities to further align industry practices and to provide market participants with common, consistent and effective practices to consider as they continue to strengthen their own approaches to addressing cyber risk. While many of the tools are already common practice among larger firms, they could be very valuable to less mature firms that may not yet be taking full advantage of the range of outlined practices and could find many of the suggested tools useful to consider. This would further help raise minimum standards as there are varying levels of maturity across

the financial sector and the size, complexity and market interconnectedness of any one firm will help dictate to what extent these practices are already in place, important to consider or possibly not appropriate for a respective firm's business model and risks.

For some of the effective practices, the sophistication of the processes might be too complex or costly for all but the largest firms. For example, undertaking red/blue teaming exercises can be very beneficial to support cyber security maturity but organizing and executing these simulations are extremely complicated and technical. In such cases it would be beneficial to apply a principle of proportionality, across organizations of various size, complexity, business model, risk profile and jurisdiction, to avoid some authorities possibly recommending all tools to all parts of their respective financial sector. For less mature firms with limited resources, it would be more important to update outdated infrastructure with systems that are better suited to help withstand cyber incidents.[5]

It is important that the practices are considered to be *voluntary* and *principles-based*, and that the wider financial ecosystem are also encouraged to consider using them

Many of the practices in the toolkit are worth considering not only for industry but also for standard-setting bodies and authorities as effective options, when formulating guidance around cyber security. Such action would promote common practices, rather than prescriptive regulation, and aid in further avoiding the fragmented approaches across jurisdictions that were noted in the Stock-take.

If these practices are recommended by authorities, it is critical that this toolkit be presented as a *voluntary* assortment of tools already commonly in use throughout the financial services industry, especially by the larger firms. Rather than jurisdictions seeing these as mandatory practices, they can be seen as common and effective tools that provide organizations with a variety of options to consider when creating or further developing their respective approaches to cyber resilience.

Developments around cyber security, including the nature of the incidents, technological advancements and effective industry practices, change rapidly. Therefore, the IIF strongly agrees with the FSB approach of providing a "toolkit of options" rather than an applied "one-size-fits-all-manner" that tries to capture the whole industry through more prescriptive measures. Yet, in a number of cases, the effective practices are quite prescriptive, including when it comes to encouraging firms to maintain Security Operations Centers (#13) or Disaster Recovery Sites (#14), as well as elements in the 'Governance' section. The IIF would encourage any jurisdiction that considers recommending these practices to opt for a *principles*-based perspective that gives firms the necessary room to tailor the practices to their own institutions, if appropriate. Providing such flexibility will allow firms to address the dynamic technological changes or changes in the threat landscape in accordance with the size, complexity and market interconnectedness of any one firm.

The financial industry ecosystem is diverse and interconnected, with close and constant connectivity between banks, insurers, asset managers, financial market infrastructure, and also increasingly the newer fintech firms, challengers and cloud computing companies, as well as third-party vendors and supply chains. It is imperative that standard-setters and authorities

[5] See for example the joint IIF-McKinsey Cyber Resilience Survey (March 2020) for recommendations and industry practices that companies can draw on to enhance their cybersecurity posture https://www.iif.com/Publications/ID/3817/Joint-IIF-McKinsey-Cyber-Resilience-Survey

encourage all parts of the financial system to consider adopting effective industry practices, by focusing on which activities are undertaken and at what risk, rather than exclusively focusing on those traditional financial institutions that are already most closely regulated.

The proposed practices could be more closely aligned with leading global practices and would thereby further help address regulatory and supervisory fragmentation

We commend the FSB in its efforts to align the toolkit with internationally recognized industry standards, including the Guidance on cyber resilience for financial market infrastructures published by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) (CPMI-IOSCO Guidance), the US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework), and the International Organization for Standardization 27000 series (ISO 27000 Series), which provides information security control standards.

Coordination and consistency between jurisdictions, as noted in effective practice #43, is very important. But it could have a more prominent role across the entire toolkit. That would include the need for consistent policy and regulation at the global level and between jurisdictions. This could be done in part by complementing the structure of the toolkit more closely with NIST and ISO, which are used widely by industry around the world. Most recently, both ISO and NIST have engaged international partners in the open, transparent, and collaborative standards development process to develop a technical specification, ISO/IEC 27101, on guidance for developing cybersecurity frameworks that leverages the content and approach of NIST Version 1.1 of the Cybersecurity Framework. NIST maps its higher-level framework to ISO 27000, which enable firms to converge the technical control focus of NIST with the more risk-driven dimension of ISO.

The global financial sector, in partnership with trade associations including the IIF, have further developed a convergence instrument called the "Financial Sector Profile" (FS Profile) that brings together these different lenses of understanding to the cybersecurity posture of a firm.[6] It brings together not just the leading international standards, but also a catalogue of regulatory and legal framework requirements. The Profile uses a common vocabulary and taxonomy by which the financial services sector regulators and industry can communicate with each other to establish a common understanding of any financial institution's cybersecurity posture.

To align the toolkit closer to existing globally-accepted frameworks – including NIST, ISO and the FS Profile – the FSB should consider adjusting the seven components ("Governance," "Preparation," "Analysis," "Mitigation," "Restoration," "Improvement," and "Coordination and Communication") to the more common taxonomy. This would entail (i) relabeling "Preparation" to "Planning" and (ii) incorporating the practices listed under "Restoration" into the "Mitigation," "Planning," and "Communications" components, to better align with well-established international cybersecurity frameworks.

Consider, for example, the following FSB CIRR effective practice:

- *"Restoration (26.) Prioritisation. Organisations prioritise restoration activities based on business, security and technical requirements. All internal and external stakeholders*

[6] FS Profile 2018. "Industry Unveils Cybersecurity Profile to Help Financial Institutions Develop and Maintain Cyber Risk Management Programs." https://www.iif.com/Press/View/ID/1243/Industry-Unveils-Cybersecurity-Profile-to-Help-Financial-Institutions-Develop-and-Maintain-Cyber-Risk-Management-Programs

are updated regularly and made aware of the conditions to be met, or restrictions, before resuming critical operations."

This is covered in the FS Profile as: *Recovery. Planning – 1.2 – Organization's recovery plans are executed by first resuming critical services and core business functions, and without causing any potential concurrent and widespread interruptions to interconnected entities and critical infrastructure, such as energy and telecommunications.*

It is also covered in the FS Profile as: Recovery. Communications – 1.1-3.1

- *The organization's governing body (e.g., the Board or one of its committees) ensures that a communication plan exists to notify internal and external stakeholders about an incident, as appropriate"*
- *The organization promptly communicates the status of recovery activities to regulatory authorities and relevant external stakeholders, as appropriate*
- *Actionable and effective mitigation techniques are taken and communicated appropriately to restore and improve the organization's reputation after an incident*
- *The organization timely involves and communicates the recovery activities, procedures, cyber risk management issues to the appropriate governing body (e.g., the Board or one of its committees, senior management and relevant internal stakeholders)*

This is also covered under CPMI-IOSCO – Response and Recovery, 6.2.3 and 6.2.4 under Contingency Planning and Planning and Preparation.

Therefore, we encourage FSB to reconsider the overall structure of the toolkit and to align the subject headings more closely with general industry practice of covering restoration activities under either under Planning, Mitigation, or Communications. While these may seem like seemingly small adjustments, it is these slightly-different-but-similar approaches that cause pervasive regulatory fragmentation and additional burdens on firms that must adhere to requirements in multiple jurisdictions.

There should be a coordinated approach to how regulators communicate with firms during a material incident

Effective practice #11 (Communication strategies, channels and plans) highlights that there should be a coordinated approach to how regulators communicate with firms during a material incident. During such incidents, firms sometimes experience repeated uncoordinated requests for information from authorities, sometimes from different departments within the same authority. There are also differences in time frames and what information is requested.

Answering duplicative requests diverts resources from managing the incident and could lead to inaccurate policy responses should the information conveyed not be consistent. Clear incident response communications between firms and authorities should be established with clear plans from the authorities as to what information they will request when and to whom in order to ensure consistency and accuracy of the information and in order to not divert resources from incident management.

Additional feedback on specific effective practices

In terms of the specific tools featured in the toolkit, we would like to offer additional feedback for consideration:

#2 – Role and responsibilities of the board. There are different approaches across firms to the role of the Board vs the senior management at the Group level. Whether at a Group or Business Unit level, the Board is accountable, at a minimum, to (1) ensuring that the organization has a comprehensive plan that addresses material cyber and operational risks and can recover business operations in a "rapid but safe" manner (2) understanding that individuals are empowered and have the appropriate level of expertise for conducting CIRR responsibilities and (3) providing credible challenge to the financial institution's CIRR strategy. Anything outside of these three elements may differ between financial institutions.

As such, the wording in this practice is too prescriptive of the specific role of the Board and the decisions around roles and responsibilities should be taken at the firm-level, rather than across the financial sector as a whole. The primary role of a board is to set the firm's overall strategy and to provide challenge to senior managers. The Board should not necessarily be involved in setting or implementing the firm's cyber strategy, but they do have a role in challenging the designed implementation.

In addition, firms might have additional considerations in place for the role of boards at business unit level, especially when an incident is material within that unit, but not at an enterprise-wide level. We recommend therefore the FSB update its text to highlight this dynamic so that the allocation of certain roles and responsibilities better allow for proportionality and scaling across a range of institutions. This is especially relevant for the wording in the final sentence: "Board and senior management also have the responsibility of implementing the required improvements." This risks inadvertently supporting an inappropriate expansion of the management board's obligations, to include specific responsibility for day-to-day activities regarding the design and implementation of the CIRR framework. Finally, there also needs to be clearer delineation between Board and Senior Management activities. The last sentence in this practice, describes Senior Management responsibilities and not the Board's responsibilities.

#3 – Roles, responsibilities and accountabilities for CIRR. This section is perhaps too specific in guidance given that firms will organize their governance in this area in different ways. Rather, organizations should be encouraged to create clearly define roles responsibilities and accountabilities for all organizational areas that may be involved in the recovery and response capabilities of a material cyber event.

For example, the description of there being one "Incident Owner" per attack in an organization seems unrealistic. Within financial institutions there would be different individuals and teams responsible for different aspects of incidents. While the practice of one person managing/coordinating actions and communications for an incident could be prudent, identifying this role as an 'Incident Owner' may blur the line of what their responsibilities or powers include, by applying a more prescriptive description of the role. For example, it might imply that the Incident Owner is also the decision-maker across the incident's lifecycle. Depending on the severity of the incident, additional but linked processes with distinct design-makers may be triggered. Crisis management for one could broaden the scope of the response process where it no longer comes down to one individual. This includes making decisions, for example, on specific business impacts.

Furthermore, this effective practice appears to combine the approach of an incident that may have low operational impact (e.g., server outage) and a material operational outage. Minor incidents may have an assigned Incident Manager to manage the incident to closure. Material operational outages may involve several organizational roles including, but not limited to: Impacted Business Units, General Counsel, Communications/Public Relations, Risk, and IT. The combination of these approaches may cause ambiguity for financial institutions that do not have access to the expertise in CIRR. Given that there are multiple organizational roles that may be involved in a cyber incident and those involved roles may differ depending on the incident, this practice may be too prescriptive when used to define the role of each group but would be more effective as a principle. For example, organizations should clearly define role responsibilities and accountabilities for all organizational areas that may be involved in the recovery and response capabilities of a material cyber event. For all these reasons, we recommend that effective practice be formulated in a more principles-based manner.

#12 – Scenario planning and stress testing. While application penetration testing and vulnerability scanning can be useful, there are growing concerns about the proliferation of tests and the testing of live systems, which can increase or even create risk, rather than reduce risk. It will become increasingly important to determine how and when firms test, especially if they operate in multiple jurisdictions, and in those cases, cooperation will be increasingly important to avoid requiring firms to use different testing and reporting protocols to meet the same ends. Moreover, standardized protocols may not be fit for purpose across organizations with different systems and risk profiles.

The final sentence for this practice also unnecessarily narrows these potential exercises by implying that "key external stakeholders" are always included; while this is a common practice, it is not always the case or potentially advisable for certain exercises. Scenario planning, on the other hand, is defined by best practice (e.g., IOSCO, CPMI) and is normally carried out through tabletop exercises or financial models and not on live systems.

We recommend the FSB revises its wording to highlight a broader range of exercises related to scenario planning and stress testing and removes the implicit qualifier that they are always done with external stakeholders.

#17 – Supply chain management. The role of the supply chain is increasing in importance, as also has been highlighted throughout the COVID-19 crisis. Firms are testing their dependencies on supply chains and testing contingency measures. Third-party risk management is an important element for each cybersecurity primary function (identify, protect, detect, respond, recover) and becomes more essential as firms progress across their digitalization journeys. This practice, however, primarily addresses measures regarding onboarding. In addition, FSB practices #23 (business continuity measures) and #28 (monitoring) briefly touch on third-party related considerations. Overall, we recommend the FSB broadens its coverage of third-party aspects to highlight additional considerations and effective practices that address indirect threats from managed service providers and mitigating risk when an incident is live.

#23 – Business continuity measures. The current wording implies that every cyber incident triggers business continuity plans (BCP). The activation of BCP however will depend on the severity of the incident, among other factors. We recommend the FSB updates this practice to highlight that BCP may be triggered by the Incident Manager or other responsible party, depending on the incident's severity and expected impact.

#26 – Prioritisation. Organizations prioritize restoration based on the criticality of that business and its services to the financial institution and to the financial services sector, this criticality drives the security and technical requirements and other restoration requirements.

#27 – Key Milestones. The redesign, reinstall, and reconfiguration of systems would not be key milestones in a CIRR plan. Financial Institutions would identify/define key times when important market activities need to occur and these times would drive the decision-making for restoration activities (e.g., system reconfiguration/rebuild). For the last sentence in this practice, the focus should not be on systems. The statement of, 'Organizations should also consider developing interim restoration goals/measures, such as continuing operations in a diminished capacity.' should provide guidance to both practitioners and supervisors in this space.

#28 – Monitoring. It is important that firms monitor third-party service providers, the network and systems to the extent possible. Firms are responsible for their relationship with third party providers and have contingency plans that may be enacted in the event that the service provider cannot provide the service or can provide the service at a diminished capacity. Firms may not be responsible for third party restoration activities, in so much, to return the service to full capacity.

When regulators are concerned about the repercussions of a serious breach, as happened recently at one of the few large cloud providers, they sometimes ask firms for internal risk assessment including third-party service providers to improve their cyber monitoring and mitigation capabilities. When doing so, it would be important to provide specific guidance on how to monitor the critical third-party service providers in light of a possible service replacement.

#34 – Exercises, tests and drills. As mentioned above, the use of red/blue teams can be quite prohibitive in terms of time and costs for less mature organizations. Also, some larger firms are already incorporating additional capabilities, such as continuous monitoring, also known as continuous security validation. Due to significant differences across and within financial sector in terms of cyber maturity and given that only a few authorities are currently organizing such testing, the threat-led penetration testing should be run on a voluntary basis. Furthermore, it would be useful if authorities could produce a guide of very high-level clear objectives rather than prescriptive tools.

Rather than relying on testing, which provides a point-in-time assessment of a specific vulnerability, firms should have the flexibility to adopt from a wide suite of monitoring and testing capabilities suited for their business model and risk profile. One of these capabilities, for example, continuous monitoring, using adversarial threat model (e.g. the MITRE ATT&CK Framework), is designed to address the limitations of a point-in-time security testing. Continuous monitoring helps to identify threats tools and techniques against which to test and facilitates firms' continuous simulation, testing and validation of the security functions in an enterprise. Continuous monitoring also has the benefit of being able to test more broadly and frequently than the time-intensive techniques like pen-testing and red-teaming.

Because continuous monitoring includes automated testing, adversarial emulation and stress testing of applicable controls, it can help address the limitations of point-in-time tests and provide the comprehensive view regulators seek of a firm's overall security posture.

#43 – Cross-border cooperation. Coordination and consistency between jurisdictions are critical, as discussed in the introductory sections of this response letter, and as such could have

more prominence across the entire toolkit. That would include the need for consistent policy and regulation at the global level, between jurisdictions and within jurisdictions. There could also be more references to prominent platforms and approaches, such as FS-ISAC, the Financial Sector Profile and the, ISO 27000 Series, NIST Framework, among others.

In addition to the comments above, please find below our comments to several the Consultation's specific questions. In some cases, the questions were more supervisory in nature and a response from one individual firm would be more relevant.

We thank the FSB Secretariat for its consideration of our comments. If you have any questions, please do not hesitate to contact Martin Boer at mboer@iif.com or Katharina Sobczak at ksobczak@iif.com.

Sincerely,

Martin Boer
Director, Regulatory Affairs
Institute of International Finance (IIF)

RESPONSES TO SELECTED CONSULTATION QUESTIONS

The FSB invites comments on the consultative document and provides the following specific questions as a guide. Please provide details and supporting information where possible.

General

Question 1.1: *Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices?*

- Since the beginning of the COVID-19 pandemic there has been no increase in material impact on firms due to cyber events.
- While there has been anecdotal evidence of a strong increase in cyber-attacks, they have namely been concentrated on lower-level phishing and spoofing attacks.
- The human element within organizations has become increasingly important given remote working, and firms are supporting colleagues, their families and communities who are impacted by the health and economic aspects of the crisis.
- In some cases, financial firms have restricted employee access to smaller parts of the company network to reduce potential incidents. However, cyber incident reporting may need to be adjusted with a 'work from home' scenario.
- Given the role of third parties and suppliers during the crisis, it could be expected that additional regulatory focus will be placed on these relationships and dependencies.
- In some cases, revision of cyber security scenarios applied in playbooks may be adjusted with COVID sensitive analysis.

Question 1.2: *To whom do you think this document should be addressed within your organization?*

- Would vary within organizations and jurisdictions.
- Often the CISO and/or Board member that they report to (CRO) at the Group level.
- In other cases: Chief Information Officers (CIO), Chief Security Officer (CSO), Heads of Cyber Security or IT transformation team.

Question 1.3: *How does your organisation link cyber incident response and recovery with the organisation's business? Does your organisation follow international standards or common frameworks? If so, which international standards or common frameworks?*

- Many firms use the "Financial Sector Profile", which synthesizes globally accepted cybersecurity principles, including those in the NIST Framework, Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT), ISO 27000 Series, G-7 Principles, and CPMI-IOSCO guidance, Treat Intelligence-Based Ethical Red Teaming (TIBER-EU), Cyber

Resilience Assessment Framework (C-RAF), ECB CROE, EBA ICT Guidelines ISF Standards of good practice, COBIT 5 and other ISACA publications, DAMA guide to data management body of knowledge.

- The Profile uses a common vocabulary and taxonomy by which the financial services sector regulators and industry can communicate with each other to establish a common understanding of any financial institution's cybersecurity posture.

Question 1.4: *Does your organisation structure its cyber incident response and recovery activities along the seven components set out in the FSB toolkit? Please describe any additional components your organisation considers.*

- As mentioned in the cover letter, the toolkit could be more closely aligned to existing globally-accepted frameworks – including NIST, ISO and the FS Profile.
- Therefore, the FSB could consider adjusting the seven components ("Governance," "Preparation," "Analysis," "Mitigation," "Restoration," "Improvement," and "Coordination and Communication") to the more common taxonomy. This would entail (i) relabeling "Preparation" to "Planning" and (ii) incorporating the practices listed under "Restoration" into the "Mitigation," "Planning," and "Communications" components, to better align with well-established international cybersecurity frameworks.

Question 1.6: *Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).*

- Encourage the sharing of information, such as through information sharing platforms like FS-ISAC, which should continue to be done on a voluntary basis.
- Encourage and facilitate the greater use of public-private platforms.
- As discussed above, the FSB could consider identifying a Lexicon owner that could manage and ensure timely and consistent updates of the Lexicon. This would also support the final CIRR toolkit, which would benefit from a glossary of terms, even if the Lexicon is not updated, to ensure that the effective practices are considered and undertaken in a consistent manner across jurisdictions.

Question 1.7: *What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?*

- Authorities can play an important role in harmonizing and coordinating requests for information, possibly including a global, standardized reporting platform.
- As discussed above, the FSB can help encourage jurisdictions to find common agreement on the definition of an "incident" and thresholds around "significance" and "materiality."
- Working closely with firms through public-private platforms.

- Ensure that any regulatory, supervisory and policy measures continue to support innovation in the financial service sector.

Governance

Question 1.1: *To what extent does your organisation designate roles and responsibilities as described in Tool 3? Does your organisation identify these roles by business line, technology application or department?*

- In some cases, a partnership between the cybersecurity team and firm's line of business, including the presence of embedded cybersecurity personnel at the line of business level.
- Including the existence of a 24/7 global cyber emergency response team.

Question 1.2: *How does your organisation promote a non-punitive culture to avoid "too little too late" failures and accelerate information sharing and CIRR activities?*

- Cultures are addressed differently across firms but would include encouragement of sharing information quickly and proactively around cyber incidents.
- The technology would include end-point protection, prevention of unauthorized installations, system and data backups, physical security, contingency planning for cybersecurity scenarios and third-party service providers.

Preparation

Question 2.1: *What tools and processes does your organisation have to deploy during the first days of a cyber incident?*

- Effective practices as detailed in the CIRR toolkit.
- Cyber Incident Response Plans.
- Playbooks.
- Digital forensic tooling and runbooks.
- Contingency planning for cybersecurity scenarios and third-party service providers.

Question 2.2: *Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.*

- Creation of COVID-19 'lessons learned' documents with actions for improvement.

Question 2.3: *How does your organisation monitor, manage and mitigate risks stemming from third party service providers (supply chain)?*

- Contractual aspects such as access and audit rights, transition, sub-outsourcing, resilience, registers, incident notification, and exit strategies.
- Evaluation of vendors' security and privacy practices and tracking vendor audit findings to different degrees.

Analysis

Question 3.2: *What are the inputs that would be required to facilitate the analysis of a cyber incident?*

- Observables, business context, IT assets concerned, available threat intelligence, data classification, impact, third-party forensics, stakeholders.

Question 3.3: *What additional tools could be useful to analyse the effectiveness of cyber incident response and recovery activities and the severity, impact and root cause of cyber incidents?*

- A regular management review process, internal and external audits.

Question 3.4: *What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?*

- Firms participate in many sector associations, which help identify and remedy cyber incidents, strengthen the overall financial system, and help formulate a global view.
- FS-ISAC
- CERTs
- ISF
- Interbank committees
- NCSC FSIE
- ENISA Cyber working group
- FSCCC
- FSARC
- CISA

Mitigation

Question 4.1: *Besides reducing impact to business and system security, what are other considerations that need to be taken into account during mitigation?*

- Immediate Regulatory Reporting, internal and external communication procedures.
- That security metrics are in place and incidents are reported to senior management, and the most serious incidents are reported to the board.

Question 4.2: *What tools or effective practices does your organisation have related to mitigating the impact from: (i) data breaches (ii) loss of data integrity and (iii) ransomware events?*

- Security Monitoring.
- Segregation of access privileges, provisioning and de-provisioning of identities, securing and authentication of identities, authorization to access resources, prevent malicious use of stolen credentials.
- State-of-the-art data mining tools and artificial intelligence to detect fraud and other anomalies in security breaches.

Question 4.4: *What additional tools could be useful for including in the component Mitigation?*

- IT Service Management tools.

Restoration

Question 5.1: *What tools and processes does your organisation have available for restoration?*

- Disaster Recovery Plan at the group and local level tested and discussed periodically with relevant leadership.

Question 5.2: *Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?*

- Crisis Management Organization and Plans.
- Business Continuity Plans.

Question 5.3: *How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?*

- Testing of cybersecurity scenarios from the Disaster Recovery plans.

Improvement

Question 6.1: *What are the most effective types of exercises, drills and tests? Why are they considered effective?*

- Penetration testing.
- Red/Blue testing.
- Continuum testing.
- Crisis testing with senior leadership: Such exercises allow non-technical leaders to understand the real impact of a security incident and the importance of all the plans and functions.

Question 6.2: *What are the major impediments to establishing cross-sectoral and cross-border exercises?*

- Realistic scenarios.
- Data privacy regulations and restrictions.
- Security concerns.
- Legal uncertainties.
- Shortage of skilled staff.

Question 6.3: *Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery?*

- Tool for crisis management coordination and visualization of crisis management situational awareness.

Coordination and communication

Question 7.2: *How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident?*

- Alternative telephone lines.
- Apps (e.g. WhatsApp, Signal).

Question 7.3: *Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?*

- Sector wide attack information.
- Patches for cyber-attacks.
- Emerging vulnerabilities.