20th July, 2020

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

By email: CIRR@fsb.org

Dear Sir/Madame,

Re: The Financial Stability Board (FSB) Effective Practices for Cyber Incident Response and Recovery: Consultative document

Citi welcomes the opportunity to respond to the Financial Stability Board (FSB) Effective Practices for Cyber Incident Response and Recovery: Consultative document.

We believe that cyber incident response and recovery is a vital agenda that is necessary to protect the financial sectors' and public interest. It also serves to decrease commercial risks and threats to our clients', local markets' and firms' growth posed by emerging, complex and inter-connected business models, which create and expose new and evolving vulnerabilities.

With an outcome-focused approach, the FSB is well-placed to drive a compelling client-centric vision by bringing together the management of various programmes in addition to cyber security, such as new product development, data protection, change management, incident response, third parties, business continuity, IT risk and scenario analysis.

Whilst we have contributed to the cyber related work of various trade associations, including UK Finance, The Institute of International Finance (IIF), the Global Financial Markets Association (GFMA) and the Bank Policy Institute (BPI), in this letter we wanted to underscore to you directly the importance of the following issues:

- Globally coherent and consistent cyber regulation underpinned by cross-border regulatory and supervisory co-operation;
- Ensuring a client-centric and business-driven cyber-security approach is taken to business services, harm and impact tolerances; and
- Strengthening and evolving public and private sector coordination and collaboration.

Proper and complete cyber security requires hard work, lateral thinking and creativity within firms, between the industry, and across the public sector. It is not a business function, but a business ethos. As such, Citi strongly encourages continued and deeper public and private sector collaboration, on an ongoing basis.

We would be delighted to meet to discuss these opportunities at a mutually convenient time. In the meantime, please do not hesitate to contact us if Citi can help in any way.

Citi's Response to the Financial Stability Board (FSB) Effective Practices for Cyber Incident Response and Recovery Consultative document

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?

Early in the COVID-19 outbreak, Citi focused on increasing in real time the amount of network bandwidth needed to continue to operate globally with all staff working remotely. Security processes became managed virtually. This included conducting security interviews and documenting digital evidence collection and analysis (e.g. malware) that was typically done on physical machines isolated from the network and thus not accessible to remote employees. Communication from remote locations across multiple teams and functions became a priority. The deployment of Symphony, a secure chat platform that allows for communication and collaboration amongst teams and employees in workspaces, channels or workflows, enabled coordination across regions and time zones. Additionally due to concerns with increased cyber threats with the large number of staff working remotely, a Social Engineering training was developed and launched to staff globally to raise awareness about the social engineering threats and techniques used to gain access to Citi systems and information.

2. To whom do you think this document should be addressed within your organisation?

This document should be addressed to Citi's Chief Information Security Officer (CISO), CISO senior staff, and senior business staff.

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?

Citi business leaders are the key players in our periodic cyber exercises, as there is an overall understanding across our firm that senior business executives need to drive the key decisions made by the organization in order to contain, respond to and recover from a cyber event, in line with what is described in section 1.1 later in this document.

Citi's Cyber Response framework follows the NIST Framework as applicable; incident response activities work in consultation with impacted lines of business, including through any disruptive activities. The shift in focus to cyber resilience, from a reactive posture, has improved this interaction across all phases (pre, post, and during) of incidents. It has also highlighted the need for business obligations to be a significant contributing factor in response, mitigation, and remediation strategies.

Attached separately is a *Cyber Scenario Checklist* to help leaders in FIs evaluate the situation and aid in identifying what parts of their organization need to be engaged and what aspects of the markets including liquidity need to be considering during decision making.

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.**

Yes, Citi addresses cyber incident response and recovery activities along the seven components set out in the FSB toolkit. Additionally, Citi leverages intelligence-led incident response and management to proactively guard against potential events before they manifest. (We expand on intelligence-led culture in section 1.2.) Appropriate authorities should have consistent and transparent processes, including information requests as well as a cadence for sharing relevant information or indicators of compromise.

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

• Information Sharing: Ensuring that accurate and effective information sharing between internal stakeholders is necessary, this can include a summary of the cyber event; mitigation actions taken to contain it; impact of the incident to business; near term pending recovery actions and ways to prevent reoccurrence. A challenge with this method, however, is that it can hinder teams within organizations, especially those of a large size, to access information that is necessary and useful for them to know. It is important to find a way to balance internal protocol without creating an unnecessary hurdle for teams.

• Integration/Standardization: Understanding that the definition of "critical" can vary for different lines of business. Importance should be placed on all response teams working on actionable intelligence and creating metrics that are meaningful and measurable during mitigation.

• Training: Organizations must ensure that the institution has all employees regularly involved and educated about security via a mature and evolving information security awareness program. By doing this, staff is encouraged to follow best practices and guidelines during time of mitigation.

• Recording: Record current playbook calls as events unfold both to inform decisions taken during an incident and to reconstruct what happened afterwards. It is also necessary to maintain regulatory compliance.

• Investigation: Quickly determining what data was impacted allows Citi to 1) mitigate Client harm through notification and fraud prevention efforts, 2) mitigate impact to Citi through remediation and containment actions (e.g. password resets, configuration modification, etc.), and 3) mitigate industry impact through prompt regulatory and sharing group notification when indicated. The focus would be on tools and practices that facilitate these three activities.

1. Governance

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?

To ensure effective response and recovery activities, including forensic analysis, and to determine the severity, impact and root cause of the cyber incident we use and suggest a central coordination entity based on the information security organization, such as a cyber security fusion center. This central entity tracks ongoing activities, reporting, and investigations associated with a cyber incident/crisis, and operates across geographies and business sectors for the definition and implementation of containment actions for an already identified and alerted incident. It should combine investigation services, technology organizations, information security officers, Risk & Control functions, Production support, Business Heads, the Regional CEO/CAO and Operations & Technology Head and Legal. This entity would provide the businesses the first response and technical analysis for all cyber incidents, including defensive tools and containment actions.

To note, the onset of a major cyber incident may prompt temporary changes in the leadership structure, such as the appointment of an incident leader who has both the necessary business understanding and awareness of containment, mitigation, and recovery strategies. This leader would coordinate closely with counterparts on the tactical level to guide decision-making and responses.

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?

Citi emphasizes an intelligence-led culture that focuses on a proactive approach to threats rather than solely reactive. Proactively leveraging processes, tools and controls plus periodically sharing relevant cyber intelligence with peer FIs enables fast, accurate, and relevant information sharing. The importance of information sharing among and between public and private sectors as well as within FI cannot be understated. Using both formal and informal channels, the ability to recognize threats and alert other organizations, and to receive information from others is one of the most important aspects to successfully managing cyber security.

An example of an intelligence-led culture, the cyber security team works directly with business lines to advise on cyber fraud and payment thresholds based on a risk assessment that leverages cyber intelligence developed internally as well as learnt from information sharing partnerships. Additionally the cyber security team feeds intelligence and information to a security operations center so that the former can make informed decisions, sometimes resulting in severing risky business-to-business connections or restricting email traffic/attachments with organizations identified to have been compromised.

Additionally, Citi fosters a "continual improvement" culture. Vulnerabilities and weaknesses are actively searched for and raised, with all employees feeling responsible for resilience, and able to challenge and raise issues in other lines of business. This puts the emphasis, while maintaining accountability, on looking forward and getting better as opposed to after-the-fact finger pointing.

2. Preparation

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

During the first days of a cyber incident, monitoring tools are persistent and continue to monitor prior to, during, and post incidents. Analysts on multiple teams leverage shared frameworks and tools to further focus response efforts. These include, but are not limited to, the MITRE ATT&CK Framework, Diamond analysis, attack diagrams, and multiple artifact collection trackers. The MITRE ATT&CK Framework is a matrix of tactics and techniques that can be leveraged to assess threats and risk. It is a helpful tool to identify and map gaps in systems and products using known threats, not hypotheticals. Vulnerability assessment teams including red teams that focus on penetration testing of systems, networks and programs, often use the ATT&CK Framework as do cyber exercise teams that develop tabletop

exercises. Diamond analysis is a model to better conduct intelligence analysis on security incidents by viewing relationships and attributes across four elements: adversary, infrastructure, capability and victim

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

In the last 12 months, Citi has updated country, regional, and global cyber incident response playbooks based on internal After Action Review processes and external assessments. Specific attention has been paid to incorporating business line input and client impact assessments into these documents. We have also updated both inter and intra team workflows to increase the velocity and focus of our incident response activities.

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

Our organization uses a Third Party Information Security Assessment process that includes active engagement in business risk and control monitoring, and reporting of changing third party risks (see answer for 4.3).

3. Analysis

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

Analysis of a cyber-incident takes many forms depending on the objective. Initial scoping and containment rely on high quality telemetry and network situational awareness. This feeds a robust and targeted response. As an organization moves through the various phases of incident response the objectives begin to change as well. Once an incident is contained the focus shifts to remediation. Effective remediation will require analysis informed by an accurate assessment of root cause. This, in turn, is predicated upon an understanding of process and workflow, inventory and status, controls and control gaps. These inputs come from the business, development, and operational teams as well as those in the information security arena.

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?

It is difficult to measure incident response recovery, given incidents have large severity variability and there is a much smaller sample size for major incidents. The use of a taxonomy and severity rating systems add significantly to both initial understanding of an incident, and throughout the incident response effort.

Research or investigation events and potential incidents will scope the potential incident and collaborate on next steps. Classification and research provides a common reference throughout the response process, indicating initial severity as well as updated assessments. Moreover, an objective analysis of a potential incident allows repeatability while fulfilling requirements specific to certain types of incidents (e.g. regulatory requirements in certain instances). In line with the ITIL and NIST frameworks, robust “lessons learnt” and problem management programs facilitate thorough root cause analysis after an incident response effort. This helps provide a mechanism for continuous improvement.

Establishing Key Performance Indicators that focus on the elements of incident response that an organization seeks to improve, change them as necessary and hold an After Action Review (or Lessons Learned) session to capture specific items that worked or did not work during an event. We believe the focus should be on robust process and company culture rather than the dependency on any one tool.

Determining root cause and contributing factors of an incident through post event analysis (once the incident has been contained) which focuses on the underlying issues, technical or otherwise, that allowed the event to happen in the first place (i.e. control failures or control gaps). This is followed by a commitment to address those issues and track the progress of those fixes.

4. Mitigation

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

• Information Sharing: Ensuring that accurate and effective information sharing between internal stakeholders is necessary, this can include summary of the situation; mitigation actions taken to contain it; impact of the incident to business; near term pending recovery actions and ways to prevent reoccurrence. A challenge with this method however is that it can hinder teams within organizations, especially those of a large size, to access information that is necessary and useful for them to know. It is important to find a way to balance internal protocol without creating an unnecessary hurdle for teams.

• Integration/Standardization: Understanding that the definition of “critical” can vary for different lines of business, we have a standard definition for Franchise Critical Applications and Processes. Importance should be placed on all response teams working on actionable intelligence and creating metrics that are meaningful and measurable during mitigation.

• Training: Organizations must ensure that the institution has all employees regularly involved and educated about security via a mature and evolving information security awareness program, this will encourage staff to follow best practices and guidelines during time of mitigation.

• Recording: Record current playbook calls as events unfold both to inform decisions taken during an incident and to reconstruct what happened afterwards. It is also necessary to maintain regulatory compliance.

• Investigation: Quickly determining what data was impacted allows Citi to 1) mitigate Client harm through notification and fraud prevention efforts, 2) mitigate impact to Citi through remediation and containment actions (e.g. password resets, configuration modification, etc), and 3) mitigate industry impact through prompt regulatory and sharing group notification when indicated. The focus would be on tools and practices that facilitate these three activities.

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?

(i) Data Breaches - Quickly determining what data was impacted allows Citi to 1) mitigate impact to the customer through notification and fraud prevention efforts, 2) mitigate impact to Citi through remediation and containment actions (e.g. password resets, configuration modification, etc), and 3) mitigate industry impact through prompt regulatory and sharing group notification when indicated. The focus would be on tools and practices that facilitate these three activities

(ii) Loss of Data Integrity - Backups - digital and tape backups are made in real time, time and size gates so that Citi can restore data from clean backups. Number and frequency of backups is based on information criticality

(iii) Ransomware - tools are used to identify rapid encryption of networked devices and to stop the process before it spreads

4.3 What tools or practices are effective for integrating the mitigation efforts of third-party service providers with the mitigation efforts of the organisation?

Our organization works together with third parties during a cyber incident – focusing on process, not a particular tool. It is an internal cyber incident process brought together by a centralized entity within our organization and business activity owners. In order to mitigate efforts with third-party service providers, we capture the Corrective Action Plans from issues identified during a Third Party Information Security Assessment (TPISA). TPISA includes cross-functional teams where the business activity owner of the third party relationship uploads evidence provided by the third party. It is than validated by the information security to ensure the original identified TPISA is issue has been addresses. Using TPISA, ownership resides with the business with whom the third party has the relationship – not with the information security team. The business uploads evidence provided by the third party and we then validate the uploaded evidence to ensure the original TPISA issue has been addressed.

While we currently do not have any tools which integrate third party's mitigation effort with our own, we have process and procedures in place to get evidence to validate if the third party has undertaken remediation of required patches to get to correct version of the software.

6. Improvement

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

The most effective exercises are ones that place the participants in their actual roles (or 1 up/down). This challenges the participant to make decisions under an artificially created high stress environment thereby giving the participant experience at making decisions under stress and learning from the experience. Citi conducts events like these with executive level Country, Regional, and Corporate executives. The Cyber Security Fusion Center also conducts tactical drills with its staff to rehearse their defined cyber crisis management process. These exercises are successful because they are developed in partnership with the exercising organization to meet specific objectives and then a detailed report with specific, tangible corrective actions is created and followed up on.

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

Most exercises will have a cross border element as leadership decision making for cyber security incidents is normally done in partnership with regional and/or global leaders. Cross sector provides an increased challenge as developing an event that has a specific or unique, tangible objective/benefit for each sector often results in a less specific objective (ex. how do we respond to ransomware). Less specific objectives can also result in less significant learnings after 1 or 2 iterations.

The lessons learned from cross sector and cross border exercises can serve to highlight the communications and decision making challenges a large and diverse organization may have. The more diverse the participants in the exercise the more complex the planning and execution of the event becomes. It is nearly an exponential level of complexity to put together a truly effective cross sector and cross border exercise. For example, the US Naval War College does this several times a year, but they have a dedicated military and civilian war gaming staff and a significant budget for these events as well as a very clearly defined and motivated group of participants.

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

As mentioned earlier in question 1, the deployment of Symphony, a secure chat platform, was launched to allow for communication and collaboration amongst teams and employees across regions and time zones.

Endpoint detection and response (EDR) is a category of tools and technology used for protecting Windows and Linux based endpoints (servers and desktops) —from potential threats. EDR is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

Citi has increased leverage of endpoint detection and response (EDR) tools. Real-time endpoint activity telemetry helps gain attack detail visibility, context and history for an alert without the need to wait for queries of specific data from an endpoint. Leveraging visibility of real-time endpoint activity enables earlier triage and the ability to review disk operations associated with an event in real-time.

Other tools include playbooks, wallet cards and related security products are useful for reference but the most important tool we have is the ability to bring together quickly decision-makers on a call and determine the best course of action. Attached separately is a *Cyber Scenario Checklist* to help leaders and FIs evaluate the situation and aid in identifying what parts of their organization need to be engaged and what aspects of the markets including liquidity need to be considering during decision making.

Looking Ahead: How Might the Public Sector Help?

1. Globally coherent and consistent regulation underpinned by cross-border regulatory and supervisory co-operation.

    a. Regulatory harmonization will limit the burden on both large and smaller organizations – for example, different regulators are making requests for onsite pen testing. We would like to see more coordination from regulators, where they partner in their requests from firms especially when it is an extensive ask.
    b. Support from FSB and other financial sector entities for the establishment of mechanisms and/or legal frameworks to combat transnational cybercrime. Criminals are less and less likely to be located in the territory where the crime is taking place, the final destination of the defrauded money may be in a third jurisdiction, and dealing with different cooperation protocols, or lack of cooperation, adds time to the process.
    c. Streamline reporting requirements – for example, identify at what stage and/or time frame during a cyber incident or attack FI needs to send reports.
    d. Common framework and standards for "risk and principals based" regulation.

2. Ensuring a client-centric and business-driven approach is taken to business services, harm and impact tolerances.
    a. Third Party diligence standards.
    b. Mapping collective vendor/supplier dependencies across the FI sector.
    c. Consider bringing systemically critical suppliers into the fold.
    d. Cyber exercises and testing specifically for financial industry sector; fire drills for critical infrastructure.

3. Strengthening and evolving public and private sector coordination and collaboration.

    a. Information Sharing – continue and enhance information sharing between public and private sectors, and across and within FI. Sharing information (and/or intelligence) can contribute to a firm's: cyber threat awareness; insights into the activity directly affecting a peer firm's network; ability to understand what is affecting a given sector or geography; how a threat manifests / operates; and, what can be done to defend against it.
    b. By exchanging cyber threat information, firms can improve:
        i. Awareness of current cyber threats affecting various sectors – at the trend and specific threat actor levels
        ii. Understanding of attackers' tactics, techniques, and procedures
        iii. Insight acquisition that would otherwise be unavailable / inefficiently available through public sources or security vendor reporting
        iv. Decision making regarding technology, controls, and resources allocation and escalation
        v. Threat targeting understanding
        vi. Detection enhancement capabilities on networks
        vii. Mitigation and responses prior to an actual event

Initial and Select Cyber Recovery Scenario Response Checklists

Each cyber event will be different and unique. To assist an organisation in responding to and recovering from a cyber event, leaders should actively engage in forming a series of high-level impact scenarios and a “checklist” of considerations.

The next section provides a suggested only quick reference checklist for organisational leaders; organisations and their business and product teams should develop their own checklists, tailored to their requirements and responsibilities:

1. to assess the impact of the event;
2. ensure the appropriate escalation and crisis management structures are in place; and
3. consider when developing recovery measures to respond to each unique event.

Note that Organisations and their Businesses (Functions and Products) can be impacted at a Global, Regional and Country level.

Scenario	Impact Assessment	Escalation: Command & Control	Recovery Considerations
Loss of Critical Application(s) **Loss of Critical**	☐ Is the application(s) used by the organisation globally, regionally or within a single country only? ☐ Is the entire application impacted or just certain features / abilities? ☐ What critical business processes and products are affected by the loss of this application(s)? ☐ What are the non-mission critical processes that can be immediately suspended? ☐ Will this event result in market / systemic risk? ☐ What critical processing timelines are impacted / at risk? ☐ What is the impact to Funding and Liquidity requirements?	☐ Have you engaged operations and technology production support teams? ☐ Has the CTI Incident Management Process been invoked? ☐ Is security and investigative services engaged? ☐ Is the Business Command Centre engaged? ☐ Do the Regional or Global Crisis Management Structures need to be engaged? ☐ What communication needs to be provided and when to the following: ○ Global Line of Business. ○ Clients. ○ Regulators ○ Legal Entity Management / Country Heads or Directors ○ Financial Market Infrastructures / Central Banks. ☐ Who is on point for coordinating the above? Have the appropriate local Crisis Management Teams been engaged?	☐ What are the business mitigations that can be deployed (manual processing, lower payment thresholds, request currency cut off extensions etc.)? Who needs to be engaged in the decision making for any such mitigations? ☐ Have Technology confirmed if the event is impacting both Production and COB? ☐ Can processing be supported by other locations? ☐ Consider alternate processing mechanisms and/or systems to process critical transactions ☐ How long can we use alternate processing methods? Are there any volume / value restrictions with alternative processing methods? ☐ Have Technology provided you with an expected duration? ☐ Have Technology provided you with a last ‘known good’ recovery point?

Scenario	Impact Assessment	Escalation: Command & Control	Recovery Considerations
Application(s) Cont'd	☐ What impact will this outage have on our client's liquidity and funding needs? ☐ What are upstream and downstream dependencies on this application(s)? ☐ Is the application hosted in a strategic data centre or hosted in-country? ☐ Which Legal Entities are impacted? Is this impacting the broker dealer and/or bank chain? ☐ Are there any local regulatory requirements that must be considered (e.g., Data Privacy, Cross CCO, and Regulatory Notification within a set timeframe)?	Have the required business crisis management teams been engaged?	☐ Can existing methods be used to recover the application (infrastructure, application, data)? ☐ Are there upstream and downstream dependencies that need to be considered? ☐ Establish client prioritization; do we need to increase / decrease daylight and overnight overdraft limits for clients? ☐ Are there any overnight processes / batch jobs that will be impaired as a result of this outage? ☐ Is there a risk of duplicative transactions when invoking a contingency option? ☐ How do we maintain the security and soundness of applications and data if invoking contingency methods? ☐ Go / No-Go for recovery measures / alternative processing – who needs be in engaged from the business / provide final approval?

Scenario	Impact Assessment	Escalation: Command & Control	Recovery Considerations
Impact to FMUs / FMIs **Impact to FMUs / FMIs Cont'd**	☐ What impact does this outage have on Clients' liquidity? ☐ Clearly identify impacted market attributes Deliver vs. Payment, Central Counterparty, Trading cycle (T+1/2/3)? ☐ What critical processing timelines will be impacted? ☐ What critical business processes are affected? ☐ What impact will this outage have on the markets (increase / decrease volumes / volatility) ☐ Will the FMI / FMU outage result in currency / FX impact (e.g. run on Sterling if UK RTGS systems are down?) ☐ Do we have an ETA for resolution? ☐ Which Legal Entities are impacted? ☐ Is there a risk of the organisation becoming a liquidity trap if clients continue to instruct payments to it? Is the organization then	☐ Have you engaged your business line operations and technology Production Support teams? ☐ Is the Business Command Centre engaged? ☐ Is the FMU / FMI shutdown notification emanating from an authorized source ☐ Who from the organisation is responsible for Crisis Management interaction with this FMI? ☐ Who from the organisation is interacting with other market participants and coordinating updates to ensure the full picture is understood? ☐ Has the technology infrastructure Incident Management Process been invoked? ☐ Are security and investigation management engaged? ☐ Do the Regional or Global Crisis Management Structures need to be engaged? ☐ What communication needs to be provided and when to the following:	☐ Are there alternate processing mechanisms existing for the impacted FMU / FMI (e.g., CHAPS – MERS) ☐ Are there transaction limits imposed on these alternate process capabilities? ☐ Do alternate bi-lateral settlement / processing capabilities exist that need to be initiated? ☐ Establish client prioritization – do we need to increase / decrease daylight and overnight overdraft limits for clients? ☐ Do we understand the regulatory issues if we were to isolate ourselves from a clearing house and/or central bank? ☐ How does the organization support Market confidence? ☐ What are the operational and liquidity and funding implications of an emergency bank holiday? ☐ Verify trade-off between excess liquidity, credit risk and market risk.

Scenario	Impact Assessment	Escalation: Command & Control	Recovery Considerations
	unable to make settlement via the FMIs/FMUs? ☐ Is the organisation a direct or indirect member of the FMI / FMU ☐ Would a 'bank holiday' assist the situation? ☐ What is the impact to market confidence from the organization's action / response thus far? ☐ Do we need to consider potential contagion and negative sentiments on the market and subsequent wider impact on retail customers? ☐ Does the organisation need to fund the markets to maintain overall liquidity.	○ Clients. ○ Regulators. ○ Legal Entity Management / CCO or Directors. ○ Clearing Houses and Exchanges. ○ Financial Market Infrastructures / Central Banks. ☐ Who is on point for coordinating the above – has this been established? ☐ Could the situation trigger a threshold for invoking the organization's Recovery & Resolution Plans?	☐ What is impact to client assets and CASS obligations? ☐ Can settlement / processing take place via other currencies? For example, if UK RTGS solutions are down, can clients settle in other currencies? What would An organisationdo to support such requests? ☐ Is there a risk of duplicative transactions when invoking the contingency option? ☐ Does the organisation need to activate contingency funding plan (if appropriate)?

Scenario	Impact Assessment	Escalation: Command & Control	Recovery Considerations
Agent / Correspondent banks that the organisation relies on to support cash flow to Clients	☐ What is the nature of the impact on the Agent / Correspondent Bank? ☐ When did the issue occur? Are there any trades / payments that are 'in-flight' and unaccounted for? If so what is the exposure? ☐ Will the outage of the Agent / Correspondent Bank result in any market confidence concerns / systemic risk? ☐ How did they get into this position? ☐ How are the markets likely to respond? Can the organisation expect increase flows as a result of this institution being impacted? ☐ What is impact to the organization's own liquidity and capital adequacy ratios? ☐ Do we have common clients? If so would our clients who also bank with the impacted	☐ Have you engaged your business line operations and technology Production Support teams? ☐ Is the Business Command Centre engaged? ☐ When did the Agent / Correspondent Bank first report the issue? ☐ When did we first recognize any impact? ☐ Is this issue public / visible to the market / clients? ☐ What clients are supported by this Agent/Correspondent Bank and therefore which cover/product teams must be engaged? ☐ Do we understand the full picture of the relationship with the Agent Correspondent Bank across all products? ☐ Have the Global Third Party Management Team and Business Bank Network Groups been engaged?	☐ Are there alternate agent/ correspondent bank relationships that can be explored? ☐ Are there alternative processing options for a subset of the transactions? What are the limits? How are the transactions prioritized? ☐ Can the affected service be processed in-house? ☐ What action needs to be taken to invoke the contingency option? What is the time to implement the contingency option? ☐ Are there any volume / capacity constraints with the contingency option(s)? ☐ Is there a risk of duplicative transactions when invoking the contingency option? ☐ Do we need to monitor intraday cash settlement? If so, in which currencies?

Scenario	Impact Assessment	Escalation: Command & Control	Recovery Considerations
Agent / Correspondent banks the organisation relies on to support cash flow to Clients Cont'd	institution need credit lines to be extended? ☐ Does the organisation need to consider taking on the impacted Bank's obligations e.g., governmental banking services to help maintain the economic wellbeing – if so – consider the risk appetite? ☐ What types of transactions are impacted (i.e., all, certain transaction types, transactions associated with certain types or limited number of Clients, a certain geography)? ☐ What is the expected duration of the outage and are there critical processing timelines affected? ☐ Are there any regulatory implications? ☐ Is the impact across the whole group or just a particular business / geography within the Agent / Correspondent Bank?	☐ Do the Regional or Global Crisis Management Structures needs to be deployed? ☐ What information is being provided by the Agent / Correspondent Bank? What information is in the public domain?	☐ Can payments be made a net basis and directly if systems / infrastructure are down? ☐ If systemic – could the organisation clear on their behalf (subject to the transfer of associated costs, our firm's ability to do so and subject to the policies and regulatory limitations)? ☐ Do we need to consider potential contagion and negative sentiments on the market and subsequent wider impact on retail customers?