Questions	Answers
Information about the respondent	
A. Name of respondent institution/firm	French Banking Federation (FBF)
B. Name of representative individual submitting response	Maya ATIG
C. Email address of representative individual submitting response	cgourlet@fbf.fr
D. Do you request non-publication of any part(s) of this response? If so, which part(s)? *Unless non-publication (in part or whole) is specifically requested, all consultation responses will be published in full on the FSB's website. An automated e-mail confidentiality claim will not suffice for these purposes.*	no
E. Would you like your response to be confidential (i.e. not posted on the FSB website)?	No

Questions	Answers
Consultation questions	
General questions	
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?	The COVID-19 has mostly brought a revamping of already-existing fraudulent activities against which our existing blocking technologies are effective. There is no real and significant raise of cyber-attacks targeting major banks. <u>Following actions have been done :</u> • Adaptation of security policies to massive remote access work. • Security focus on strong auth: improvement of our follow-up capacities (dashboards) • Definition of new use cases on workstations cyber risks • Focus to be done on third party and supply chain KYS
2. To whom do you think this document should be addressed within your organisation?	• Global, Deputy and Departmental CISOs • Chief Information Officers • Enterprise and Operational Risk Officers • CISO community • PCR teams • Cybersecurity operations teams • Operational risk teams • BCM teams • CERT • IT department/incident teams

Questions	Answers
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?	French banks all started from a common framework (mostly ENISA or NIST) and made it evolve to fit their specificities. FBF members have developed internal policies and procedures to support their organization's business continuity and cyber security incident recovery and responses. Such policies and procedures follow the main common European and international framework (mostly ENISA or NIST), regulation requirements (EBA guidelines, national legislations, etc.) and well-formed and industry recognised best practices (such as NIST, ISO27001, PCI, etc.). The current fragmentation of cybersecurity regulations across the financial services industry is a key concern for the European banking industry: rather than improving resilience, a global regulatory environment for financial services cybersecurity that is not properly coherent is likely to increase financial stability risk by driving complexity into the system. In order to ensure such coherence and reduce the above-mentioned risk, the FBF believes that the current toolkit should further encourage authorities to adopt more uniform practices by referring to existing and well-established mechanisms and best practice. Many companies use the "Financial Sector Profile" that 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
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.	The organisation structure for cyber incident response and recovery activities of FBF members appears to be aligned with the components described in the FSB toolkit. All existing cyber incident response frameworks can be mapped easily with the seven components of the toolkit.

Questions	Answers
5. Based on your organisation's experience, please provide any additional effective practice(s) for any of the tools. Please list the number of the tool (e.g. Tools 1 – 46) and describe the effective practice(s).	It is difficult to add effective practises without going into a very specific and dedicated activities. FBF members proposed to enhance tool #14 as follows: Disaster recovery sites should be placed on different locations to reduce having same time exposure on: • Physical threats (e.g. Earthquake) • Terrorist actions Another example of a useful investment would be: #36. Technological aids: CIRR training solutions for staff that recreates the conditions of an attack.
6. Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).	Nothing to add ; provided examples are sufficient and explicit enough to illustrate each topic.
7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?	FBF members confirmed that banks are in constant contact with competent authorities and with National or European centers for cyber threats, with the aim to collect and distribute any useful information (e.g. remediation actions, business continuity, etc.). However, members also noticed that the regulatory framework should not limit too much the cooperation between peers for the resolution of cyber incidents, as it happens with the limited data exchange between CERTs resulting from the strict compliance with privacy regulations or with incident reporting overload. Coordination between authorities is particularly important for cyber incident reporting. The current regulatory landscape is in fact characterized by a high degree of fragmentation, with differing thresholds, timing, templates and

Questions	Answers
	information requirements. This fragmentation is not only increasing complexity and administrative burdens for financial institutions, which continue to be the most targeted entities by cyber criminals, but it is also adding costs and diverting resources from where they are most needed. Authorities should work closely with FI for the development of a public-private secured platform. National authorities could organize information exchange around a regular meeting with CERTs teams and provide a template of exchange to keep on following with trends and threats.(ex: *Cyber information sharing and collaboration program* in the US) National authorities should also rethink their way to cooperate with the private sector by selecting useful information to share securely and develop bilateral networks of cooperation on cybercrime. In conclusion : - legislations should not prevent cooperation between peers for the resolution of cyber incidents (as already discussed, privacy regulations are sometimes a problem for exchanging data between CERTs) - Authorities should pay attention to the reporting overload they can generate during a crisis (specific inquiries…)

Questions		Answers
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?	No unique answer to provide, this is different from one bank to another.
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?	French banks promote a non-punitive culture through : • dedicated training programs : banks are training and encouraging their personnel to immediately inform the IT Security and Control Office on any suspicious activity they observe. Moreover, banks are also participating in numerous cyber-awareness campaigns. • Awareness campaigns: they are numerous and widespread within each organisation. • Past incidents example used to illustrate the fact that full disclosure is the best way to go for everybody's interest. • IT/Digital and communication tools charter to be acknowledged by each collaborator. • Phishing campaigns, training.
2.	**Preparation**	
2.1	What tools and processes does your organisation have to deploy during the first days of a cyber incident?	No many things to add that is not already covered by the toolkit. In addition to the tools and processes identified in the toolkit, the majority of French banks have also planned and implemented mechanisms to identify and categorise the threat as well as tools to isolate the threat source .

Questions		Answers
2.2	Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.	There is still a significant difference in the number and modality of cyber incident response plans implemented by banks across Europe. However, some FBF members reported that at least two (2) cyber security simulation exercises have been performed over the last 12 months in order to measure the effectiveness of the cyber incident procedure and the efficiency of the cyber incident response and recovery tools .
2.3	How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?	FBF members usually mitigate risks stemming from third party service providers with : Contractual aspects with specific security clauses + pre-contracting risk analysis + mitigation plans following-up + initial and periodic security questionnaires for a selection of outsourced services. Nothing more to provide without going into very specific, local, and dedicated activities.
3.	**Analysis**	
3.1	Could you share your organisation's cyber incident analysis taxonomy and severity framework?	See answer 3 to general questions. Severity frameworks are usually confidential but influenced by the criteria provided by the ECB for Significant Incident reporting.
3.2	What are the inputs that would be required to facilitate the analysis of a cyber incident?	.

Questions	Answers
	Although each organisation has its own specific inputs to facilitate the analysis of a cyber incident, system logs, network traffic and communication logs (input and output to external organization network) have been considered as the most common by FBF members. Input that would be required to facilitate the analysis of cyber incident : Preparation by the efficient threat intelligence
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?	Nothing to add that is not already covered by the toolkit or too dedicated to a specific context.
3.4 What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?	French organisation : A National Crisis Management organization led by Banque de France, an Inter-CERT-FR community led by the ANSSI, a sub-community of it dedicated to major French banks, the FS/ISAC (for some banks), the FBF cyber working group for best practices sharing, the FIRST (for some banks), the TF-CSIRT (for some banks), the CIRCL and CERT-EU, plus ad-hoc intelligence sharing communities like the ones that were created in the context of COVID-19. For some banks : participation to “Institute of international finance” + “European financial services roundtable”
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?	Too specific to every single organisation, production, technology, and context. However, classic containment measures must be taken: cut ties with internal and external providers, and cut internet access.

Questions	Answers
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?	FBF members follow international best practices and standard recommendations to mitigate the impacts from cyber incidents. These actions are concentrated at CERTS level. Banks are also using the cyber kill chain to better understand and combat ransomware, security breaches, and advanced persistent attacks (APTs). The use of this valuable solution should be further encouraged. Example of tool to mitigate the impact : Threat intelligence in order to better get prepared to new attacks modus operandi.
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?	There is plurality of views, offers and solutions: the risk management policy for third parties providers is specific in establishments (monitoring tools and specific criteria) but is part of the integrated risk monitoring policy (which includes crisis and incident management)
4.4 What additional tools could be useful for including in the component Mitigation?	Too specific to every single organisation, production, technology, and context.
4.5 Are there situations in which effective practices for mitigation and restoration activities of the organisation are the same or overlap substantially? If yes, please provide examples.	Yes, there is, but it is too specific to every single organisation, production, technology, and context.
5. Restoration	
5.1 What tools and processes does your organisation have available for restoration?	Too specific to every single organisation, production, technology, and context.
5.2 Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?	Too specific to every single organisation, production, technology, and context. Members use cyber incident taxonomy and criticality scale.

Questions	Answers
5.3 How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?	Too specific to every single organisation, production, technology, and context.
6. Improvement	
6.1 What are the most effective types of exercises, drills and tests? Why are they considered effective?	According to FBF members, penetration test and red team exercises are the most effective exercises because, by simulating real-time attacks, they test the organization's resilience and identify areas of improvement. Yes, these exercises often spot areas of improvement
6.2 What are the major impediments to establishing cross-sectoral and cross-border exercises?	FBF members identified the following impediments to establish cross-sectoral and cross-border exercises: Different Legal/Regulation Frameworks; Financial Factors; Institutional factors; Cultural Factors. To be captivating exercises have to include a few technical details, it is very hard to provide realistic ones in a cross-sectoral or cross border scenario (it is already hard in a cross-bank one). Major impediments are: different regulatory frameworks, financial sector specificities, strong disparity maturity.
6.3 Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery?	During attack phases and through the lifecycle of a cyber-attack, gathering intelligence and sharing it with peers and industry it is very important: major FBF banks carry out these activities through ad-hoc tools on a case-by-case basis. Some FBF members also consider AI-based tools as useful instruments to improve cyber incident response and recovery . When facing major incident computer forensics experts with enough real situation experience are useful to improve incident response and recovery.

Questions	Answers
	Cyber warfare training tools can be very useful to ensure continuous improvement of response teams. Ex: cyberange (Thalès)
7. Coordination and Communication	
7.1 Does your organisation distinguish "coordination activities" from broader "communication" in general? If yes, please describe the distinct nature of each component.	FBF members make a clear distinction between the CIRT team, which is responsible to coordinate activities during the incident handling period, and the other units responsible to communicate with other stakeholders : - CERT team are involved in with the handling of the crisis/incident - Communication team is more in charge of diffusing messages to internal and external stakeholders **It is imperative to coordinate internal and external communication towards clients / the press / social media.**
7.2 How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident?	In such cases, FBF member banks usually use duplicate autonomous channels, such as mobile applications (Signal, Threema, etc.), secure communication channels through mobile (like Citadel) and even courier.
7.3 Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?	Punctual finding from monitoring tools (ex: Darkweb monitoring) bank investigations that are more of interest for authorities (Police) than the private organisations.
Other comments	Remarks / questions on the toolkit **§3 Scribe / independent Observers (p 4 of the toolkit)** Cyber crisis management embed traditionally a role of "crisis secretary", exclusively in charge of recording events and decisions. For efficiency of organizations, we consider, in most of the cases, that those crisis secretaries are independent enough to assume also the role of independent observers, as long as :

Questions	Answers
	- they are exclusively dedicated to those two roles (i.e. crisis secretary and independent observer) - and are not hierarchically dependent from the operational teams in charge of the crisis resolution operations. However, we confirm that in case of strong magnitude crisis, the crisis management team could be usefully completed with a role of independent observer not dedicated to any other role, even the role of crisis secretary. As a criteria of independency, we suggest this role could be assigned to a member of the 2nd or 3rd line of defense. **§8 Metrics (P 5 of the toolkit)** We agree with the establishment of metrics to measure impacts and report to the management. However, the examples provided in the box suggest that a very quantitative and statistic approach would be suitable to cyber incidents. This is not the case : when a cyber incident hits a company delivering many services, at the infrastructure level, consequences are widespread on all company services, with different kind of impacts. Therefore, figures like "number of records" or "duration of unavailability" cannot be compared for different services, as the impact is business-dependent (equity markets SLA measure unavailability in minutes whereas life insurance or real estate portfolios SLA measure unavailability in weeks).