Electronic Money Association
Crescent House
5 The Crescent
Surbiton, Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
www.e-ma.org

Jan Ceyssens
Head of Unit
DG FISMA B.5
European Commission
Rue de Spa 2 / Spastraat 2
1000 Bruxelles

19 March 2020

Dear Jan

Re: EMA response to European Commission Consultation on Digital Operational Resilience Framework for financial services

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our comments and proposals.

Yours sincerely,

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA responses

No	Question	EMA response
1	Taking into account the deep interconnectedness of the financial sector, its extensive reliance on ICT systems and the level of trust needed among financial actors, do you agree that all financial entities should have in place an ICT and security risk management framework based on key common principles?	The EMA agrees that financial service providers should consider (and identify/monitor/ track/manage) ICT and security risks as part of their overall risk management framework. The establishment of key common principles that are followed by the risk management frameworks of financial service providers could be beneficial and should extend beyond ICT and security risks. Any common risk management framework principles should acknowledge the divergence in scope, size and operational footprint of financial service providers across the EU.
2	Where in the context of the risk management cycle has your organisation until now faced most difficulties, gaps and flaws in relation to its ICT resilience and preparedness? Please rate each proposal from 1 to 5, 1 standing for 'not problematic' and 5 for 'highly problematic'). ▪ Identification Detection ▪ Ability to protect ▪ Respond ▪ Recovery ▪ Learning and evolving	▪ Identification Detection -> 3 ▪ Ability to protect -> 2 ▪ Respond -> 3 ▪ Recovery -> 2 ▪ Learning and evolving ->4 ▪ Information sharing with other financial actors on threat intelligence ->5 ▪ Internal coordination (within the organisation) ->2

	▪ Information sharing with other financial actors on threat intelligence ▪ Internal coordination (within the organisation) ▪ Other (specify)	▪ Other (specify). Threat intelligence information sharing by government/law enforcement agencies (and CERTs/relevant NCAs) with PSPs -> 5 ▪ Other (specify). Realistic exercising of business continuity arrangements to establish the attainability of stated continuity objectives -> 3
3	What level of involvement and/or what type of support/ measure has the Board (or more generally the senior management within your organisation) offered or put in place/provided for, in order to allow the relevant ICT teams to effectively manage the ICT and security risk? Appropriate allocation of human and financial resources Appropriate investment policy in relation to the ICT and security risks Approval by the Board of an ICT strategy (that also deals with ICT security aspects) Active role of the Board (or the senior management) when your organisation faces major cyber incidents or, as the case may be, role of the Board in the ICT business continuity policy Top leadership and guidance received in relation to ICT security and ICT risks	As part of the authorisation/licensing process, the senior management of payment service providers (PSPs) is required to: ▪ Allocate appropriate funds and resources to support risk management activities, ▪ Establish/agree an ICT Strategy that supports the company business strategy and, ▪ Track the implementation of the ICT strategy. To meet ongoing regulatory compliance requirements, senior PSP management is also required to: ▪ Establish sound business continuity management processes, ▪ Establish an effective detection and reporting process for Major security and operational incidents as these are defined in the EBA Guidelines on major incident reporting under PSD2 (EBA/GL/2017/10).

4	How is the ICT risk management function implemented in your organisation?	As detailed in Guideline 2.5 of the EBA Guidelines on the security measures for operational and security risks under PSD2 (EBA-GL-2017-17), PSPs are required to establish three effective lines of defence, or an equivalent internal risk management and control model, to identify and manage operational and security risks. In order to comply with the Guideline above, PSPs must ensure that the risk management function has sufficient independence, resources and reporting lines to the senior management body of the PSP.
5	Which main arrangements, policies or measures you have in place to identify and detect ICT risks? Do you establish and maintain an updated mapping of your organisation's business functions, roles and supporting processes? Do you have an up-to-date registry/inventory of supporting ICT assets (e.g. ICT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes)? Do you classify the identified business functions, supporting processes and information assets based on their criticality? Do you map all access rights and credentials and do you use a strict role-based access policy? Do you conduct a risk assessment before deploying new ICT technologies / models? Other (please specify)	[Responses to be provided by individual members.]

6	Have you experienced cyber-attacks with serious repercussions for your clients or counterparties? To the extent you deem it necessary, please explain and illustrate in particular the nature of the attack and the impacts on the clients/counterparts.	[Responses to be provided by individual members that may be prepared to share insights on cyber attacks they have experienced.]
7	How many cyber-attacks does your organisation face on average every year? How many of these have/are likely to create disruptions of the critical operations or services of your organisation?	[N/A]
8	Do you consider that your ICT systems and tools are appropriate, regularly updated, tested and reviewed to withstand cyber-attacks or ICT disruptions and to assure their operational resilience? Which difference do you observe in this regard between in-house and outsourced ICT systems and tools?	[N/A]
9	Has your organisation developed and established a cloud strategy?	[N/A]
10	If the answer to Question 9 (above) is Yes: Do you use on-premise cloud technology? Do you use off-premise cloud technology Does this strategy contribute to managing and mitigating ICT risks? Do you use multiple cloud service infrastructure providers? How many?	[N/A]

	Did your Board and senior management establish a competence center for cloud in your organisation?	
11	Do you have legacy ICT systems that you would need to reconsider for enhanced ICT security requirements? What would be the level of investments needed (in relative or absolute terms)?	[N/A]
12	What in your view are possible causes of difficulties you experienced in a cyber-attack/ ICT operational resilience incident? ICT environmental complexity Issues with legacy systems Lack of analysis tools Lack of skilled staff Other (please specify)	[N/A]
13	Do you consider that your organisation has implemented high standards of encryption?	[N/A]
14	Do you have a structured policy for ICT change management and regular patching and a detailed backup policy?	Guideline 4.7 of the *EBA Guidelines on the security measures for operational and security risks under PSD2 (EBA-GL-2017-17)* already instructs PSPs to check regularly that the software used for the provision of payment services, including the users' payment-related software, is up to date and that critical security patches are deployed. Guideline 6 of these Guidelines instructs PSPs to establish sound business continuity management to minimize the impact of any incident on their

		ability to deliver payment services to their customers. Most PSPs have a documented backup policy that forms part of their business continuity management framework.
15	Do you consider that your organisation has established and implemented security measures to manage and mitigate ICT and security risks (e.g. organisation and governance, logical security, physical security, ICT operations security, security monitoring, information security reviews, assessment and testing, and/or information security training and awareness measures)?	The *EBA Guidelines on the security measures for operational and security risks under PSD2 (EBA-GL-2017-17)* require PSPs to identify and monitor a range of risks that may impact the delivery of regulated services as part of their risk management framework; ICT and security risks are managed through this framework. PSPs deploy mitigating controls to manage specific ICT/security risks based on their impact rating. The effectiveness of these security controls must be audited by auditors with expertise in IT security and payments; these auditors are required to be operationally independent within or from the PSP. PSPs are required to submit an Operational and Security Risk Report to the relevant national competent authority at least once every 12 months.
16	On average, how quickly do you restore systems after ICT incidents, in particular after a serious/major cyber-attack? Are there any differences in that respect based on where the impact was (impact on the availability, confidentiality or rather the integrity of data)?	[N/A]
17	Which issues you struggle most with, when trying to ensure a quick restoration of systems and the need to maintain continuity in the delivery of your (critical) business functions? Lack of comprehensive business continuity policy and/or recovery plans	[N/A]

	Difficulties to keep critical/ core business operations running and avoid shutting down completely Internal coordination issues (i.e. within your organisation) in the effective deployment of business continuity and recovery measures Lack of common contingency, response, resumption/recovery plans for cyber security scenarios - when more financial actors in your particular ecosystem are impacted No ex-ante determination of the precise required capacities allowing the continuous availability of the system Difficulties of the response teams to effectively engage with all relevant (i.e. business lines) teams in your organization to perform any needed mitigation and recovery actions Difficulty to isolate and disable affected information systems Other (please specify)	
18	What are your views on having in the legislation a specific duration for the Recovery Time Objective (RTO) and having references to a Recovery Point Objective (RPO)? To the extent you deem it necessary, please explain your reasoning.	The EMA believes that the senior management of individual PSPs are much better placed to determine appropriate Recovery Objectives (RTO, RPO). These objectives will reflect the type, scope, and scale of the operational footprint of the services provided by individual regulated firms at a given time more accurately. These Recovery Objectives are reviewed and updated frequently to reflect the evolution of the services offered by a PSP. In this context, we are concerned that legislators will be unable to set Recovery objectives that (a) reflect the large differences in size, scope, and

		service portfolio across financial service providers and (b) are robust in the face of continuing service and technology evolution. Regulations often assume that imposing a particular methodology or set of controls provides the ideal solution. We believe that regulations should rather focus on outcomes rather than prescribing specific solutions to achieve these outcomes. PSPs understand the risks they face and should be afforded the flexibility to develop their own treatment to achieve outcomes described in regulations. Where regulations are too prescriptive in proposing a one-size-fits-all solution, the results can be counterproductive (e.g. by limiting new service innovation or by failing to evolve to address emerging threats)
19	Through which activities or measures do you incorporate lessons post-incidents and how do you enhance the cyber security awareness within your organisation? Do you promote staff education on ICT and security risk through regular information sessions and/or trainings for employees? Do you regularly organize dedicated trainings for the Board members and senior management? Do you receive from the Board all the support you need for implementing effective cyber incident response and recovery improvement programs? Do you make sure that the root causes are identified and eliminated to prevent the occurrence of repeated incidents?	Guideline 8 of the *EBA Guidelines on the security measures for operational and security risks under PSD2 (EBA-GL-2017-17)* instructs PSPs to establish and implement periodic security awareness programs to educate their staff on security-related risks. Employees that hold specific key roles receive targeted information security training at least once every 12 months. *Guidelines 2.17 & 2.20 of the EBA Guidelines on major incident reporting under PSD2 (EBA/GL/2017/10)* require PSPs to include detail on the identified root cause of any previously reported incident in the Final Report that is submitted to the relevant NCA.

	Do you conduct ex post root cause analysis of cybersecurity incidents?	
20	Is your organisation currently subject to ICT and security incident reporting requirements?	EMA Members are already required to compile and submit ICT/Security incident reports to the relevant NCAs as stated in: ▪ *The EBA Guidelines on major incident reporting under PSD2* (EBA/GL/2017/10), ▪ Directive (EU) 2016/1148 – the NIS Directive, ▪ Separate Card Scheme operating regulations for PSPs that form part of the payment cards' ecosystem. ▪ General Data Protection Regulation (Art. 33)
21	Do you agree that a comprehensive and harmonised EU-wide system of ICT and security incident reporting should be designed for all financial entities?	Yes, the EMA agrees that a proportionate and harmonised ICT & security incident reporting regime should apply to all regulated financial entities across the Union. The EMA expects that the adoption of a common incident reporting system will help streamline the incident reporting process for financial service providers across all EU jurisdictions. The goals of such a system should include: ▪ At a tactical level, the sharing of actionable information between system participants (on whom reporting obligations / costs are being imposed) ▪ The compilation and sharing of information to identify emerging threats and to guide strategic initiatives of regulated entities.

22	If the answer to the previous question (no. 21) is yes, please explain which of the following elements should be harmonised? Taxonomy of reportable incidents Reporting templates Reporting timeframe Materiality thresholds Other (please specify)	The EMA believe that a common EU incident reporting regime for ICT and security incidents that applies to financial service providers should seek to harmonise: ▪ The types of incidents that will be reported, ▪ The incident reporting templates and the information that is included in every report, ▪ The timeframe/frequency of submitted incident reports, ▪ The incident characteristics that trigger the declaration of an incident that will need to be reported.
23	What level of detail would be required for the ICT and security incident reporting? Please elaborate on the information you find useful to report on, and what may be considered as unnecessary. To the extent you deem it necessary, please explain your reasoning	The EMA proposes that the focus of any initial reporting should be on the scope/type of financial services that are impacted by the incident. Any initial reporting could also seek to establish an overview of the type of ICT/security incident that is being reported. The prompt submission of any initial report is often more important than the collection of comprehensive incident data to include in the report; the latter process often takes some time. Subsequent reporting should include more detail on the: ▪ Materiality thresholds that were breached to give rise to a report, ▪ Security controls deployed by the PSP to mitigate the impact of the incident, ▪ Projected timeline for return to normal operations, ▪ Incident characteristics, ▪ Impacted systems/assets/services,

		▪ Root cause(s) of the incident.
24	Should all incidents be within the scope of reporting, or should materiality thresholds be considered, whereby minor incidents would have to be logged and addressed by the entity but still remain unreported to the competent authority?	We would recommend that only ICT/security incidents that breach specific materiality thresholds should be reported to the relevant NCA. Incidents of lower impact can be managed by the financial service provider on an individual basis. Such an approach will allow NCAs to focus on the review of submitted Major Incident Reports. The EMA would recommend that the Commission seeks to incorporate the lessons learnt by the EBA and by relevant NCAs during their review of Major Incident Reports submitted by PSPs in compliance with the *EBA Guidelines on major incident reporting under PSD2* (EBA/GL/2017/10).
25	Which governance elements around ICT and security incident reporting would be needed? To which national competent authorities should ICT and security incidents be reported or should there be one single authority acting as an EU central hub/database? To the extent you deem it necessary, please explain your reasoning.	The EMA would recommend that the governance process elements associated with the incident reporting process described in the *EBA Guidelines on major incident reporting under PSD2* (EBA/GL/2017/10) are replicated in any overarching ICT/security incident reporting framework for all financial service providers. Specifically, the internal ownership of the process by a designated business role in the reporting entity and the submission of all reports according to agreed timescales. Financial service providers should be afforded the flexibility to use consolidated reporting to report incidents that (a) impact multiple regulated entities that are part of the same group or (b) relate to the same service or 3rd party service provider (e.g. cloud hosting provider). We recommend that incidents should only be reported to the Home NCA of a financial service provider. The adoption of such an approach would limit the likelihood of over-reporting of the same incident across multiple NCAs and make it easier to identify the point of origin of security-related incidents that have a cross-border impact.

		The fragmentation of efforts to improve cybersecurity across different EU (and international) bodies risks making it too complicated for service providers to develop effective cybersecurity strategies. Having to address inconsistencies in the regulatory framework, where competent authorities at a national level impose unique reporting or other requirements, results in a significant overhead for little gain. For example, Data Protection regulation is applied differently across the EU, making it difficult to implement a consistent strategy for the sharing of data with law enforcement and other businesses to prevent fraud. In particular, EMA members are concerned where requirements are imposed on companies by states where they are not established.
26	Should a standing mechanism to exchange incident reports among national competent authorities be set up? To the extent you deem it necessary, please explain your reasoning.	We believe that the existence of a standing incident report exchange mechanism between NCAs is a good first step that will improve the ability of NCAs to assess/track incidents that impact the delivery of financial services across multiple jurisdictions. Going forward, we would encourage the establishment of a centralised, EU data Hub/Portal to which entities could submit reports directly. This could guarantee the confidentiality of the information, and allow the secure exchange of incident reports among relevant NCAs in a controlled fashion. The Hub could also be used to allow regulated entities to submit incident reports to the relevant NCAs (Home/Host) using a single centralised reporting channel as part of an effort to streamline reporting arrangements.
27	What factors or requirements may currently hinder cross-border cooperation and information exchange on ICT and security incidents? To the extent you deem it necessary, please explain your reasoning and provide concrete examples.	The cross-border information exchange on ICT and security incidents is currently impeded by: ▪ Data privacy concerns (emanating from GDPR and from national data privacy legislation),

		▪ The absence of any established cross-border information sharing mechanism among industry participants, ▪ The wariness of financial service providers to share incident information with other industry participants to limit reputational damage, ▪ Existing regulatory reporting burdens, particularly where they are imposed by states where a financial service provider is not established. ▪ Inconsistencies in the regulatory framework, where competent authorities at a national level impose unique reporting or other requirements results in a significant overhead for little gain.
28	Is your organisation currently subject to any ICT and security testing requirements? If the answer is yes: Do you face any issues with overlapping or diverging obligations? Do you practice ICT and security testing on a voluntary basis?	EMA members comply with Guideline 7 of the *EBA Guidelines on the security measures for operational and security risks under PSD2* (EBA-GL-2017-17) that instructs PSPs to establish and implement a testing framework to validate the robustness and effectiveness of the security measures deployed to address security risks. PSPs that come into contact with payment card data also need to comply with the PCI-DSS card data security framework; this framework introduces its own requirements on the testing of defences deployed to protect payment card data. The application of multiple security control testing requirements often gives rise to duplication of testing effort and to time-consuming attempts to reconcile control testing requirements across multiple frameworks.
29	Should all financial entities be required to perform a baseline testing/assessment of their ICT systems and tools? What could its different elements be?	It would be appropriate to introduce a requirement to perform a baseline testing/assessment of the controls deployed to address ICT & security risks for all regulated financial service providers. The assessment may comprise:

	Gap analyses? Compliance reviews? Vulnerability scans? Physical security reviews? Source code reviews? Others (please specify)	▪ Business Continuity Planning & testing, ▪ 3rd party security penetration tests, ▪ Internal vulnerability scans, ▪ Physical security reviews, ▪ Reviews of compliance with the company Security Policy.
30	For the purpose of being subject to more advanced testing (e.g. threat led penetration testing, TLPT), should financial entities be identified at EU level (or should they be designated by competent authorities) as "significant" on the basis of a combination of criteria such as: Proportionality–related factors (i.e. size, type, profile, business model)? Impact – related factor (criticality of services provided)? Financial stability concerns (Systemic importance for the EU)? Other appropriate qualitative or quantitative criteria and thresholds (please specify)?	The EMA supports the concept of requesting Significant financial service providers to complete TLPT. The identification of such entities by their Home state NCA will allow a more accurate designation of financial service providers as Significant (rather than allowing Host NCAs to carry out this task on an individual basis). The designation of Significant financial service providers should use the type of EU-wide market criteria that are listed in the Survey question (e.g. market share, service criticality, impact on financial stability across EU jurisdictions).
31	In case of more advanced testing (e.g. TLPT), should the following apply? Should it be run on all functions?	TLPT should seek to exercise the security controls deployed to protect all *Critical* Functions (as identified in the most recent Business Impact Analysis – BIA) carried out by the Significant financial service provider.
	Should it be focused on live production systems?	See feedback above.

	To deal with the issue of concentration of expertise in case of testing experts, should financial entities employ their own (internal) experts that are operationally independent in respect of the tested functions?	We do not perceive a need for all financial service providers to employ internal independent experts to carry out TLPT. Currently, PSPs use external specialist entities to carry out such testing on a periodic basis.
	Should testers be certified, based on recognised international standards?	It would be appropriate to ensure that entities offering TLPT services to financial service providers have attained one of the well-known industry certifications for security penetration testing services (e.g. CREST).
	Should tests run outside the Union be recognised as equivalent if using the same parameters (and thus be held valid for EU regulatory purposes)?	TLP tests that are executed outside the Union should be recognised as equivalent for an agreed period of time as long as they meet specific requirements (on the scope, process followed).
	Should there be one testing framework applicable across the Union? Would TIBER-EU be a good model?	The EMA believe that it would be appropriate to avoid establishing a single TLP testing framework (like TIBER-EU) to be used by financial service providers across the Union. The focus of any TLPT requirement should be on (a) the scope and frequency of such tests and (b) the levels of competence and independence of the entity that carries out the test.
	Should the ESAs be directly involved in developing a harmonised testing framework (e.g. by issuing guidelines, ensuring coordination)? Do you see a role for other EU bodies such as the ECB/SSM, ENISA or ESRB?	We would encourage an effort by the ESAs and ENISA to generate only high-level requirements for any future TLPT framework and allow individual testing service providers flexibility in meeting these requirements. There may be a role for national cybersecurity certification schemes - as developed under the Cybersecurity Act (Regulation EU 2019/881) – to certify individual TLPT service providers.
	Should more advanced testing (e.g. threat led penetration testing) be compulsory?	Our view is that the requirement to complete TLPT should only apply to Significant financial service providers (as identified in Question 30 above).

		Other financial service providers may carry out such testing on a voluntary basis.
32	What would be the most efficient frequency of running such more advanced testing given their time and resource implications? Every six months Every year Once every three years Other	We believe that current industry best practice of completing such testing once every 12 months (and after a significant change/re-configuration of the deployed security controls) provides an appropriate balance between security and convenience.
33	The updates that financial entities make based on the results of the digital operational testing can act as a catalyst for more cyber resilience and thus contribute to overall financial stability. Which of the following elements could have a prudential impact? The baseline testing/assessment tools (see question 29)? More advanced testing (e.g. TLPT)? Other (please specify)	We are not clear on the reference to a prudential impact in this question. If the EC suggests a link between prudential regulation compliance with the updates provided by financial service providers on the output of digital operational resilience testing, we would caution against the establishment of such a link. Prudential requirements are typically very clear and prescriptive; the outputs of any digital operational resilience testing will be varied and prove difficult to match with a set of prescriptive criteria.
34	What are the most prominent categories of ICT third party providers which your organisation uses? To the extent you deem it necessary, please explain your reasoning.	The most widely used categories of ICT third party providers used by PSPs comprise: ▪ Cloud hosting providers, ▪ Customer service/support service providers, ▪ Payment Transactions Processors/Payment Gateways and,

		▪ Customer onboarding service providers; these comprise customer identity verification and Sanctions/PEP checking service providers.
35	Have you experienced difficulties during contractual negotiations between your organisation and any ICT third party providers, specifically with regard to establishing arrangements reflecting the outsourcing requirements of supervisory/regulatory authorities? To the extent you deem it necessary, please explain your reasoning, elaborating on which specific outsourcing requirements were difficult to get reflected in the contract(s).	To deliver the cost, flexibility and time-to-deploy benefits that their customers expect, most cloud-based IT service providers insist on: (a) Offering generic Service Level Agreements, (b) Retaining the right to transfer data across different datacentre clusters and across systems shared with other entities, and (c) Engaging appropriate sub-contractors to carry out a range of support services. Therefore, many regulated firms have limited negotiating leverage to introduce changes to the standard service delivery agreements offered by the large reputable cloud IT service providers to reflect requirements by the relevant NCAs. Additionally, the growing use of shared, flexible, global infrastructure to deliver cloud-based IT services can make it challenging for a regulated firm to identify the applicable jurisdiction and the location of all relevant business premises at the time of negotiating a service delivery agreement. In turn, this limits the regulated firm's ability to specify the required access to system data and business premises of the cloud service provider that should be afforded to itself, its auditor and to the relevant NCA. Furthermore, in many instances service users do not have internal resources with the skill-set/tools required to test their internal ability to deliver specific outsourced IT services. In fact, for many cloud-based service users it is precisely the unwillingness to invest in building up such internal resource that led them to use cloud IT service outsourcers.

		Access to system/internal process data of cloud IT service providers is not currently provided in most cloud service outsourcing contracts. This is because systems are shared across many cloud outsourcers' clients and it would be extremely difficult to parse such system data and share only data that is specific to an individual client without compromising other clients' data.
36	As part of the Commission's work on Standard Contractual Clauses for cloud arrangements with financial sector entities, which outsourcing requirements best lend themselves for standardisation in voluntary contract clauses between financial entities and ICT third party service providers (e.g. cloud)? To the extent you deem it necessary, please explain your reasoning	The outsourcing requirements that a cloud hosting provider should grant scheduled (or emergency) staff/facility/data access to the auditors of the financial service providers or to the relevant NCA could be a strong candidate for standardisation in voluntary contract clauses. PSPs are finding it difficult to introduce such access clauses in the Service Level Agreements that the large cloud hosting providers currently offer to their clients.
37	What is your view on the possibility to introduce an oversight framework for ICT third party providers? Should an oversight framework be established?	The EMA considers it would be useful (although challenging from a logistical/operational point of view) to introduce an oversight framework for specific categories of ICT third party providers; for example, the Big 3 cloud hosting providers (AWS, MS Azure, Google Cloud Platform) or the bigger Payment Processors and Payment Gateways. Such a framework should empower the consumers of cloud services to be able to make competitive comparisons of the measures taken to achieve digital operational resilience by such third party providers.
	Should it focus on critical ICT third party providers?	The EMA believe that any oversight framework for ICT third party providers should focus on Critical third-party providers.

	Should "criticality" be based on a set of both qualitative and quantitative thresholds (e.g. concentration, number of customers, size, interconnectedness, substitutability, complexity, 20 etc.)?	The assessment of criticality of ICT third party providers should largely be based on a set of quantitative criteria to ensure a consistent application of the assessment process across jurisdictions and service providers.
	Should proportionality play a role in the identification of critical ICT third party providers?	Proportionality should be considered in the process of identification of Critical ICT third party providers.
	Should other related aspects (e.g. data portability, exit strategies and related market practices, fair contractual practices, environmental performance, etc.) be included in the oversight framework?	Data portability, support for credible exit strategies, and environmental performance are appropriate parameters to consider as part of an oversight framework for ICT third party providers.
	Should EU and national competent authorities responsible for the prudential or organisational supervision of financial entities carry out the oversight?	NCAs - that are currently responsible for the organizational supervision of financial service entities – could be good candidates to carry out the oversight of Critical ICT third party service providers. It is likely that NCAs will require the technical assistance of EU/national entities like ENISA or national CERTs to carry out such oversight.
	Should a collaboration mechanism be established (e.g. within colleges of supervisors where one national competent authority assumes the lead in overseeing a relevant ICT service provider to an entity under its supervision - see e.g. CRD model)?	The EMA would support the establishment of a collaboration mechanism between NCAs that end up carrying any oversight of Critical ICT third party service providers.
	Should the oversight tools be limited to nonbinding tools (e.g. recommendations, cross border cooperation via joint inspections and exchanges of information, onsite reviews, etc.)?	The oversight framework for Critical ICT third party providers should comprise a combination of binding and non-binding tools to deliver the intended regulatory outcomes while minimising industry disruption.

	Should it also include binding tools (such as sanctions or other enforcement actions)?	See comment to the sub-question above.
38	What solutions do you consider most appropriate and effective to address concentration risk among ICT third party service providers? Diversification strategies, including a potential mandatory or voluntary rotation mechanism with associated rules to ensure portability (e.g. auditing model) Mandatory multi-provider approach Should limits be set by the legislator or supervisors to tackle the excessive exposure of a financial institution to one or more ICT third party providers? Other (please specify)	The view of the EMA is that regulators should highlight the responsibility of regulated entities to monitor/manage concentration risk among third party service providers. Regulated entities should be afforded flexibility to choose the most effective risk mitigation controls to address concentration risk; such controls may comprise some of the solutions listed in the Question statement (diversification strategies, credible exit strategies, data portability). EMA members would require further guidance from regulators in identifying ICT third party providers whose use raises significant concentration risks at an industry level. Regulators are better placed in identifying such third-party providers than individual regulated entities.
39	Do you agree that the EU should have a role in supporting and promoting the voluntary exchanges of such information between financial institutions? To the extent you deem it necessary, please explain your reasoning.	The financial services industry is currently lacking widely available mechanisms/fora to exchange digital operational resilience information. The EMA would welcome the support of any national/ international organisation to establish such mechanisms.
40	Is your organisation currently part of such information-sharing arrangements?	EMA members currently receive access to digital operational resilience information through participation in a range of national/international cybersecurity information sharing networks. These comprise services like the CiSP service operated by the UK NCSC

	If you have answered yes to the question, please explain how these arrangements are organised and with which financial counterparts you exchange this information. Please specify the type of information exchanged and the frequency of exchange.	(https://www.ncsc.gov.uk/section/keep-up-to-date/cisp) to distribute cybersecurity information to financial service industry participants. We also note that recent launch of the *Cyber Information and Intelligence Sharing Initiative (CIISI-EU)* chaired by the ECB. However, EMA members are not clear on the access conditions attached to the output of this initiative by individual payment service providers. Overall, there are very few channels that financial service providers can use to exchange such information among themselves.
41	Do you see any particular challenges associated with the sharing of information on cyber threats and incidents with your peer financial institutions?	As noted in the response to Question 27 (above) the typical challenges associated with the exchange of operational resilience incident data with other financial service industry participants comprise: ▪ Data privacy concerns (emanating from GDPR and national data privacy legislation), ▪ The absence of established national/cross-border information sharing channels among industry participants, ▪ Wariness on the part of financial service providers to share incident information with other industry participants (to limit reputational damage), ▪ Surrendering competitive advantage achieved through investment in threat detection capabilities and, ▪ Contractual limitations (on onward information distribution) imposed by 3rd party suppliers of threat intelligence.

42	Do you consider you need more information sharing across different jurisdictions within the EU? To the extent you deem it necessary, please explain your reasoning and clarify which type of information is needed and why its sharing is beneficial.	The EMA view is that there is a real need for more information sharing of digital operational resilience incident data between financial service providers across EU jurisdictions to: ▪ Identify and react in a timely fashion to threat actors whose activities span multiple providers / jurisdictions. ▪ Gain a better understanding of the tactics, techniques, and procedures forming the root causes of such incidents that often impact service providers across jurisdictions, ▪ Share lessons learnt, ▪ Allow service providers to revise their security controls to address emerging operational resilience risks before such risks impact the delivery of their services, ▪ Enable the identification and adoption of best industry practices to prevent/address operational resilience events.
43	Does your organisation currently have a form of cyber insurance or risk transfer policy? If you answered yes, please specify which form of cyber insurance and whether it comes as a stand-alone cyber risk	[N/A]
44	What types of cyber insurance or risk transfer products would your organisation buy or see a need for? To the extent you deem it necessary, please specify and explain whether they should cover rather first or third-party liability or a combination of both?	[N/A]

45	Where do you see challenges in the development of an EU cyber insurance/risk transfer market, if any? Lack of a common taxonomy on cyber incidents Lack of available data on cyber incidents Lack of awareness on the importance of cyber/ICT security Difficulties in estimating pricing or risk exposures Legal uncertainties around the contractual terms and coverage Other (please specify)	The EMA perceive that the development of an efficient EU cyber-insurance market is impeded by the lack of: ▪ A common taxonomy of cybersecurity events, ▪ Accurate (and available) data on the occurrence and impact of cybersecurity events, ▪ Clarity on the liability of 3rd party service providers for cybersecurity incidents; the tools/services of such service providers are often used to initiate/execute cybersecurity attacks.
46	Should the EU provide any kind of support to develop EU or national initiatives to promote developments in this area? If so, please provide examples.	The EMA would support national/international initiatives that aim to enable the establishment of an efficient EU cyber-insurance market. An elaborated approach to the prudential recognition of cyber insurance/risk transfer as a risk mitigation control would be useful and should be considered.
47	Does your organisation fall under the scope of application of the NIS Directive (i.e. is identified as operator of essential services) as transposed in your Member State? If you answered yes to the question, please specify the requirements you are subject to, indicating the financial sector you are operating in.	A number of EMA members fall within the scope of Directive (EU) 2016/1148 (the NIS Directive) as Operators of Essential Services or Digital Service Providers. They are subject to the security control and incident notification requirements detailed in Articles 14 and 16 of the NIS Directive, respectively.
48	How would you assess the effects of the NIS Directive for your specific financial organisation? How would you assess the impact of the NIS Directive on your financial sector - taking into account the 3 specific financial sectors in its scope (credit institutions, trading venues and central clearing	The EMA view is that the impact of the application of the NIS Directive on the payments industry has been largely positive. It has raised awareness on the importance of tracking a wide range of cybersecurity-related risks and of maintaining a channel of communication with the NIS competent authority to share incident notifications. It has also

	parties), the designation of operators of essential services and the lex specialis clause?	underlined the significance of the cybersecurity controls deployed by Critical 3rd party service providers that support the ongoing delivery of regulated payment services.
49	Are you covered by more specific requirements as compared to the NIS Directive requirements and if so, do they originate from EU level financial services legislation or do they come from national law?	EMA members are required to comply with cybersecurity and operational resilience risk management requirements originating both in EU level (e.g. Directives/Regulations as well as EBA Regulatory Technical Standards, Opinions, Guidelines) and in national legislation.
50	[For financial institutions established in a Member State that has designated as NIS competent authority a national authority that is not a financial supervisor]: Did you encounter issues based on the fact that in the Member State where you are established the NIS competent authority is not the same as your own financial supervisory authority? Please provide details on your experience in the context of the application of NIS and explain any issues you may have encountered.	[N/A]
51	[For financial institutions established in a Member State that has designated as NIS competent authority a national authority that is not a financial supervisor]: How do you cooperate with the NIS competent authority in the Member State where you are established? Do you have agreements for cooperation/MoUs? Please provide details on your experience.	[N/A]

52 - 56	[For financial supervisors, designated NIS competent authorities, single points of contact]	[N/A]
57	To the extent possible and based on the information provided for in the different building blocks above (incident reporting requirements, testing framework, oversight of third party providers, information sharing, cyber insurance, NIS Directive), which possible impacts and effects (i.e. economic, social, corporate, business development perspective etc.) could you foresee, both in the short and the long term? Please provide details.	The EMA perceives that the application of the digital operational resilience management framework building blocks that are listed above can: ▪ Allow financial service providers to increase their ability to continue to deliver their services across a range of incident scenarios, ▪ Increase the confidence of service users in the reliability of the financial services ecosystem in the EU, ▪ Enable the delivery of new, innovative financial service propositions at competitive price points.
58	Which of the specific measures set out in the building blocks (as detailed above) would bring most benefit and value for your specific organisation and your financial sector? Do you also have an estimation of benefits and the one-off and/or recurring costs of these specific measures? Please provide details.	The EMA view of the regulatory measures - that are referenced in earlier questions of this Consultation document - is that the measures that would provide the most beneficial impact to the EU payments industry comprise: ▪ Streamlining the communication between industry participants and NCAs related to operational & security incidents, ▪ The establishment of a standardised exchange mechanism/channel to share operational resilience incident information between industry participants, ▪ The establishment of an oversight framework for Critical providers of ICT & security services and, ▪ Support for the establishment of a well-functioning cyber-insurance market in the EU.

59	Which of these specific measures would be completely new for your organisation and potentially require more steps/gradual approach in their implementation? Please provide details.	EMA members (payment industry participants) would require some time to review their existing outsourcing agreements with Critical ICT third-party providers to align with any additional regulatory compliance requirements related to a new oversight framework targeting the providers of such services. We support the view that the application of any such regulatory compliance requirements should include a transition period of appropriate length. The introduction of any mandatory cyber insurance cover requirements should also wait for the operation of an efficient EU cyber insurance market that offers products to smaller PSPs at reasonable prices.
60	Where exactly do you expect your company to put most efforts in order to comply with future enhanced ICT risk management measures and with increased safeguards in the digital environment? For instance, in respect to your current ICT security baseline, do you foresee a focus on investing more in upgrading technologies, introducing a corporate discipline, ensuring compliance with new provisions such as testing requirements, etc.? Please provide details.	[N/A]
61	Which administrative formalities or requirements in respect to the ICT risks are today the most burdensome, human-resource intensive or cost-inefficient from an economic perspective? And how would you suggest they should be addressed? Please provide details.	The incident reporting requirements originating from a number of regulatory frameworks (NIS Directive, the EBA Guidelines on incident reporting under PSD2) require EMA members to assign significant resource to support the related operational processes. We would advise the streamlining of these requirements to (a) avoid effort duplication by the regulated party, (b) strike a balance between notification timelines and accuracy/quality of submitted information and (c) revise the incident

		notification triggers to introduce more risk-based quantitative materiality thresholds. The task of assessing/monitoring the effectiveness of the risk management frameworks of Critical ICT third party providers for operational resilience risks is also a complex process that regulated entities have to perform. The application of an oversight framework to specific categories of Critical ICT third party providers will allow financial service providers to assess outsourcer operational resilience risk controls in a more efficient manner.
62	Do you have an estimation of the costs (immediate and subsequent) that your company incurred because of ICT incidents and in particular cyber-attacks? If yes, to the extent possible, please provide any useful information (in relative or absolute) terms that you may disclose. Please provide details.	[N/A]

Members of the EMA, as of March 2020

AAVE LIMITED
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Ceevo
Circle
Citadel Commerce UK Ltd
Coinbase
Contis
Corner Banca SA
Curve
eBay Sarl
Em@ney Plc
ePayments Systems Limited
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
Flex-e-card
Flywire
Gemini
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
Imagor SA
Intuit Inc.
Ixaris Systems Ltd
Modulr FS Europe Limited
Moneyhub Financial Technology Ltd
MuchBetter
myPOS Europe Limited
Nvayo Limited
One Money Mail Ltd
OpenPayd
Optal
Own.Solutions
Park Card Services Limited
Paybase Limited
Paydoo Payments UAB
Payoneer
PayPal Europe Ltd
Paysafe Group
PPRO Financial Ltd
PPS
QIX Ltd
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Soldo Financial Services Ireland DAC
Stripe
SumUp Limited
Syspay Ltd
Token.io
Transact Payments Limited
TransferMate Global Payments
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Valitor
Vitesse PSP Ltd
Viva Payments SA
WEX Europe UK Limited
Wirecard AG
Wirex Limited
WorldFirst
Worldpay UK Limited
WorldRemit