Consultation Response

European Commission Public Consultation on 'Digital Operational Resilience: Making the EU financial sector more secure'

19th March 2020

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on **DIGITAL OPERATIONAL RESILIENCE FRAMEWORK FOR FINANCIAL SERVICES**: **MAKING THE EU FINANCIAL SECTOR MORE SECURE.** AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia.

AFME is registered on the EU Transparency Register, registration number 65110063986-76.

We summarise below our high-level response to the consultation, which is followed by answers to the individual questions raised.

I. General comments

Executive Summary

AFME welcomes the European Commission's public consultation on '***Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure***' **(the "CP").** We believe that the focus of this CP is a positive effort to propose legislative changes that can deepen the European Single Market for digital financial services, make the European financial services sector regulatory framework more supportive of innovation, and enhance the resilience of the financial system.

AFME recognises the increasing importance of digitisation for financial services and the wider-economy, and the potential implications for cyber and Information and Communications Technology (ICT) risks. AFME supports the European Commission's view that the EU should adopt a harmonised approach on how cyber and ICT risks are managed. This will minimise the risk of diverging requirements across Member States and provide consistency and clarity of regulatory requirements; particularly for firms operating cross-border. We believe the objectives set by the Commission can be best achieved by establishing minimum legislative standards that seek to harmonise regulation for the management of cyber and ICT risks across the financial services sector.

AFME has identified the following high-level considerations for the Commission in response to this CP:

- **The subject of the CP should more clearly align to the content of the proposed legislative changes which specifically address cyber and ICT risk.**
  - The proposed legislative changes in the CP are intended to support the 2019 final Guidelines developed from the EBA on 'ICT and Security Risk Management'.
  - AFME recommends the Commission to revise the CP title wording of 'digital operational resilience'. This is to avoid confusion with other resilience initiatives (such as the 2016 BIS/CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures, the 2018 ECB Cyber Resilience Oversight Expectations for Financial Market Infrastructures, and the 2019 Bank of England Building Operational Resilience Consultation Paper).

- **The proposed legislative changes in the CP should be consistent, and not duplicate, existing regional and global principles and regulation relating to cyber and ICT risks**.
  - It is unclear how the proposed legislative changes overlap or complement existing EU standards. For example, both the EBA Guidelines on 'ICT and Security Risk Management', and the EBA Guidelines on 'Outsourcing', include requirements for managing outsourcing arrangements to third party providers. Duplicate requirements across different sets of Guidelines creates greater uncertainty and complexity for firms.
  - Further, the legislative proposals should aim to complement, and not overlap, existing regional and global guidance for cyber and ICT risk management. For example:
    - The FSB Cyber Lexicon[1];
    - The FSB 'Guidance on Arrangements to Support Operational Continuity in Resolution'[2]; or
    - The Basel Committee 'Principles for the Sound Management of Operational Risk'[3];
    - The Basel Committee 'Cyber-resilience: range of practices'[4]; and,
    - The Bank for International Settlements 'Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions'[5];
  - AFME recommends the Commission maintain consistency of any legislative proposals to existing global and Member State level definitions, papers, and guidance relating to cyber and ICT risk.
  - Further, AFME recommends the Commission take into consideration ongoing discussions at the Basel Committee for Banking Supervision (BCBS), specifically on operational resilience, which is likely to provide specific definitions and guidance in Q1 2020. This will ensure consistency with the BCBS of any legislative changes proposed, or developed, before the guidance is made public.

- **The proposed legislative changes in the CP should remain principles based and focus on minimum requirements for the management of cyber and ICT risks across the EU financial services sector**.
  - In line with global standards, principles-based legislation would provide the flexibility needed for the continuously evolving nature of cyber and technology risks and prevent prescriptive and detailed requirements being introduced that could become obsolete in the short to medium term.
  - We note several proposals in the CP that deviate from a principles and outcomes driven regulatory approach for the management of cyber and ICT risks. As such, AFME recommends the European Commission consider avoiding developing legislation in the following areas:
    - Potential specific legislation for Recovery Time Objective (RTO) and Recovery Point Objective (RPO);
    - Potential prescriptive requirements for TLPT (e.g. testing live production systems, compulsory tests, prudential impact of tests); and,
    - Potential prescriptive requirements for third party management (e.g. mandatory multi-provider approach, exposure limits set by regulators).
  - AFME recommends the proposals should focus on how firms can demonstrate capabilities and outcomes to mitigate risks, and that firms are aligned with regulatory expectations. For example, this would increase consistency and alignment with the BIS CPMI-IOSCO guidance on 'Cyber resilience for financial market infrastructures;[6], and ensure the guidelines can be implemented with proportionality in mind. A principles-based legislation would also align with the final guidance developed by the EBA in the 'Guidelines on ICT and security risk management'.

- **AFME encourages the Commission to ensure that any legislative changes in the CP can continue to support innovation in the EU and global financial services sector.**
  - AFME welcomes the specific opportunities identified in the CP which we believe will continue to support innovation. These are:
    - Harmonisation with international standards;
    - Reduction of regulatory inconsistencies and fragmentation (e.g. for instance on incident reporting);

[6] https://www.bis.org/cpmi/publ/d146.pdf (2016)

- Leveraging international cooperation where possible (e.g. sharing of TLPT test results); and,
- Focusing on making the regulatory framework efficient and standardised where possible.

- AFME recommends that any legislative changes focus on principles based minimum standards for the management of cyber and ICT risks that apply to all financial services participants and authorities.

AFME welcomes the opportunity to discuss our response to this CP and to identify opportunities to support this important initiative.

II. Comments to the sections of the public consultation

Introduction

AFME welcomes the overall objective of the European Commission to propose legislative changes to deepen the Single Market for digital financial services, make the EU financial services sector regulatory framework more innovation friendly and enhance the resilience of the financial system.

However, the title of the consultation paper ('CP'), '*Digital Operational Resilience*' should more clearly reflect the specific scope and content of the proposed legislative changes (namely cyber and ICT risk management).

'Resilience', and 'Operational Resilience', is the subject of separate guidance, such as the 2016 BIS/CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures, the 2018 ECB Cyber Resilience Oversight Expectations for Financial Market Infrastructures, and the 2019 Bank of England Building Operational Resilience Consultation Paper.

This change to the CP title would help to minimise confusion of terminology and more align the proposals with their intended purpose of reflecting the final Guidelines developed by the EBA on 'ICT and Security Risk Management'.

Further, AFME recommends the Commission take into consideration that the Basel Committee for Banking Supervision (BCBS) Operational Resilience Group (ORG) is planning to publish specific definitions and guidance on Operational Resilience in Q1 2020. We believe it will be important for the European Commission to consider, and where feasible align to, these global guidelines for any legislative proposals made.

2.1. ICT and security requirements

- ***Overarching comments***

AFME welcomes the proposal to establish harmonised requirements for cyber and ICT security risk management across the EU financial services sector. We believe that legislative proposals should focus on a principles-based approach, and minimum standards, for cyber and ICT security risk management to ensure they can be implemented with proportionality in mind, across firms of various size, complexity and location. This will increase harmonisation and reduce fragmentation.

AFME encourages the Commission to consider tools developed by the industry, such as the Financial Services Sector Cyber Security Profile (FSSCP), which is currently used by firms to compare cyber security frameworks and establish best practice.

Specific legislation proposed in the CP for Recovery Time Objective (RTO) and Recovery Point Objective (RPO) would deviate from this principle based approach and may even exacerbate the risk of a cyber incident impacting the wider-financial ecosystem (see Answer to question 18).

- ***Specific feedback on proposed legislative changes***

Supporting Information

Question	In scope/Out of scope	Response
1	AFME to respond	Yes
1.1	AFME to respond	• AFME welcomes the proposal to establish harmonised requirements for cyber and ICT security risk management across the EU financial services sector. Such a legislative proposal should focus on a principles-based approach to common minimum standards for cyber and ICT security risk

		management, to ensure they can be implemented with proportionality in mind, across firms of various size, complexity and location.
2	AFME to not respond	
2.1	AFME to respond	• Select areas covered by the FSSCP: Identification, Detection, Ability to protect, Respond, Recovery, Learning and evolving, Information sharing with other financial actors on threat intelligence, Internal coordination (within the organisation), Governance, Third party risk.
2.2	AFME to respond	• Rather than specific difficulties in the different stages of the risk management cycle, firms face difficulties reconciling between the different cyber risk management frameworks. The Financial Services Sector Cybersecurity Profile (FSSCP) from the Financial Services Sector Coordinating Council[1] is a mapping tool that has been developed to compare and reconcile the various frameworks for cyber risk management assessment in use by financial firms and demonstrate regulatory compliance. This enables firms, and potentially regulators, to detail how different subsections of each of the three Core Standards (the NIST Cybersecurity Framework, ISO, and the CPMI-IOSCO Guidance), as well as other frameworks may overlap with or be functionally equivalent to each other. [1] https://fsscc.org/Financial-Sector-Cybersecurity-Profile • See separate summary note provided on the FSSCP.
3	AFME to not respond	
3.1	AFME to not respond	
3.2	AFME to respond	• AFME recommends the Commission consider the nuances between the different functions of the management body. For instance, the executive function of the management body should have responsibility over the ICT function and strategy. However, the accountability of an Executive Board should focus on setting the firm's overall risk strategy/appetite, focusing on strategic outcomes for the firm as a whole, and the ability to challenge decisions of the ICT functions.
4	AFME to respond	• AFME recommends the Commission avoid specific reference to how the ICT risk management function should be implemented for mitigating ICT risks. Any requirements for the implementation of the ICT risk management function should be harmonised with existing regulatory requirements, be principles and risk based to focus on ensuring an effective internal risk management and control model. • AFME notes that the EBA in their final ICT GLs have revised the guidelines to not explicitly refer to how the three line of defence model should be implemented but rather describe the responsibilities of each. This is in line with a principle and risk-based regulatory framework. AFME recommends that where relevant all regulatory guidance should be consistent with this approach (e.g. EBA Guidelines on internal governance (EBA/GL/2017/11)).
5	AFME to not respond	
5.1	AFME to not respond	
5.2	AFME to respond	• Instead of specific requirements or activities firms should perform to identify and detect ICT risks, AFME recommends the Commission consider adopting a principle based regulatory framework that enables firms and regulators to remain flexible and adaptable to ICT risks.

		• A principles-based approach would provide the flexibility required for the continuously evolving nature of technology risks and avoid prescriptive and detailed requirements that may become obsolete over time. Such a framework would be consistent with a risk-based approach, whereby firms have flexibility in implementing appropriate capabilities that can meet the regulatory expectation of appropriate risk mitigation. For instance, rather than prescriptive requirements on how firms should implement ICT controls, the regulatory framework should focus on firms having an effective internal risk management and control model. • This would for example increase the consistency and alignment with the BIS CPMI-IOSCO guidance on "Cyber resilience for financial market infrastructures" and ensure any requirements can be implemented with proportionality in mind. Where more detailed guidance is provided the EC should consider separating these out as examples or use cases, to provide examples of how specific requirements could apply or be interpreted. • AFME encourages the Commission to consider tools developed by the industry, such as the FSSCP, which is currently used by firms to compare cyber security frameworks and establish best practice. See further detail provided in response to question 2.2.
6	AFME to not respond	
6.1	AFME to not respond	
7	AFME to not respond	
8	AFME to not respond	
8.1	AFME to respond	• Financial service firms are subject to various regulatory requirements on how they are expected to manage their ICT systems. These requirements subject firms to various controls and tests so that firms can gain assurance and attest that their systems can withstand and recover from operational disruptions. • Due to the evolving nature of ICT risks, AFME believes these requirements are most effective and appropriate if embedded in principles and risk-based approach, enabling firms to be flexible and prioritise investments where they are the most needed/important. In addition, such an approach reconciles with firms being able to demonstrate outcomes, such as the ability of firms to operate, minimise disruption and protect assets. • For in-house versus outsourced ICT systems and tools, financial service firms recognise their accountability and oversight of ICT systems and tools whether in-house outsourced, that includes compliance with regulatory requirements. Firms recognise that oversight of outsourced ICT providers is required, as a minimum, to the same extent as if the firm was providing the service internally. • Financial services firms use of ICT Third Party Providers, through contractual outsourcing arrangements, has been subject to regulatory and supervisory requirements for many years. We recognise there has been a significant increase in the regulatory focus on ICT Third Party Outsourcing over the last three years (such as the 2019 EBA Guidelines on Outsourcing) and we also note that there is further regulatory guidance expected in 2020 (such as further guidance from ESMA on cloud and outsourcing). These recent regulatory requirements (including contractual aspects such as access and audit rights, transition, sub-outsourcing, resilience, registers, and exit strategies) have provided additional clarity to firms and ICT Third Party Providers.

		We therefore recommend that the European Commission continues to support harmonising the EBA Guidelines on Outsourcing across Member States, which will support both firms and providers in their contracting obligations, alongside any proposals for SCCs • However, it is important to note that while some third parties may not be subject to financial services regulatory requirements, they may still meet high standards in term of security and resiliency in how they operate. A principles and risk-based approach, on how firms manage ICT risks and achieve risk mitigation outcomes, would therefore be appropriate to compare security standards across firms of various sectors. • For instance, the Bank of England in its 2019 'Future of Finance report' states 'financial services (should) embrace cloud technologies, which have matured to the point they can meet the high expectations of regulators and financial institutions. Shifting from in-house data storage and processing to cloud environments can speed up innovation, enable use of the best analytical tools, increase competition and build resilience.'
9	AFME to <u>not</u> respond	
9.1	AFME to respond	• AFME believes that public cloud adoption can drive a number of key benefits. These include greater business agility and innovation; improved overall cost management; increased operational efficiency; enhanced client experience and service offerings; and effective risk mitigation such as increased security and resilience. As such, AFME promotes a proportionate and risk-based approach for the safe and secure adoption of cloud computing that includes areas such as data security, systems resilience, contingency plans and exit strategies (taking into account the size, type and activity outsourced). • As part of firm's cloud strategy, firms are expected to meet the requirements set out by the EBA in the Outsourcing guidelines. These are only now being adopted into national regulation and the risk management benefits of compliance have yet to be fully assessed. AFME believes further time is needed to allow these changed to take effect before further regulation or legislation in this area is considered. • In addition to applicable regulatory requirements firms may wish to consider a range of various strategic considerations for their business as part of a cloud strategy.
10	AFME to <u>not</u> respond	
10.2	AFME to <u>not</u> respond	
11	AFME to <u>not</u> respond	
11.1	AFME to not respond	• Legacy systems are usually found in firms that have been in existence for a long time, like incumbent banks, and have had to upgrade their technology platform over time while maintaining critical systems live and operational. • As a result, legacy systems are often cited as a challenge for banks due to their on-going maintenance cost, potential complexity to manage and drag to innovate. • However, legacy systems have been tried and tested over multiple years by firms and offer appropriate levels of security and resilience. Legacy systems should not be viewed as high-risk per se. Rather the regulatory focus, whether with legacy or new systems, in-house or outsourced IT, should be on firm's appropriate implementation of their risk management and controls.

12	AFME to not respond	
12.1	AFME to not respond	
12.2	AFME to respond	• There are various reasons that could make a cyber or an operational incident difficult for a firm to mitigate, manage and recover from. AFME believes that this does not come down to a single identifiable factor, rather it may depend on a number of specificities related to the scenario/incident itself. Cyber incidents could be potentially more difficult for firms to manage and mitigate, compared to more traditional operational disruptions, due to the adversarial and malicious nature of the attack. In some circumstances, this could make cyber incidents more difficult to detect, lead to corrupted data or spread across the network quickly. • AFME would like to stress that when an operational incident occurs, firms need to be able to detect and respond to incidents in a time critical manner. This means being able to dedicate scarce resources where they are the most needed against a critical path to a safe recovery. Any distraction during this phase, such as excessive regulatory reporting, could jeopardise the safe recovery of firms by diverting scarce resources away to satisfy compliance driven activity.
13	AFME to not respond	
13.1	AFME to respond	• Firms implement various types and levels of encryption that are commensurate with the risk/sensitivity of the information (e.g. risk-based). As a general point, encryption is used by firms to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information.
14	AFME to not respond	
14.1	AFME to respond	• For ICT change management, firms have processes in place to introduce changes to the environment in a controlled manner. • For backups, firms have processes in place for data replication and backups integrated as part of their business continuity strategy. • Overall, AFME believes that a principles and risk-based approach for how firms manage ICT change management and data backups would provide the flexibility needed while being commensurate to the risks, as the technology and threats evolves.
15	AFME to not respond	
15.1	AFME to respond	• As part of firm's ICT and Security risk management, firms are expected to meet the requirements set out by the EBA in the ICT guidelines.
16	AFME to not respond	• AFME does not recommend imposing a sector critical standard, requiring firms to establish a specific Recovery Time Objective for their sector critical systems. Such a standard could be impractical, technically infeasible and potentially risks impacting the safety and soundness of financial stability by increasing contagion risks to the wider financial system. An average time for restoration cannot and should not be defined for serious/major cyber-attacks. In a severe cyber incident that involved data corruption, the restoration would prioritise the integrity of the data and the safe return of operation. The time required for that could vary considerably. Any requirement to restore systems by a fixed time without consideration of other factors could result in unintended consequences that worsened, rather than improved, the consequences of the incident. AFME believes a more practical and feasible approach would be to focus more broadly on

		resumption of service, measured by the entity's best efforts to ensure the ability to safely meet contractual and regulatory service obligations. • AFME recognises that the implementation of a specific/prescriptive sector critical Recovery Time Objective standard seems to be aligned with the requirements detailed in BIS BCBS "Principles for the Sound Management of Operational Risk"[7] regarding "loss data collection" (page 11). While AFME encourages alignment with international standards, we are not supportive of a prescriptive approach for Recovery Time Objective. Nonetheless, to support traceability of requirements to their source, we recommend the European Commission consider referencing this requirement to the BCBS publication, to help clarify and trace requirements to their potential source. • Further, AFME recommends the European Commission take into consideration that the Financial Stability Board (FSB) is planning to publish a public consultation on a toolkit of effective practices for cyber incident response and recovery in Q2 2020. We believe it will be important for the European Commission to align to these global guidelines for any legislative proposals made and therefore consider legislative action after global publications are finalised.
17	AFME to not respond	
17.1	AFME to respond	• As previously mentioned in response to question 16, AFME does not recommend imposing a sector critical standard, requiring firms to establish a specific Recovery Time Objective for their sector critical systems. Such a standard could be impractical, technically infeasible and potentially risks impacting the safety and soundness of financial stability by increasing contagion risks to the wider financial system
17.2		
18	AFME to respond	• AFME does not recommend imposing a sector critical standard, requiring firms to establish a specific Recovery Time Objective for their sector critical systems. Such a standard could be impractical, technically infeasible and potentially risks impacting the safety and soundness of financial stability by increasing contagion risks to the wider financial system. AFME believes a more practical and feasible approach would be to focus more broadly on resumption of service, measured by the entity's best efforts to ensure the ability to safely meet contractual and regulatory service obligations. • The implementation of a specific/prescriptive sector critical Recovery Time Objective standard seems to be aligned with requirements detailed in BIS BCBS "Principles for the Sound Management of Operational Risk"[8] regarding "loss data collection" (page 11). We recommend the European Commission consider reference to this document, as it would help clarify and trace requirements to their potential source.
19	AFME to not respond	
19.1	AFME to not respond	
19.2	AFME to respond	• As part of firms' business resiliency strategy, firms consider lessons learned from post incidents to enhance resiliency capabilities and develop business continuity programs. • In addition to lessons learned post-incidents, firms leverage voluntary information sharing platforms to prepare and respond to incidents (e.g. sharing of incidents, threats, vulnerabilities, best practices, mitigations).

[7] https://www.bis.org/publ/bcbs195.pdf
[8] https://www.bis.org/publ/bcbs195.pdf

		• AFME believes that the safety and soundness of the financial sector, including its ability to withstand and recover from cyber threats, is a common objective for the public and private sector. We welcome partnerships at national, regional and international level, that can connect multiple actors across the financial services value-chain, in sharing cyber threat related information, amongst trusted participants. For instance, this is an area in which it would be beneficial for regulators, who have the mandate to see across the system and different firms, to provide information back to firms and support their preparedness, response and recovery to oncoming cyber threats.

2.2. ICT and security incident reporting requirements

- ***Overarching comments***

AFME welcomes the European Commission's proposal to reduce the fragmentation of incident reporting requirements. There is an increasing risk of proliferation of incident reporting requirements on firms which may increase the reporting burden and divert resources from risk mitigation.

The Commission should consider how to support efficient reporting mechanisms, such as 'provide once, satisfy many', or how reporting information could be aggregated by authorities and shared with the industry to support preparedness and response. AFME recommends the Commission consider how to standardise and align the various reporting schemes already in place to increase efficiency, rather than introducing new or competing requirements,

- ***Specific feedback on proposed legislative changes***

Question	Comment	Reasoning
20	AFME to <u>not</u> respond	
20.1	AFME to respond	• Firms with operations and customers in the EU are subject to mandatory regulatory cyber incident reporting requirements: o NIS directive: major incident reporting for operators of essential services o GDPR: data breach notification o eIDAS: incident reporting for trusted services providers o PSD2: incident reporting for payment service providers o ECB SSM: incident reporting for significant institutions o Target 2: incident reporting for critical participants • This means that a single incident could trigger firms having to report to different authorities, complying with the applicable impact assessment details and thresholds, timeline, data set, and communication means. • In addition to applicable EU regulatory requirements firms could be subject to National Competent Authority reporting requirements in Members States where they have operations. • Large multinational financial institutions are present also outside Europe, having activities around the globe. In this case, it is possible that those jurisdictions could have further applicable incident reporting and data protection requirements.
21	AFME to respond	Yes
21.1	AFME to respond	• AFME agrees that there should be a comprehensive and harmonised EU-wide system of ICT and security incident reporting for financial firms. • A clear, appropriate and harmonised incident reporting framework would bring benefits to both private and public sector actors. Public sector actors would benefit from better quantitative inputs on incidents and clearer information on the potential level of impact on firms, the wider-sector and consumers during an incident. Private sector actors would benefit from being

		able to dedicate resources to incident management, rather than reporting, ensuring safe and sound recovery. • In addition, AFME believes that a comprehensive and harmonised incident reporting framework, would serve as a foundational component to increase efficiency of sector-wide coordination during an incident. Only a common and harmonised incident reporting framework, will allow incident data to be aggregated and analysed, in a time critical manner for public-private real-time collaboration between regulators, supervisors, law enforcement, financial institutions and other cross sectoral infrastructure actors. • As a concrete example to promote comprehensive and harmonised cyber incident reporting, and cooperation between public and private sector, some firms participating in the CyberSec4Europe Consortium are involved in a pilot project to deliver a smart engine addressing the need to respond to incident reporting mandatory requirements. The smart engine pilot project is supported by the European Commission's Horizon2020 Programme.
22	AFME to respond	Select all
22.1	AFME to <u>not</u> respond	
22.2	AFME to respond	• In addition to the areas identified by the European Commission, AFME recommends baselining a comprehensive harmonised incident reporting framework with a common taxonomy of incidents, based of relevant international standards. Such a taxonomy should be comprehensive, to include various operational disruptions (including cyber), but flexible in nature to evolve over time.
23	AFME to respond	• AFME believes an incident reporting framework should encompass only significant security incidents, based on common materiality thresholds to avoid firms having to report on all non-material incidents. Common materiality thresholds should be proportionate/risk-based to be flexible to risks and applicable to firms of various sizes/types. • We note firms currently complete internal impact assessments during or after an incident. Where feasible and common objectives align, between public and private sector, AFME recommends aligning incident reporting requirements to internal impact assessments. • AFME advocates for the use of a single common incident reporting template, so that firms can report an incident once rather than currently having to report a single incident to multiple EU and Member States NCA's.
24	AFME to respond	No
24.1	AFME to respond	• AFME believes an incident reporting framework should encompass only significant security incidents, based on common materiality thresholds to avoid firms having to report on all non-material incidents. Common materiality thresholds should be proportionate/risk-based to be flexible to risks and applicable to firms of various sizes/types. • A common materiality threshold would filter out non-material incidents for firms reporting which would be beneficial for both public and private sector. This would reduce the reporting burden on firms and increase data quality of incidents reported to authorities. • As previously mentioned in response to question 19.2, firms record and review lessons learned from adverse events allowing firms to prepare for future adverse events. In addition to lessons learned post-incidents, firms benefit from voluntary information sharing platforms to prepare and respond to incidents (e.g. sharing of incidents, threats, vulnerabilities, best practices, mitigations).

		• The objective of this reporting should be to inform authorities in high-risk incidents. Firms should be required to log, but not immediately report minor incidents. These can be reported to authorities at a later time in order to build evidence for policy making and to understand threat trends.
25	• AFME to respond	• AFME believes incident reporting should be completed under secure communication channels with the relevant authorities, as the information reported may contain sensitive and confidential data. • As a starting point, AFME believes firms should report an incident once rather than having to currently report a single incident to multiple EU and Member States NCA's. However, beyond the reduction of the reporting burden on firms, managing major incidents through a centralized authority could ensure that sensitive information is protected and provide a process for incident reporting, analysis and information dissemination across industries and other regulators within and outside jurisdictions. • AFME encourages the European Commission consider the development and implementation of tools that could facilitate the handling of incident reporting and the various requirements of stakeholders involved.
26	AFME to respond	Yes
26.1	AFME to respond	• Overall, AFME believes firms should report an incident once rather than having to currently report a single incident to multiple EU and Member States NCA's. Once firms report an incident, there should be a mechanism/tool in place whereby EU institutions and Member State NCA's could receive or access the reported information based on their individual needs/requirements provided appropriate governance around incidents reporting is implemented. AFME believes it is important that firms remain in control of incident reporting data and handling, to avoid undue dissemination of potentially sensitive/confidential data.
27	AFME to respond	• Firms with a global footprint engage with a broad range of regulatory authorities around the world during an incident. Liaising with multiple regulatory and law enforcement bodies requires firms to develop a significant number of individually crafted communications, showing the value of standardizing information-sharing protocols and incident reporting templates.

2.3. Digital operational resilience testing framework

- ***Overarching comments***

AFME welcomes the European Commission's proposal to develop a coherent cyber resilience testing framework across the EU financial sector, setting-up of a common set of guidance that could lead to the mutual acceptance/recognition of test results (even from other jurisdictions and the EU supervisory community).

- ***Specific feedback on proposed legislative changes***

Question	Comment	Reasoning
28	AFME to <u>not</u> respond	
28.1	AFME to <u>not</u> respond	
28.2	AFME to <u>not</u> respond	

28.3	AFME to respond	• Overall, in the EU, financial service firms are required to perform ICT and security testing requirements. Those vary in range, size in complexity but could be grouped around the following three areas: o ICT information security reviews, assessment and testing, in alignment with the EBA ICT Guidelines 'Section 3.4.6: information security reviews, assessment testing'; o Completion of IT questionnaires (e.g. ECB IT risk self-assessment questionnaires submitted by banks in 2018); o Threat Led Penetration Testing (e.g. TIBER-EU, CBEST). • It is worth noting that firms with presence in multiple jurisdictions may be subject to multiple overlapping regulatory requests at one time, from various authorities, which are aimed at the same objective but inconsistent (e.g. difference in style, language, template, timeframe). This increases resourcing constraints on firms, who driven by compliance, dedicate scarce resources to satisfy regulatory requests. We believe that coordination and harmonisation of regulatory requests for ICT and security testing would benefit firms and public sector authorities • AFME welcomes the European Commission's proposal to harmonise cyber resilience testing practices with international standards, as a mechanism that can lead to the mutual acceptance/recognition of test results, even from other jurisdictions, across the EU supervisory community. This would align with the core objectives of the G7 Cyber Expert Group, which indicated that one of the core objective of the 'G7 fundamental elements for threat led penetration testing' is to support cross-authority interaction and cross-jurisdictional TLPT for multinational entities, facilitating mutual acceptance of test results. • AFME believes firms should not be mandated to outsource testing to third party providers, rather this should be a firm led choice, to determine the best provider of such tests. Indeed, firms may have their own testing teams that are familiar with their firm's environment and able to quickly pivot to more advanced and useful testing. Firms may also rely on external testing and have already budgeted to do so. Mandating a specific/prescriptive approach may limit optimal results of testing and may place unnecessary financial burden on firms due to the scarcity and costs associated with third party providers. For instance, to ensure the independence and objectivity of a firm-led test, firms should have a formal governance structure under which to conduct the testing that includes defined testing standards and procedures, clear roles and responsibilities of the different teams involved, and rules of engagement, which may all be reviewed with the regulator. • Further, certain third party practices on testing could present risks to firms and the sector, e.g., installing untested software or hardware in production networks, and providing unfettered network access to complete tests. Consistent with firms' controls and security expectations for third parties, it should not be expected of firms to provide unrestricted, full technical tests results to unvetted third parties or regulatory stakeholders. Such information without appropriate restrictions could become a roadmap for bad actors on an institution's vulnerabilities. • Further, AFME notes that the BIS has documented a range of ICT and security testing requirements in its 2018 report on 'Cyber-resilience: Range of practices' and that the FSB will be consulting in Q1 2020 on a 'toolkit of effective practices relating to a financial institution's response to, and recovery from, a cyber incident'. AFME recommends the Commission take those initiatives into consideration for international consistency.
29	AFME to <u>not</u> respond	
29.1	AFME to <u>not</u> respond	

29.2	AFME to respond	• AFME believes firms, in the EU, should meet the requirements set out in the EBA ICT Guidelines (see answer provided above). • Rather than focus on specific elements, AFME believes that an effective ICT and security risk management framework applicable to all financial service firms, requires a flexible, risk-based approach that can adapt to the quickly evolving risks of the financial sector landscape. Such requirements should instead focus on ensuring an effective internal risk management and control model for firms.
30	AFME to not respond	
30.1	AFME to not respond	
30.2	AFME to respond	• AFME believes firms are already identified as 'significant'. • At EU-level, the European Central Bank identifies significant firms regularly, indicating which firms it directly supervises. For example, on December 4th, 2019, the ECB published a list of 119 banks in will directly supervise in 2020. • At a National level, Member States identify 'significant' firms by their National Competent Authorities. For example, the Federal Financial Supervisory Authority of Germany (BaFin) published on January 13th, 2020 a list of 13 firms qualified as systemically important institutions. • Finally, at a global level, the Financial Stability Board and Basel Committee for Banking Supervision publish regularly a list of 'Global systemically important banks. For example, on November 22nd, 2019, the Financial Stability Board published a list of 30 G-SIBs. • AFME recommends the European Commission consider not developing an additional and potentially overlapping list of 'significant' institutions which may be inconsistent with current practices.
31	AFME to not respond	
31.2	AFME to respond	• AFME believes a harmonised EU testing framework would provide benefits to both firms and supervisors. Existing frameworks should be considered to drive mutual recognition of such tests – not just within the EU but also with non-EU peers where similar frameworks are in development or already in place, e.g. CBEST in the UK. This would align with the core objectives of the G7 Cyber Expert Group, which indicate that one of the core objective of the 'G7 fundamental elements' is to supporting cross-authority interaction and cross-jurisdictional TLPT for multinational entities, facilitating mutual acceptance of test results. • TIBER-EU in particular is a strong option for harmonisation across the EU. Leveraging existing momentum and investments in TIBER's development would help stand-up a consistent testing method. • However, AFME recommends the European Commission consider embedding responsible behaviour as part of test requirements so that due consideration is given on the impact on tests on firm's resources, security and potential for disruption. For instance, testing live production systems should not be required if a firm's development and testing environments mirror that of production. Testing of all functions would also not prove beneficial, in particular for firms that shared infrastructure and consistent control framework; this would just prove duplicative and unnecessarily increase costs and testing duration. • Similarly, the use of a firm's own red team resources should be supported as this would help address concentration issues of testing experts and also reduce risk exposure stemming from external testing. AFME recommends the Commission consider firms' ability to perform test by providers (internal or

		external), as long as those tests are performed by resources having the necessary level of independence and expertise required. • Advanced testing frequency should take into account the practical steps needed to maximise benefits of test findings and improve a firm's cyber resilience capabilities. Testing once every three years would allow a firm sufficient time to plan, test, analyse findings, plan and implement remediation actions before starting a new cycle of tests. A shorter duration would work against the EC's objective of enhancing financial sector resilience. • Finally testing practices should be flexible in nature to evolve with an evolving risk landscape and best practices. Prescriptive requirements may drive firms to satisfy regulatory compliance, rather than continuously assessing its maturity and posture to build increased levels of resiliency through continuous monitoring.
32	AFME to not respond	
32.1	AFME to respond	• Testing scheduling and frequency should be agreed with firms so that practical steps are taken to maximise benefits of test findings and improve a firm's cyber resilience capabilities. As an illustration, testing once every three years may not allow a firm to allocate sufficient time and resources to plan, test, analyse findings, plan and implement remediation actions before starting a new cycle of tests.
33	AFME to not respond	
33.1	AFME to not respond	
33.2	AFME to respond	• As a general rule, AFME understands that the prudential treatment of ICT and security requirements would mean developing rules requiring financial firms to hold sufficient capital and have adequate risk controls in place. • However, AFME believes that, in line with international standards, principles-based legislation would provide the flexibility needed for the continuously evolving nature of cyber and technology risks and prevent prescriptive and detailed requirements being introduced that will become obsolete over time. Developing prescriptive controls or requesting firms to hold specific capital requirements, may drive firms' resources satisfying regulatory compliance, rather than continuously assessing their maturity and posture to build increased levels of resiliency.

2.4. Addressing third party risk: oversight of third party providers (including outsourcing)

- ***Overarching comments***

AFME cautions any immediate introduction of additional mandatory requirements on how financial service firms manage and oversee outsourcing to Third Party ICT Providers. Outsourcing to ICT Third Party Providers has been used by financial services firms for many years, and firms recognise their accountability and oversight of ICT third party providers, including compliance with regulatory requirements.

Whilst we welcome the focus on this important topic by the European Commission, we believe that a detailed assessment is needed, coordinated at the global level, for the possible introduction of any frameworks to oversee ICT Third Party Providers and concentration risk. This is to prevent any conflict, complexity or restrictions this could create for innovation, competition and individual firm's ability to use existing and future third parties. This is also needed to prevent increased regulatory fragmentation, and potential greater data localisation, for cross-border firms and ICT third party providers.

- ***Specific feedback on proposed legislative changes***

Question	Comment	Reasoning

34	AFME to not respond	
35	AFME to not respond	
35.1	AFME to respond	• Financial services firms use of ICT Third Party Providers, through contractual outsourcing arrangements, has been subject to regulatory and supervisory requirements for many years. Firms have mature governance and compliance procedures to ensure that applicable regulatory and supervisory requirements are addressed when outsourcing to an ICT Third Party Provider. • Due to the high level of regulation for financial services, and firms' internal procedures (such as legal, compliance, and reporting), contractual negotiations are important so that all requirements (including regulatory) are met. • ICT Third Party Providers must demonstrate, and meet, compliance to regulatory and supervisory requirements required by firms for outsourcing of a service to take place.
36	AFME to respond	• AFME believes that any possible development of Standard Contractual Clauses (SCCs) between financial firms and ITC Third Party Providers should be voluntary, principles-based, and seek to harmonise existing mandatory outsourcing requirements that are required by the broadest range of firms. • We recognise that there is currently a lack of contractual and technical standardisation between ICT Third Party Providers which provide similar service offerings. This can often make contractual negotiation burdensome with a provider, and complex where a firm wishes to use multiple providers (such as in a hybrid service model). • However, introducing SCCs between firms and ICT Third Party Providers should not create additional regulatory and operational complexity for firms (such as the need for extensive renegotiation of current contracts, changes to existing outsourcing services, or increases in the costs of services). SCCs should also ensure that a level playfield field for ICT Third Party Providers is not restricted (e.g. reduced competition in the market), or restrictions are placed on firms to manage their outsourcing arrangements in a risk and principles-based approach. • There has been a significant increase in the regulatory focus on ICT Third Party Outsourcing over the last three years (such as the 2019 EBA Guidelines on Outsourcing) and we also note that there is further regulatory guidance expected in 2020 (such as further guidance from ESMA on cloud and outsourcing). • These recent regulatory requirements (including contractual aspects such as access and audit rights, transition, sub-outsourcing, resilience, registers, and exit strategies) have provided additional clarity to firms and ICT Third Party Providers. • We therefore recommend that the European Commission continues to support harmonising the EBA Guidelines on Outsourcing across Member States, which will support both firms and providers in their contracting obligations, alongside any proposals for SCCs
37	AFME not to respond	
37.1	AFME to respond	• AFME believes that further assessment is required for the possible introduction of any oversight framework for ICT Third Party Providers. This is to prevent introducing any conflict, complexity or restrictions for innovation, competition and the ability of firms to use existing and future ICT Third Party Providers. Effective third party and ICT and security risk

		management require a flexible, risk-based approach to adapt to changes in the financial services industry and advances in technology. • Firms recognise their accountability and oversight of ICT Third Party providers that includes compliance with regulatory requirements. Firms recognise that oversight of ICT Third Party Providers is required, as a minimum, to the same extent as if the firm was providing the service internally (e.g. the performance of risk assessments – including of concentration risk, due diligence, contracts and service agreements, and reporting). • An oversight framework for ICT Third Party Providers should be coordinated globally due to the interconnected nature of financial services and service providers. This will prevent a fragmented approach evolving in the EU which may impact a firm's ability to engage ICT Third Party Providers and/or encourage further data localisation within financial markets (e.g. restrictions on the use of cloud services outside of Europe). • We recommend that a further detailed assessment on the possible introduction of any oversight framework for ITC Third Party Providers is conducted by the European Commission with industry involvement and is coordinated at the global level.
38	AFME not to respond	
38.1	AFME to respond	• Firms already perform their own risk assessments of concentration to ICT Third Party Providers to determine criticality of outsourcing arrangements. Based on these assessments, firms may take action to address concentration risks if necessary, in a risk-based approach. Examples could include: • Using multiple providers for certain services (e.g. using two or more regional or global Cloud providers for substitutability or distributing workloads); or • Adopting hybrid service models to (e.g. using on-premise hosting, public and/or private Cloud capabilities, for critical activities or for business continuity purposes).
38.2	AFME to respond	• AFME believes that the proposed solutions on financial services firms to address concentration risk (e.g. multi-provider, exposure limits, rotation mechanisms) would potentially impact the ability for a firm to manage its oversight obligations, continuously enhance its resilience capabilities, adapt to emerging business models and technologies, and make commercial decisions (e.g. for which services a multi-provider cloud approach is appropriate). • Whilst we support competition and increased portability and interoperability between ICT Third Party Providers, we note that variations of the solutions proposed are already adopted by firms today in a risk-based approach (for example, in consideration of specific ICT providers, the services being outsourced, and their importance/criticality). • Mandating solutions on firms via some, or all ICT Third Party Providers, will increase the burden and complexity of managing existing outsourcing arrangements and services. • We recommend that a further detailed assessment on the possible introduction of any oversight framework for ITC Third Party Providers is conducted by the European Commission with industry involvement and is coordinated at the global level.

2.5. Other areas where EU action may be needed

- ***Overarching comments***

AFME is supportive of timely and effective information sharing across the EU financial services sector. AFME believes this can be achieved through the implementation of the NIS Directive. The setting up of a cooperation group, in order to support and facilitate strategic cooperation and exchange of information among Member States, would be welcomed. However, it is also important to simplify and reduce constraints on sharing personally identifiable information (PII), in particular those related to "grey-areas" (e.g. as an IP address is considered PII, even metadata related to fraudulent account takeovers cannot be shared).

Question	Comment	Reasoning
39	AFME to not respond	
39.1	AFME to respond	• AFME welcomes tools and mechanisms to facilitate information sharing across the financial sector. Theses forums enable firms to prepare, respond and recover from incidents, based on voluntary sharing of non-sensitive or confidential data, between trusted parties. • AFME cautions the European Commission in creating additional mandatory requirements, geared towards information sharing, which may limit the qualitative input of these trusted networks. Rather, the Commission could build awareness to a broader set of firms, across the EU, to use the current existing mechanisms and tools available for information sharing.
40	AFME to not respond	
40.1	AFME to respond	See answer provided in response to question 39.1
41	AFME to not respond	
41.1	AFME to respond	• AFME recommends the European Commission consider that the sharing of cyber threats and incidents could present challenges for firms due to the confidential/sensitive nature of the data. The benefits of information sharing could be significantly reduced if firms were too be scrutinised on the basis of the information shared. We believe that information sharing benefiting the financial sector, prepare, respond and recover from incidents, should be based on voluntary sharing of non-sensitive or confidential data, between trusted parties.
42	AFME to not respond	
42.1	AFME to respond	• AFME believes the financial sector currently leverages and has available a set tools and mechanisms in place for information sharing. The European Commission could build awareness to a broader set of firms, across the EU, to use the current existing mechanisms and tools available for information sharing. • We believe that the safety and soundness of the financial sector, including its ability to withstand and recover from cyber threats, is a common objective for the public and private sector. We welcome partnerships at national, regional and international level, that can connect multiple actors across the financial services value-chain, in sharing cyber threat related information, amongst trusted participants. For instance, this is an area in which it would be beneficial for regulators, who have the mandate to see across the system and different firms, to provide information back to firms and support their preparedness, response and recovery to oncoming cyber threats.
43	AFME to not respond	
43.1	AFME to respond	• AFME is aware that some firms, as part of their overall cyber resilience strategy, have in place cyber insurance programs. These voluntary insurance programs are in no means expected to replace existing firm capabilities to respond and recover from cyber incidents. Indeed, cyber incidents are extremely difficult to

		assess and quantify: how would a firm quantify the potential reputational damage of a cyber incident? Rather insurance programs are an additional capability firms can leverage to support the response and recovery from cyber incidents. • AFME supports a mature and developed insurance market that could support firms with additional capabilities to respond and recover from cyber incidents, but cautions the European Commission against developing mandatory requirements for cyber insurance programs.
44	AFME to not respond	
45	AFME to not respond	
45.1	AFME to not respond	
45.2	AFME to not respond	
46	AFME to not respond	
46.1	AFME to not respond	
46.2	AFME to not respond	

2.6. Interaction with the NIS directive

- ***Specific feedback on proposed legislative changes***

Question	Comment	Reasoning
47	AFME to not respond	
47.1	AFME to not respond	
47.2	AFME to not respond	
48	AFME to respond	• AFME believes the NIS directive has contributed to the creation a common baseline cyber security strategy across the EU, in particular by raising the level of cyber preparedness and maturity for those countries where capabilities where still immature. Capabilities Members States have developed under the NIS directive have allowed to create a common frame for Operators of Essential Services, to respond and recover from cyber incidents. For example, the setting up of a cooperation group, in order to support and facilitate strategic cooperation and exchange of information among Member States. • AFME acknowledges the various and potentially inconsistent implementations of the NIS directive across Member States. However, AFME believes the European Commission should not focus efforts on ensuring precise and detailed consistency in implementation, rather that the EU can effectively respond to large scale cyber threats, by leveraging existing capabilities. Efforts should then be emphasized on gaps or weaknesses identified.
49	AME to not respond	
50	AFME to not respond	
51	AFME to not respond	

52	N/A	Question dedicated to NIS competent authority: Out of scope
53	N/A	Question dedicated to NIS competent authority: Out of scope
54	N/A	Question dedicated to NIS competent authority: Out of scope
54.1	N/A	Question dedicated to NIS competent authority: Out of scope
54.2	N/A	Question dedicated to NIS competent authority: Out of scope
55	N/A	Question dedicated to NIS competent authority: Out of scope
55.1	N/A	Question dedicated to NIS competent authority: Out of scope
55.2	N/A	Question dedicated to NIS competent authority: Out of scope
56	N/A	Question dedicated to NIS competent authority: Out of scope

3. Potential impacts

- ***Specific feedback on proposed legislative changes***

Question	Comment	Reasoning
57	AFME to respond	• Overall, AFME believes the EU (e.g. it's firms, consumers and public sector actors) has an opportunity to significantly benefit from the proposal presented if the European Commission focuses efforts on: o Legislative changes that are consistent, and not duplicate, of pre-existing global and regional principles and regulations relating to cyber and ICT risks; o Remains principles based and focused on minimum requirements for the management of cyber and ICT risks across the EU financial services sector; o Ensures that any legislative changes continue to support innovation in the EU and global financial services sector. • However, there is a risk that further fragmentation or an inappropriate regulatory framework emerges, if the Commission takes an approach that introduces: o Specific legislation for RTO and RPO; o Prescriptive requirements for TLPT (e.g. testing live production systems, compulsory tests, prudential impact of tests); and o Prescriptive requirements for third party management (e.g. mandatory multi-provider approach, exposure limits set by regulators).
58	AFME to respond	• AFME has identified the following areas where it believes the most benefits could be achieved: o Harmonisation with international standards; o Reduction of regulatory inconsistencies and fragmentation (e.g. for instance on incident reporting); o Leveraging international cooperation where possible (e.g. sharing of TLPT test results); and o Focusing on reducing regulatory fragmentation by making the regulatory framework efficient and standardised where possible.
59	AFME to respond	• AFME believes the following areas would be the most problematic for firms: o Specific legislation for RTO and RPO; o Prescriptive requirements for TLPT (e.g. testing live production systems, compulsory tests, prudential impact of tests); and

		○ Prescriptive requirements for third party management (e.g. mandatory multi-provider approach, exposure limits set by regulators).
60	AFME to not respond	
61	AFME to respond	See answers provided in response to question 57
62	AFME to not respond	
62.1	AFME to not respond	
62.2	AFME to not respond	

Contacts

AFME	Andrew Harvey	+44(0)20 3828 2694	aharvey@gfma.org
AFME	David Ostojitsch	+44 (0)20 3828 2761	david.ostojitsch@afme.eu
AFME	Emmanuel Le Marois	+44 (0)20 3828 2761	emmanuel.lemarois@afme.eu
AFME	Madeline Taylor	+44 (0)20 3828 2688	madeline.taylor@afme.eu

About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. AFME represent the leading global and European banks and other significant capital market players. AFME advocates for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society. AFME aims to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work. For more information, visit https://www.afme.eu/