European Banking Authority Consultation Paper on "EBA Draft Guidelines on ICT and Security Risk Management"

13th March, 2018

LONDON – The Association for Financial Markets in Europe (AFME) welcomes the European Banking Authority (EBA) Consultation Paper on "EBA Draft Guidelines on ICT and Security Risk Management".

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to respond to the EBA's consultation paper on its Draft Guidelines on ICT and Security Management (referred to hereafter as "the Guidelines" or "GLs") to support the financial services industry in developing a harmonised approach to supervisory assessment, and expectations, for the management of ICT risks across the EU.

AFME welcome the initiative to provide the following comments in response to questions posed by the EBA in its **Consultation Paper on "EBA Draft Guidelines on ICT and Security Risk Management"**.

I. General comments

Executive Summary

AFME welcomes the draft Guidelines (GLs) on "EBA Draft Guidelines on ICT and Security Risk Management" in an effort to harmonise supervisory assessment and expectations for the management of ICT risks across the EU. AFME recognises the increasing importance of digitisation for financial services and the wider-economy, and the potential implications for technology risk and resilience. However, individual jurisdictions should aim to adopt harmonised approaches on how ICT risks are managed to minimise diverging regulatory requirements for firms operating cross-border.

AFME has identified the following high-level considerations for the EBA in response to this consultation:

- **The guidelines should provide further clarity on the timeline and expectations of Member State National Competent Authorities (NCAs) implementation and intended use for supervision**. The timeline for implementation is unclear once the GLS are finalised. It will be key for Member State NCA implementation to be consistent and clear to discourage information gathering exercises via ICT questionnaires, which may become burdensome for firms to complete if not standardised or coordinated.

- **The guidelines should be consistent with pre-existing principles and regulation relating to ICT Risk Management**. AFME recommends the GLs make the link to internationally recognised and Member State level definitions, papers, and guidance relating to ICT resilience. Without explicit reference or a gap analysis, it is currently not clear how the guidelines overlap or complement existing standards in place.
  For example, these could include:
  - The FSB Cyber Lexicon[1];
  - The Basel Committee "Principles for the Sound Management of Operational Risk"[2];
  - The FSB's "Guidance on Arrangements to Support Operational Continuity in Resolution[3]; or
  - The EBA's "Guidelines on Outsourcing"[4].

[1] http://www.fsb.org/wp-content/uploads/P121118-1.pdf (2018)
[2] https://www.bis.org/publ/bcbs195.pdf (2011)
[3] http://www.fsb.org/wp-content/uploads/Guidance-on-Arrangements-to-Support-Operational-Continuity-in-Resolution1.pdf (2016)
[4] https://eba.europa.eu/-/eba-consults-on-guidelines-on-outsourcing (2018)

- Specifically, in relation to the recent EBA Guidelines on Outsourcing, the current guidance for managing ICT risks in relation to outsourcing arrangements to third party providers could be included in two documents. Addressing requirements across two different sets of guidelines could create greater uncertainty on applicable requirements or lead to differences in interpretation between Member State NCAs as each document is translated and implemented.

- **The guidelines should remain principles based**. A principles-based guidance 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. Rather, the EBA should focus on how firms can demonstrate capabilities or outcomes in alignment of supervisory expectation. This would for example increase the consistency and alignment with the BIS CPMI-IOSCO guidance on "Cyber resilience for financial market infrastructures"[5], and ensure the guidelines can be implemented with proportionality in mind. Where more detailed guidance is provided the EBA should consider separating these out as examples or use cases, such as how the three line of defence could be implemented, to provide examples of how the requirements could apply or be interpreted.

- **The guidelines should avoid reference to how the three line of defence should be implemented**. AFME request that the GLs avoid direct reference to how a three line of defence model should be implemented for mitigating ICT risks. The GLs specify that where the three line of defence model is applied the internal control function should take responsibility for the management of ICT risks. This may not be technically applicable to firms existing structures or could result in an outcome where ICT risks are managed differently than other types of risks. The GL requirements should instead focus on ensuring and demonstrating an effective internal risk management and control model.

- **The guidelines should remain focused on minimum standards for ICT and Security Risk Management**. The EBA should consider identifying and removing requirements in the GLs that relate areas that are not directly related to technology resilience, such as references to business continuity management. This would ensure that the guidelines are focused on ICT risks and avoid inconsistent or duplicative requirements.

AFME would welcome the opportunity to discuss our response to this consultation and identify opportunities to support this initiative.

II. Comments to the consultation paper sections

Executive Summary & Background and Rationale (pages 1 - 10)

AFME welcomes the purpose of the EBA GLs in establishing a harmonised EU risk management framework and supervisory practices for ICT and security. However, the GLs should focus on principles based and common minimum standards for ICT and Security Risk Management, rather than prescriptive requirements.

Compliance and reporting obligations (page 11)

AFME welcomes the purpose in establishing harmonised requirements for ICT and security, across Payment Service Providers (PSP's) and Credit Institutions. However, the GLs should focus on principles based and common minimum standards for ICT and Security Risk Management to ensure they can be implemented with proportionality in mind.

Subject matter, scope and definitions (pages 12 - 14)

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

AFME welcomes that the GLs address ICT risks in line with the increased importance and growing use and reliance on technology. We recommend additional references are added to international publications on technology and cybersecurity risks, such as the FSB Cyber Lexicon, where relevant.

Supporting Information

Section	Comment	Reasoning
N/A	General comment: • Amendment	• § 10 (p13) "Operational or security incident" Based on the broad scope of the definition provided we recommend the term to cover "Incident" rather than "Operational or security incident ".
N/A	General comment: • Amendment	• § 10 (p14) "ICT projects" We recommend the definition consider reference to ICT projects "end of life" or "removal" as part of wider ICT or business transformation programmes.
N/A	General comment: • Clarification	• § 10 (p14) "ICT asset" We recommend the EBA consider reference to the FSB Cyber Lexicon (e.g. "Asset") where the definition here has been extrapolated. This would help clarify and trace key terms used to their potential source.

4.1. Proportionality (page 15)

AFME recommends the GLs remain principles based. A principles-based guidance would provide the flexibility required for a proportionate implementation. Currently the guidelines contain some detailed guidance, such as relating to the three line of defence model, which may not be applicable to all Payment Service Users or Credit Institutions. We recommend where detailed guidance is provided the EBA consider separating these out as examples or use cases, providing examples of how the requirements could apply or interpret.

4.2. ICT Governance and strategy (page 15)

With regards to the management body responsibilities, AFME recommends the EBA 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 risk strategy/appetite, and the ability to challenge decisions of the ICT functions. We recommend that Executive Board responsibilities be amended in the GLs (in paragraph 55) to permit delegation where deemed adequate, for instance where it is expected from the management body to implement processes. The need for the management body to approve specific risk type policies should also be reconsidered.

Further, AFME recommends the EBA to consider the recommendations provided in response the EBA Outsourcing guidelines[6].

Section	Comment	Reasoning
4.2.3	General comment: • Clarification	• § 7, 8, 9 (p16) "Without prejudice to … and performance targets" Currently, the EBA requirements for the management of ICT risks in relation to outsourcing arrangement to third party providers, could be included in two documents; these GLs and the recent EBA Outsourcing GLs. Catering for requirements across two different sets of GLs could create uncertainty on

[6] https://www.afme.eu/globalassets/downloads/consultation-responses/afme-prd-eba-draft-outsourcing-guidelines.pdf

		applicable requirements. It could also lead to differences in interpretation between MS NCAs as each document is translated and implemented.

4.3. ICT Risk Management Framework (pages 16 - 19)

AFME recommends guidelines avoid reference to how the three line of defence should be implemented for mitigating ICT risks. The EBA guidelines specify that where the three line of defence model is applicable, the internal control function should take responsibility for the management of ICT risks. This may not be technically applicable to all firm structures and result in ICT risks being managed differently than other types of risks. The requirements should instead focus on ensuring an effective internal risk management and control model.

AFME fully appreciates the need for firms to document key processes for ICT risks assessment and mitigation, and map business functions, roles, processes and information assets supporting critical business functions, classified by criticality. However, the way firms decide to complete this mapping may vary. AFME recommends the EBA remain principles based in how firms decide to document and map these dependencies and criticalities to avoid this activity increasing resource requirements and becoming compliance driven.

It would also be helpful to provide additional background on a firm's expectations to report ICT critical mapping documents to regulatory or supervisory stakeholders that may wish to use this information.

We recommend that mapping documents be updated as relevant changes occur rather, or at least every 3 years, rather than on an annual basis.

Supporting Information

Section	Comment	Reasoning
4.3.1.	General comment: • Amendment	• § 11 (p16) "Where the three lines of defence model … and second lines of defence (see section 4.3.6)" Reference to the three line of defence in this paragraph is prescriptive. We recommend the EBA remain principles based in their approach and explicitly specify, where an example is provided, on how the three line of defence could be implemented. Further, the guidance states the second line (or "internal control function") is "expected to take responsibility for the management of ICT risks" instead we recommend: "This internal control function should take responsibility for *oversight and challenge of* ICT risks".
4.3.2.	General comment: • Clarification	• § 16 & 17 (p17) "Financial institutions … business functions and processes" Reference to the mapping of critical business functions and supporting roles, processes, information assets appears highly aligned with the overall approach currently taken by the UK authorities, and potentially the Basel Committee, on Operational resilience. We recommend the EBA consider reference to Operational resilience to avoid potential inconsistencies or divergent approaches are developed. In addition, the mapping requirements, in the EBA's current drafting. seem to indicate that it would be expected of firms to complete a mapping of all functions, across all jurisdictions and legal entities. We recommend the EBA clarify the scope and expectation of firms to ensure this is realistically completed, in line with business criticality and firms' risk appetite. Further, the paragraph references "third parties". It is not clear if the requirements here are in addition to the EBA's draft "Outsourcing Guidelines" requirements, in particular relating to inter-group arrangements or fourth parties.

4.3.3.	General comment: • Clarification	• § 21 (p18) "Financial institutions … update the current risk assessment of financial institutions." Reference to the identification of ICT risks (e.g. "risk assessment") appears highly aligned with the overall approach currently taken by the UK authorities, and potentially the Basel Committee, on Operational resilience. We recommend the EBA consider reference to Operational resilience to avoid potential inconsistencies or divergent approaches are developed. Further, the identification of ICT risks (e.g. "risk assessment"), in the EBA's current drafting, seem to indicate that it would be expected of firms to complete a risk assessment of all activities, in addition to what is already performed, rather than focusing on what is critical and significant from an operational resilience perspective. We recommend the EBA clarify the scope and expectation of firms to ensure this is realistically completed, in line with current practices, business criticality and firms' risk appetite.

4.4. Information security (pages 19 - 23)

AFME recommends the GLs avoid reference to how the three line of defence should be implemented for mitigating ICT risks. The GLs specify that firms should establish an independent information security function (2nd line) segregated from ICT operations processes, separate from audit, and reporting directly to the management body. This may not be technically applicable to all firm structures and result in ICT risks being managed differently from other types of risks. The requirements should instead focus on ensuring an effective internal risk management and control model.

We recommend that security reviews, assessments and testing are performed as relevant, rather than on an annual basis, depending on system criticality.

Supporting Information

Section	Comment	Reasoning
4.4.1.	General comment: • Clarification	• § 30 (p19) "The information security policy should…and should apply to all employees." We recommend the Guidelines not make demand of financial service firms to communicate internal information security policies with third parties.
4.4.2.	General comment: • Amendment	• § 32 (p19) "Financial institutions should establish … to the management body." Reference to the three line of defence in this paragraph is prescriptive. We recommend the EBA remain principles based in their approach and explicitly specify, where an example is provided, on how the three line of defence could be implemented. Further, the guidance states the management body is "expected to take responsibility for the management of ICT risks" instead we recommend: "This internal control function should take responsibility for *oversight and challenge of* ICT risks".
4.4.5.	General comment: • Amendment	• § 39.c (p21) "network segmentation, data leakage prevention systems or the encryption of network traffic should be implemented" The implementation of this requirement, in the EBA's current drafting, seems to indicate that it would be expected of firms to complete this blanket control across all activities. We recommend the EBA clarify the scope and expectation of firms,

		and that it would be performed on a risk-based approach, to ensure it is realistically completed, in line with best practices.
4.4.5.	General comment: • Amendment	• § 39.f (p22) "encryption of data at rest and in transit." Similarly, to point 39.c above, the implementation of this requirement, in the EBA's current drafting, seems to indicate that it would be expected of firms to complete this blanket control across all activities. We recommend the EBA clarify the scope and expectation of firms, and that it would be performed on a risk-based approach, to ensure it is realistically completed, in line with best practices.
4.4.7.	General comment: • Clarification	• § 46 (p23) "The information security testing … and systems." Currently the text references "test carried out by independent testers". AFME recommends the EBA consider firms' ability to perform test by internal or external providers, as long as those tests are performed by resources having the necessary level of independence and expertise required.
4.4.7.	General comment: • Clarification	• § 49 (p23) "Financial institutions should … but at least every three years." Reference to "all critical ICT systems" and "non-critical systems", does not currently indicate how criticality would be determined. This is particularly complex when balancing national versus regional considerations. We recommend the EBA consider clarifying that the expectation would be for firms to demonstrate having adequate processes for determining criticality and an appropriate process for action on this basis. This would
4.4.7.	General comment: • Clarification	• § 44 - 51 (p22-23) "Financial institutions … and known potential attacks." Currently financial services firms complete a range of activity to assess and mitigate operational and ICT risk, such as Operational Risk Control Self-Assessment (RCSA). We recommend the EBA consider activities, regulatory requirements or best practices in use by the industry. that could align with the requirements as set in the EBA GLs.

4.5. ICT Operations management (pages 24 - 25)

AFME appreciates the need for firms to manage ICT operations based on documented and approved procedures and maintain an up-to-date ICT asset inventory. However, the way firms decide to complete this documentation and maintain an ICT asset inventory may vary. AFME recommends the EBA to remain principles based in how firms decide to document and maintain an ICT asset inventory to avoid this activity increasing resource requirements and becoming compliance driven.

We also believe it would be helpful to provide more background on a firm's expectations to report ICT documentation or asset inventory to regulatory or supervisory stakeholders.

We recommend that mapping documents be updated as relevant changes occur or at least every 3 years, rather than on an annual basis.

While AFME recognizes the broad benefits of automation to increase firm's operational efficiency, as indicated in our April 2018 briefing note "Artificial Intelligence: Adoption in Wholesale Capital Markets" (here), there are a number of potential risks associated with the use of automation.

Firms will need to establish high standards of risk management with key control principles around governance; education and awareness; standards and development methods; data quality and assurance; and operational control. Further, firms may achieve operational efficiency through other means than automation. Therefore, we recommend the EBA remain principle based in how firm decide to increase ICT operational efficiency and remove reference to the automation of ICT operations.

AFME recognizes the benefits of ICT operations capacity monitoring and performance management which should enable better detection, analysis and correction of errors and response to performance issues in a timely manner. However, the implementation of such programs for financial service firms operating globally is often costly, complex and may not deliver immediately the benefits expected. For example, the logging and monitoring of procedures for critical ICT operations may not increase operational efficiency if not implemented appropriately. We recommend the EBA remain principle based in how firm decide to increase ICT operational efficiency and remove reference to prescriptive requirements on how firms achieve this outcome.

AFME recognizes the benefits of ICT systems and data backups and restoration procedures to ensure firms can recover as required and that those procedures should be aligned with business needs, such as business recovery requirements or the criticality of the data and ICT systems. However, we recommend EBA remain principle based in how firms decide to implement data and ICT systems backups and restoration procedures and remove prescriptive requirements on how firms achieve this outcome, as further considerations may be required (e.g. impact tolerance levels, firms risk appetite).

Supporting Information

Section	Comment	Reasoning
4.5.	General comment: • Clarification	• § 58 & 59 (p24) "Financial institutions should… including cyber-attacks." Similarly, to the points indicated above, it is currently not clear the extent to which firms have to document interdependencies.

4.5.1. ICT Incident and problem management (page 25)

AFME welcomes the principles-based guidance from the EBA on resumption of service in the event of a disruption. We recommend the EBA consider separating out the list of activities firms should consider in their incident and problem management as examples of how the requirements could apply or interpret (see paragraph 65).

Indeed, AFME views imposing a sector critical standard, requiring entities to establish a specific Recovery Time Objective for their sector critical systems, as impractical, technically infeasible and potentially a risk to financial stability and contagion risk. A more practical and feasible approach which focuses 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.

Supporting Information

Section	Comment	Reasoning
4.5.1.	General comment: • Clarification	• § 64 & 65 (p25) "Financial should establish … with the applicable regulation." The implementation of this requirement seems to align with the requirements detailed in BIS BCBS "Principles for the Sound Management of Operational Risk"[7] regarding "loss data collection" (page 11). We recommend the EBA consider reference to this document, as it would help clarify and trace requirements to their potential source.

4.6. ICT Project and Change Management (pages 26 - 28)

AFME acknowledges the importance of ICT project management and promoting adequate standards to ensure the safe and secure implementation or change of ICT systems. However, we recommend EBA remain principles-based in on how firms implement adequate standards for ICT project and change management, and rather focus on firms being able to demonstrate adequate capabilities and outcomes.

Supporting Information

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

Section	Comment	Reasoning
4.6.	General comment: • Clarification	• § 66 - 82 (p26-28) "Financial institutions … documented and authorised." The implementation of this requirement, in the EBA's current drafting, seems to indicate that it would be expected of firms to complete this blanket control across all activities regardless of criticality. We recommend the EBA clarify the scope and expectation of firms, and that it would be performed on a risk-based approach, to ensure it is realistically completed, in line with best practices.
4.6.3.	General comment: • Amendment	• § 81.c (p28) "testing and independent… to production environment" The implementation of this requirement seems to align with the requirements detailed in BIS BCBS "Principles for the Sound Management of Operational Risk"[8] regarding "Principle 7: Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk." (page 6). We recommend the EBA consider reference to this document, as it would help clarify and trace requirements to their potential source.

4.7. Business continuity Management (pages 28 - 30)

AFME acknowledges the importance of aligning ICT systems and services with areas relevant to firms' business resilience (e.g. Business Impact Analysis (BIA), Business Continuity Planning (BCP), Response and Recovery Plans, Testing of plans, Crisis communication).

AFME welcomes a risk-based approach for business continuity management of ICT systems and services and encourages the EBA to consider alignment, where relevant, with key concepts developed by the UK authorities in their proposed approach to operational resilience (here). AFME acknowledges the specific considerations identified by the EBA to ensure plans are available to the business, encompass coordination with relevant internal and external stakeholders and cover critical third-party providers.

However, AFME recommends the EBA:

- Consider removing reference to prescriptive activities expected from the management body, such as "the documentation and approval of business continuity plans" or the "analysis, address and reporting of test result deficiencies". As previously stated in response to point 5. the need for the management body to approve specific risk type policies should be reconsidered.
- Remain principles-based for considerations to resumption of service in the event of a disruption. AFME views imposing a sector critical standard, requiring entities to establish a specific Recovery Time Objective (RTO) or Recovery Point Objective (RPO) for their sector critical systems, as impractical, technically infeasible and potentially a risk to financial stability and contagion risk. A more practical and feasible approach which focuses 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.
- Consider aligning terms and concepts related to operational resilience (e.g. "adequate set of severe but plausible testing scenarios", "demonstrate ability to sustain the viability of the business until critical operations are re-established") with terminology proposed by the UK authorities in their approach to operational resilience.
- Consider reviewing the expectation of annual testing of critical business functions, to as relevant changes occur or at least every 3 years, rather than on an annual basis. Further AFME recommends the EBA consider how mutual recognition of tests could be achieved in order to satisfy cross-jurisdictional requirements where firms operate across jurisdictions.
- Consider reviewing the expectation of annual updates of BCPs, to as relevant changes occur or at least every 3 years, rather than on an annual basis.

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

Finally, AFME recommends the EBA further consider the impact on firms operating across multiple jurisdictions in having to comply with multiple requirements or reporting obligations. There is an increasing risk of the proliferation of incident reporting requirements on firms, which may increase the reporting burden on firms, as well as divert resources from actual risk mitigation.

The EBA 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 industry to support preparedness and response. AFME is supportive of an effective and coordinated incident response plan that would support the industry in the event of a large-scale disruption, which may require input and testing with the public sector's response (e.g. EU blue-print).

Supporting Information

Section	Comment	Reasoning
4.7.	General comment: • Clarification	• § 83 - 97 (p28 - 30) "Financial institutions should … and appropriate manner." The implementation of this requirement seems to align with the requirements detailed in BIS BCBS "Principles for the Sound Management of Operational Risk"[9] regarding "Business Resiliency and Continuity: Principle 10" (page 6). We recommend the EBA consider reference to this document, as it would help clarify and trace requirements to their potential source.
4.7.2.	General comment: • Clarification	• § 86 - 88 (p29) "Based on the BIA … information security, is ensured." Reference to disruption of business services (e.g. "severe business disruption that") appears highly aligned with the overall approach currently taken by the UK authorities, and potentially the Basel Committee, on Operational resilience. We recommend the EBA consider reference to Operational resilience to avoid potential inconsistencies or divergent approaches are developed.

4.8. Payment service user relationship management (pages 28 - 30)

AFME acknowledges the role of PSP's in keeping PSU's informed of security updates.

However, AFME believes there is a potential risk to the level playing field and to financial stability if further consideration to a horizontal data sharing framework is not developed under the PSD2.

Contacts

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/

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