EBF_036317
13 March 2019

EBF RESPONSE TO THE EBA GUIDELINES ON ICT AND SECURITY RISK MANAGEMENT

General comments:

- In an environment of increasing interconnectedness and complexity in the chain of actors providing financial services, wherein ICT and Cyber security are fundamental in preserving the integrity of systems and data, the EBF welcomes the initiative of EBA to provide guidance for an enhanced resilience of the financial ecosystem, creating at the same time a level playing field for all entities involved.

- It is important for the Guidelines to combine clarity with a degree of flexibility, so as to accommodate internal organisation variations within financial institutions and avoid being too prescriptive (e.g. as to the content of the three lines of defence).

- The EBF proposes that it would be helpful for EBA to make an addition in Section 3 "Background and rationale" about how they envisage the supervision of the implementation of the Guidelines (e.g. possible role for the NCAs).

- The EBF believes that a risk-based approach should be adopted in these Guidelines, especially when controls are mentioned.

- Harmonisation of regulatory requirements is a standing request of the European banking sector so as to facilitate compliance and avoid duplication and overlapping. Therefore, it is proposed that these draft Guidelines are linked – where relevant - to European and international practices/requirements/standards already in place.

Specific comments:

Guidelines Section - Paragraph	Proposal for amendment	Justification
3. Background and rationale **§4:** i) unlike most other sources of risk, malicious cyber-attacks are often difficult to identify or fully eradicate and the breadth of damage difficult to determine;	unlike most other sources of risk, malicious cyber-attacks are often difficult **to anticipate (due to an ever-changing threat scenario),** identify **(due to the advanced techniques employed by many of the attackers),** or fully eradicate **(due to their propagation speed),** and **determine** the breadth of **the** damage **caused by them** ~~difficult to determine~~;	The complexities of today's cyber risks are not limited to their management when attacks are already in place. Rather, financial institutions are currently tackling means to anticipate the cyber risks by leveraging threat intelligence and intelligence sharing among them and with other relevant stakeholders (e.g. public institutions).
§7: These guidelines apply in relation to the management of ICT risk within financial institutions (as defined in paragraph 8). For the purposes of these guidelines, the term ICT risk addresses the operational and security risks of Article 95 PSD2.	These guidelines apply in relation to the management of ICT risk within financial institutions**,** as defined in paragraph ~~8~~**9**. For the purposes of these guidelines, the term ICT risk addresses the operational and security risks of Article 95 PSD2.	Correction of typos.
§8: For PSPs (as defined in paragraph 8) these Guidelines apply for their provision of payment services, in line with the scope and mandate of Article 95 PSD2. For institutions (as defined in paragraph 8) these Guidelines apply for all the activities that they provide.	For PSPs (as defined in paragraph ~~8~~**9**) these Guidelines apply for their provision of payment services, in line with the scope and mandate of Article 95 PSD2. For institutions (as defined in paragraph ~~8~~**9**) these Guidelines apply for all the activities that they provide.	
4. Guidelines **Definitions** **§10** Operational or security incident	A singular unplanned event or a series of linked unplanned events which has or will probably have an adverse impact on the integrity, availability, confidentiality **and/or**	Since "continuity" of ICT systems and services is included in the term "availability", which is already mentioned in this definition, it is proposed that the term

A singular unplanned event or a series of linked unplanned events which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of ICT systems and services.	authenticity ~~and/or continuity~~ of ICT systems and services.	"continuity" is deleted, unless something different is meant. In that case, it should be mentioned explicitly what "continuity" means.
§10 ICT projects Any project, or part thereof, where ICT systems and services are changed, replaced or implemented. ICT projects can be part of wider ICT or business transformation programmes.	Any project, or part thereof, where ICT systems and services are changed, replaced, **dismissed** or implemented. ICT projects can be part of wider ICT or business transformation programmes.	The removal of ICT systems should be covered by the same caution attributed to their change, replacement or implementation.
§10 Information asset A collection of information, either tangible or intangible, that is worth protecting.	A collection of information, either tangible or intangible, that ~~is~~ **supports the critical business functions and processes in the business environment, and that the entity** ~~deems to be~~ **characterises as worth protecting following a risk assessment.**	It might be complex to identify what, in absolute terms, make certain sets of information (or other assets as well) worth protecting. As stated in §17, information assets support financial institutions' "business functions and supporting processes, such as ICT systems, people, third parties and dependencies on other internal and external systems and processes". In other words, "the critical business functions and processes".
§10 ICT asset An asset of software and hardware that is found in the business environment.	An asset **either** ~~of~~ software ~~and~~ **or** hardware**,** that is found in the business environment.	Need for more clarity.
4.1 Proportionality **(Proposal for addition)**	**2. Proportionality cannot be understood as grounds for exemption. All**	The EBF considers that all addressees of these Guidelines should address and manage cyber risk, therefore it is better to

	addressees should address and manage their ICT and security risks.	be clear on the obligation of all addressees to comply with the proposed Guidelines.
4.2.3 Use of third party providers **§7**: Without prejudice to the EBA Guidelines on outsourcing arrangements (EBA GL 2019/XX) and Article 19 PSD2, financial institutions should ensure the effectiveness of the risk mitigating measures as defined by their risk management framework, including the measures set out in these Guidelines, when operational functions of payment services and/or ICT services and ICT systems, are outsourced, including to group entities, or when using third parties.	[…] when **critical/important** operational functions of payment services and/or ICT services and ICT systems, are outsourced, including to group entities, or when using third parties.	The addition is proposed so as to be aligned with the Revised EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02).
§8a: appropriate and proportionate information security objectives and measures including requirements such as minimum cybersecurity requirements, specifications of financial "institutions" data life cycle, and any requirements regarding location of data centres and data encryption requirements network security and security monitoring processes;	appropriate and proportionate information-**related ~~security objectives and~~** measures including requirements such as minimum cybersecurity requirements, specifications of financial "institutions" data life cycle, and any requirements regarding location of data centres and data encryption requirements network security and security monitoring processes;	The EBF finds the wording "security objectives" not clear and proposes that "measures" is sufficient.
4.3.1 Organisation and objectives **§10**: "Financial institutions should identify and manage their ICT risks according to the three lines of defence model…"	For proposed amendments regarding the three lines of defence, please see comments on §32 below.	
§11: Where the three lines of defence model is applied, the ICT function(s) in	[…] in charge of ICT systems, processes and security operations, **which could be** acting	The description of the three lines of defence in the draft Guidelines is overly prescriptive

charge of ICT systems, processes and security operations, acting as the first line of defence, should operate under the supervision of an internal control function acting as a second line of defence. This internal control function should take responsibility for the management of ICT risks. The internal audit function, acting as the third line of defence should have the capacity to independently review and provide assurance of the respective roles the first and second lines of defence (see section 4.3.6)	as the first line of defence, should operate under the supervision of an internal control function**, which could be** acting as a second line of defence. ~~**This internal control function should take responsibility for the management of ICT risks.**~~ The internal audit function, **which could be** acting as the third line of defence should have the capacity to independently review and provide assurance of the ~~**respective roles the**~~ **above-mentioned functions (see section 4.3.6)**	and does not allow organisations to have the necessary flexibility to perform all functions.
§12: Financial institutions should define and assign key roles and responsibilities, and relevant reporting lines for the risk management framework to be effective. This framework should be fully integrated into, and aligned with, financial institutions' overall risk management processes.	Please clarify what kind of integrations are expected (e.g. AMA – capital reserve, risk appetite framework etc.).	Need for clarity.
§15: The ICT risk management should be approved and reviewed, at least once a year, by the management body. Financial institutions should ensure that before any major change of ICT system or ICT services, processes or procedure, and after any significant operational or security incident they identify and assess without undue delay, whether there are any ICT risks resulting from this change or incident.	The ICT risk management should be approved and reviewed, at least once a year, by the **appropriate** management body. ~~**Financial institutions should ensure that before any major change of ICT system or ICT services, processes or procedure, and after any significant operational or security incident they identify and assess without undue delay, whether**~~	Proposal to divide this paragraph into two different paragraphs and move the second paragraph under section 4.6.3 (ICT change management). With regard to the management body, the EBF proposes to add the designation "appropriate", in order to cater for different internal organisation structures.

	~~**there are any ICT risks resulting from this change or incident.**~~ **§XX: Financial institutions should ensure that before any major change of ICT system or ICT services, processes or procedure, and after any significant operational or security incident they identify and assess without undue delay, whether there are any ICT risks resulting from this change or incident.** …………………………………………………………………….. Please clarify whether the ICT risk management framework is meant as a single framework.	…………………………………………………………………… There are separate InfoSec and ORM frameworks. Consolidating the two in a single framework could create operational inconsistencies.
4.3.3 Classification and risk assessment **§19:** To define the criticality of these identified business functions, supporting processes and information assets, financial institutions should, at a minimum, consider the confidentiality, integrity and availability requirements. Asset owners, who are accountable for the classification of the information assets should be identified.	To define the criticality of these identified business functions, supporting processes and information assets, financial institutions should, at a minimum, consider the confidentiality, integrity, ~~and~~ availability **and regulation** requirements. Asset owners, who are accountable for the classification of the information assets should be identified.	There are cases where criticality is described by regulations/standards, such as PCI, SWIFT and GDPR.
§22: Financial institutions should ensure that they continuously monitor threats and	Financial institutions should ensure that they continuously monitor threats and	The amendment is proposed for clarification, as there are different methods to evaluate

vulnerabilities relevant to their business processes, supporting functions and information assets and regularly review the risk scenarios impacting them.	vulnerabilities relevant to their business processes, supporting functions and information assets and regularly review the **ICT risk framework** ~~**risk scenarios impacting them**~~. …………………………………………………………………………… Please clarify how financial institutions are expected to monitor threats.	ICT risks, including scenario analysis and the evaluation of threats and controls against information assets (i.e. business applications) or infrastructure assets. …………………………………………………………………………… Need for clarity.
4.3.6 Audit **§28:** A formal follow up process including provisions for the timely verification and remediation of critical security related audit findings should be established.	A formal follow up process including provisions for the timely verification and remediation of critical ICT ~~**security related**~~ audit findings should be established.	The follow-up process for the verification of critical security related findings would better be extended to all critical ICT findings (independently of whether these are security-related or not).
4.4.1 Information security policy **§30:** The policy should include a description of the main roles and responsibilities for information security management and it should set out the requirements for people, processes and technology in relation to information security, recognising that staff at all levels have responsibilities in ensuring financial institutions' information security. The policy should ensure the confidentiality, integrity and availability of financial institutions' critical logical and physical assets, resources and sensitive data whether at rest, in transit or in use. The information security policy should be communicated within financial institutions	[…]The policy should ensure the confidentiality, integrity and availability of financial institutions' critical logical and physical assets, resources and sensitive data whether at rest, in transit or in use, **according to the risk tolerance of the financial institutions**[…]. ……………………………………………………………………………... […]The information security policy should be communicated within financial institutions, ~~**and**~~ **while** to third parties used by financial institutions **a legal document reflecting the necessary parts of the policy will be communicated.** ~~**as applicable, and**~~ **The information security policy** should apply	It is suggested to link the security policy to the risk tolerance of a financial institution, as related to best practices and legislation. ……………………………………………………………………………

and to third parties used by financial institutions, as applicable, and should apply to all employees.	to all employees **of the financial institutions**.	The information security policy is a confidential and sensitive document that cannot be communicated to third parties.
4.4.2. Information security function **§32:** Financial institutions should establish an information security function, with the responsibilities assigned to a designated person. Financial institutions should ensure the independence and objectivity of the information security function by appropriately segregating it from ICT operations processes (where the three lines of defence model is applied, this function should be the second line of defence function – see section 4.3.1).	Financial institutions should establish an information security function, with the **responsibiliti~~es~~y for it** assigned to a designated person. Financial institutions should ensure the independence and objectivity of the information security function by appropriately segregating it from ICT operations processes ~~**(where the three lines of defence model is applied, this function should be the second line of defence function – see section 4.3.1).**~~	The amendment is proposed for clarity, as the EBF believes that the accountability of the security function can be assigned to a single person, but not all the responsibilities under the security function (which, in turn, would require a role/team). ………………………………………………………………………. In the EBF's view it would be too restrictive and less effective to impose a specific operational or organisational model given that these may vary significantly across financial institutions. The EBF recommends that the Guidelines are not overly prescriptive. To that end, it is proposed that the idea of clearly segregated lines of defence remains, but without assigning specific roles to each one of them. There are cases where an Information Security function/Unit also includes Security Operations which are independent from the rest of IT Operations (e.g. firewall administration vs. network administration). This segregation ensures that Information Security is fully independent (in terms of governance, organization and technology) and cooperates very closely with IT, but as an operating model it effectively creates an

		overlap between the first and second lines as regards to the Information Security role in this context. In addition, it would be more efficient to only list the requirements regarding the security and risk management control objectives. The above argument is further illustrated by the lack of clarity in the relation between the term "internal control function" with "information security function": In §§10 and 11 it could be understood as referring either to the internal control function or, generally, to the second line of defence function of non-financial risks. §32 refers to the information security function also as a function of the second line of defence and also mentions that this function is responsible for the security policy, to monitor its implementation and to report to the management independently. This would imply that the CISO function would be part of the second line of defence. It is not clear how this is related to the internal control function described in §§10 and 11. However, if the EBF's proposal for deletion of the phrase "where the three lines of defence model is applied, this function should be the second line of defence function – see section 4.3.1" is not accepted,

		the EBF suggests clarification on the new role of the information security function in relation to the other second level of defense roles.
4.4.3 Logical security **§34d:** Logging of user activities: privileged users' activities, at a minimum, should be logged and monitored. Access logs should be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with 4.3.3., without prejudice to the retention requirements set out in EU and national law. Financial institutions should use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of services.	No amendment to propose, just a highlight.	This paragraph rightly refers to a retention period "commensurate with the criticality and identified by the company functions". At this stage, there are still variations among the different national laws that need to be taken into account.
§34e: Access management: access rights should be granted, removed or modified in a timely manner, according to predefined approval workflows involving the business owner of the information being accessed (information asset owner). In case of termination of employment access rights should be promptly removed.	Access management: access rights should be granted, ~~**removed**~~ **withdrawn** or modified in a timely manner, according to predefined approval workflows involving the business owner of the information being accessed (information asset owner). In case of termination of employment access rights should be promptly removed.	Quite often, e.g. for sub-contractors, access rights are only withdrawn for a period of time and not removed altogether.

§34g: Authentication methods: financial institutions should enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods should be commensurate with the criticality of ICT systems, the information or the process being accessed. This may include password complexity requirements and/or other authentication methods based on relevant risk (e.g. strong or 2-factor authentication for access that are fraud sensitive, allow access to highly confidential/sensitive information, or that could have material consequences for critical operations).	[…]This ~~**may**~~ **should at minimum** include password complexity requirements ~~**and/**~~or other authentication methods based on relevant risk (e.g. strong or 2-factor authentication for access that are fraud sensitive, allow access to highly confidential/sensitive information, or that could have material consequences for critical operations).	The amendments proposed aim at avoiding multiple interpretations.
4.4.5 ICT operations security **§39:** Financial institutions should implement procedures to prevent occurrence of security issues in ICT systems and ICT services and should respectively minimise their impact on ICT service delivery. These procedures should include the following measures:	[…]These procedures, **following a risk-based approach,** ~~**should**~~ **could** include**,** **for example,** the following measures:	The provision in §39 is overly prescriptive. The EBF believes in the need to adopt a risk-based approach.
§39c: network segmentation, data leakage prevention system or the encryption of network traffic should be implemented	network segmentation, data ~~leakage~~ **loss** prevention system or the encryption of network traffic should be implemented	There is no agreement on the definition of the term "data leakage". The systems responsible for preventing data exfiltration are known as "Data Loss Prevention (DLP)" systems.

§39d: protection of endpoints including servers, workstations and mobile devices should be implemented. Financial institutions should evaluate whether an endpoint meets the security standards defined by financial institutions before it is granted access to the corporate network;	protection of endpoints including servers, workstations and mobile devices should be implemented**, according to risk-based principles**. Financial institutions should evaluate whether an endpoint meets the security standards defined by financial institutions before it is granted access to the corporate network;	Need to pinpoint the importance of a risk-based approach.
§39e: financial institutions should ensure that integrity-checking mechanisms are in place to verify the integrity of software, firmware, and information;	financial institutions should ensure that integrity-checking mechanisms are in place to verify the integrity of **critical** software, firmware, and information;	The proposed amendment aims at better defining the scope of this provision, which could be burdensome and also have a strong impact on costs.
§39f: encryption of data at rest and in transit.	encryption of data at rest and in transit. **The choice of cryptographic controls should be based on the security objectives (confidentiality, integrity/ authenticity, authentication, non-repudiation) and be a result of a risk-based approach.**	It is proposed to adopt a risk-based approach, as it is not possible to encrypt all data at rest and in transit.
§40: Furthermore, on an on-going basis, financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate related risks appropriately. These changes should be part of the financial institutions' formal change management process, which should ensure that changes are properly planned, tested, documented, authorised and deployed.	Please clarify.	The item seems very generic. It is not clear if the control refers to manual processes or if it focuses on automated processes (i.e. static and dynamic code analysis before going live).

4.4.6 Security monitoring **§42:** Financial institutions should establish and implement processes and organisation structures to identify and constantly monitor security threats that could materially affect their ability to provide services. Financial institutions should actively monitor technological developments to ensure that they are aware of security risks. Financial institutions should implement detective measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities for software and hardware, and check for corresponding new security updates.	Financial institutions should establish and implement processes and organisation structures to identify and constantly monitor security threats that could materially affect their ability to provide services. ~~**Financial institutions should actively monitor technological developments to ensure that they are aware of security risks.**~~ Financial institutions should implement detective measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities for software and hardware, and check for corresponding new security updates.	It is not clear how the financial institutions are expected to actively monitor technological developments to ensure that they are aware of security risks.
4.4.7 Information security reviews, assessment and testing **§45:** Financial institutions should establish and implement an information security testing framework that validates the robustness and effectiveness of the information security measures and ensure that this framework considers new threats and vulnerabilities, identified through threat monitoring and the ICT risk assessment process.	Financial institutions should establish and implement an information security testing framework that validates the robustness and effectiveness of the information security measures and ensure that this framework considers ~~**new**~~ threats and vulnerabilities~~,~~ identified through threat monitoring and the ICT risk assessment process. …………………………………………………………………….. Please specify the term “testing framework”.	For clarity. …………………………………………………………………… It seems that “testing framework” refers to a concept that goes beyond the simple drafting of a test plan into the merits of how the tests are performed.

§46: The information security testing framework should ensure that tests: a) are carried out by independent testers with sufficient knowledge, skills and expertise in testing information security measures and not involved in the development of the information security measures; and b) include vulnerability scans and penetration tests (including threat led penetration testing where necessary and appropriate) adequate to the level of risk identified with the business processes and systems.	a) are carried out by independent **internal or external** testers with sufficient knowledge, skills and expertise in testing information security measures and not involved in the development of the information security measures; […]	Institutions should have the freedom to decide whether to adopt external or internal security experts as long as the said experts have an adequate level of independence with regard to the environment they should test.
§48: Financial institutions should monitor and evaluate results of the security tests, and update their security measures accordingly without undue delays in case of critical ICT systems.	Financial institutions should **continuously** monitor and evaluate results of the security tests, and update their security measures **on a risk-based approach** ~~**accordingly**~~**.** ~~**without undue delays in case of critical ICT systems.**~~ **A risk treatment plan should be established including necessary compensative controls, in order to reduce risk, when patching is not an option.**	The EBF proposes this amendment to allow for more flexibility in the proper handling of any weaknesses revealed from tests. Namely, financial institutions might find very low impact weaknesses as a result of a security test and should have the flexibility to decide to defer updating a critical system to its next release, as an update might introduce more risk than the risk of not fixing the weakness (e.g. patching too quickly, before a patch is fully tested, could create other vulnerabilities). Furthermore, the management could be willing to accept the risk of not implementing a (low impact) security measure.

§49: Financial institutions should perform on-going and repeated tests of the security measures. For all critical ICT systems (paragraph 18), these tests shall be performed at least on an annual basis. Non-critical systems should be tested regularly on a risk-based approach, but at least every three years.	Financial institutions should perform on-going and repeated tests of the security measures. For all critical ICT systems (paragraph 18), these tests shall be performed at least on an annual basis. Non-critical systems should be tested regularly on a risk-based approach~~**, but at least every three years.**~~	Since this paragraph already provides for a risk-based approach, there is no need to be more presriptive.
4.4.8 Information security training and awareness **§54:** Financial institutions should establish and implement periodic security awareness programmes to educate their staff, including the management body, on how to address information security related risks.	Financial institutions should establish and implement periodic security awareness ~~**programmes**~~ **sessions** to educate their staff, including the management body, on how to address information security related risks.	The EBF agrees with the necessity to raise awareness on all levels and proposes this amendment for more flexibility.
4.5 ICT Operations management **§55:** Financial institutions should manage their ICT operations based on processes and procedures that are documented, implemented and approved by the management body. This set of documents should define how financial institutions operate, monitor and control the ICT systems and services, including documenting critical ICT operations and should enable financial institutions to maintain an up-to-date ICT asset inventory.	Financial institutions should manage their ICT operations based on processes and procedures that are documented, implemented and approved by the **appropriate** management body.	The EBF proposes to add the designation "appropriate", in order to cater for different internal organisation structures.
§56: To increase the efficiency of financial institutions' ICT operations, financial	[…]Financial institutions should ensure that the performance of their ICT operations is	Given the relevance of security, this should be taken into account by ICT operations

institutions should, as far as possible, automate ICT operations (e.g. job scheduling processes, monitoring of ICT systems, maintenance and repair of financial institutions' assets, shift handover) to minimise potential errors arising from the execution of manual tasks. Financial institutions should ensure that the performance of their ICT operations is aligned with the business requirements.	aligned with the business **and security** requirements.	when performing their duties, at least with the same attention as to the other requirements that ICT operations are subject to.
§60: Financial institutions should monitor and manage lifecycle of ICT assets to ensure that they continue to meet and support business and risk management requirements. Financial institutions should monitor that the ICT assets are supported by their vendors or in-house developers and that all relevant patches and upgrades are applied based on a documented process. The risks stemming from outdated or unsupported ICT assets should be assessed and mitigated.	Financial institutions should monitor and manage lifecycle of ~~**ICT**~~ **software** assets to ensure that they continue to meet and support business and risk management requirements. Financial institutions should monitor that the ~~**ICT**~~ **software** assets are supported by their vendors**,** ~~**or**~~ in-house developers **or other external ICT experts** and that all relevant patches and upgrades are applied based on a documented process. The risks stemming from outdated or unsupported ~~**ICT**~~ **software** assets should be assessed and mitigated.	It is suggested that this provision is limited to software assets, as hardware can be managed in a different way, following a specific hardware technology lifecycle. Moreover, the EBF proposes "or other external ICT experts" to reflect that it is possible to have support also from third parties (for example for open source solutions) that are not the vendor of the software.
§63: Financial institutions should ensure that data and ICT system backups are stored in one or more locations out of the primary site, which are secure and sufficiently remote from the primary site so as to avoid being exposed to the same risks.	Financial institutions should ensure that data and ICT system backups are stored in one or more **different** locations ~~**out of the primary site**~~, which are secure and ~~**sufficiently remote from the primary site so as to avoid being**~~ **not** exposed to the same risks.	For clarity.

4.5.1 ICT incident and problem management **§64:** Financial should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and enable financial institutions to continue or resume critical business functions and processes when disruptions occur. Financial institutions should determine appropriate criteria and thresholds for classifying an event as an operational or security incident, as set out in the 'Definitions' section of these Guidelines, as well as early warning indicators that should serve as an alert to enable early detection of these incidents.	Financial **institutions** should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and enable financial institutions to continue or resume critical business functions and processes when disruptions occur. Financial institutions should determine appropriate criteria and thresholds for classifying an event as an operational or security incident, as set out in the 'Definitions' section of these Guidelines, as well as early warning indicators that should serve as an alert to enable early detection of these incidents.	Correction of typo.
§65c: a problem management procedure to identify, analyse and solve the root cause behind one or more incidents - financial institutions should analyse operational or security incidents that have been identified or have occurred within and/or outside the organisation. Financial institutions should consider key lessons learned from these analyses and update the security measures accordingly;	a problem management procedure to identify, analyse and solve the root cause behind one or more incidents - financial institutions should analyse operational or security incidents that have been identified or have occurred within **~~and/or outside~~** the organisation. Financial institutions should consider key lessons learned from these analyses and update the security measures accordingly;	It is unlikely that a financial institution will be able to act to "identify, consider and resolve" problems external to its organisation.
§65f: specific external communication plans for critical business functions and processes	ii) to provide timely information to external parties (e.g. customers, other market participants, the supervisory authority, **any existing sectoral CERT/CSIRT),** as	The addition is proposed so as to ensure maximum involvement of sector structures dedicated to cybersecurity, in order to facilitate crisis management coordination

i) to collaborate with relevant stakeholders to effectively respond to and recover from the incident; ii) to provide timely information to external parties (e.g. customers, other market participants, the supervisory authority, as appropriate and in line with the applicable regulation.	appropriate and in line with the applicable regulation.	and sectoral response in case of systemic events.
4.6. ICT Project and Change management	It is proposed to amend this section in such a way that it facilitates agile working in ICT development projects.	The requirements of this section are very much based upon the traditional development method (referred to as the "waterfall methodology") which is characterised as the less iterative and inflexible approach, as progress flows in largely one direction through the phases of conception, initiation, analysis, design, construction, testing, deployment and maintenance. However, financial institutions have adopted more and more the agile way of working for the development of software. This means that the requirements as described in §73 which foresees that the process of the development of ICT systems should include a/b/c/d, cannot be met by the financial institutions that use agile methods. *Agile vs Waterfall* The iterative approach of "agile" supports a product rather than a project mindset. This provides greater flexibility throughout the

		development process; whereas on projects the requirements are defined and locked down from the very beginning, making it difficult to change them later. Iterative product development allows the software to evolve in response to changes in business environment or market requirements. As agile working in development of software is more and more standard practice for the financial institutions, the EBF believes that these Guidelines would have to facilitate this. In competitive environments the need for flexibility, especially with the limited separation of duties (SoD) and new ways of organisation projects, is seen as mandatory.
4.6.2 ICT systems acquisition and development **§75:** Financial institutions should ensure that measures are in place to prevent unintentional alteration or intentional manipulation of the ICT systems during development.	Financial institutions should ensure that measures are in place to ~~**prevent**~~ **mitigate the risk of** unintentional alteration or intentional manipulation of the ICT systems during development.	For more flexibility.
§78: Financial institutions should implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Specifically, financial institutions should ensure segregation of production environments	Financial institutions should implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of ~~**unverified**~~ **unauthorised or unaccepted** changes to production systems. Specifically, financial institutions should ensure segregation of production environments from development,	For clarity.

from development, testing and other non-production environments.	testing and other non-production environments. **Copying of production data to other environments shall not take place. Only scrambled data can reside in non-production environments.**	…………………………………………………………………… The addition is proposed to ensure adequate segregation.
§79: Financial institutions should implement measures to protect the integrity of source code of ICT systems that is developed in-house. They should also document the development, implementation, operation, and/or configuration of the ICT systems in a comprehensive manner to reduce unnecessary dependency on subject matter experts. The documentation of the ICT system should contain at least user documentation, technical system documentation and operating procedures.	[…]They should also document the development, implementation, operation, and/or configuration of the ICT systems ~~in a comprehensive manner~~ **according to best practices** to reduce unnecessary dependency on subject matter experts[…].	Reference to best practices avoids the lack of clarity of the term "comprehensive manner" and caters for future developments in the protection of source code.
4.6.3. ICT change management **§81e:** a process for urgent or emergency ICT changes. Financial institutions should handle changes in case of emergency (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards. Such changes should be traceable and notified ex-post to the relevant asset owner for ex-post analysis;	Please clarify.	In §19 there is reference to "asset owners" who are accountable for the classification of the information assets. In this point, reference to the "asset owner" seems to be different and unclear as to whether it refers to the business owner or the IT person responsible for the application.

4.7.1 Business impact analysis **§84:** As part of sound business continuity management, financial institutions should conduct a business impact analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impact, quantitatively and qualitatively, using internal and/or external data and scenario analysis. The BIA should also consider the criticality of the identified and classified business functions, supporting processes and information assets, and their interdependencies in accordance with section 4.3.2.	Please clarify to which criticality dimension this point refers to. ………………………………………………………………….. Please clarify what does “external data” refer to. Please clarify whether BCP requirements need to be included in the BIA.	These Guidelines consider criticality in an extended sense, assessing the dimensions of confidentiality, integrity and availability as well as continuity. ………………………………………………………………….. Need for clarity.
4.7.2. Business continuity planning **§86:** Based on the BIA, financial institutions should establish plans to ensure business continuity (business continuity plans - BCPs) which should be documented and approved by the management body. The plans should specifically consider risks that could adversely impact ICT systems and ICT services. The plans should support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of their business functions, supporting processes and information assets. Financial institutions should coordinate with relevant internal and	Based on the BIA, financial institutions should establish plans to ensure business continuity (business continuity plans - BCPs) which should be documented and approved by the **appropriate** management body. The plans should specifically consider risks that could adversely impact ICT systems and ICT services. **Besides other risks, t**he plans should support objectives to protect and, if necessary, re-establish ~~**the confidentiality, integrity and availability of**~~ their business functions, supporting processes and information assets. Financial institutions should coordinate with relevant internal and	The EBF proposes to add the designation “appropriate”, in order to cater for different internal organisation structures. ………………………………………………………………….. BCPs cover all risks, not only ICT risks. ………………………………………………………………….. The continuity plans are intended to respond to unplanned interruptions of critical processes, not to incidents of confidentiality or integrity of information (the latter could

external stakeholders, as appropriate, during the establishment of these plans.	external stakeholders, as appropriate, during the establishment of these plans.	cause problems of continuity, but not necessarily).
§87: Financial institutions should put BCPs in place to ensure that they can react appropriately to potential failure scenarios and that they are able to maintain the operation of their critical business activities after a disruption within a Recovery Time Objective (RTO, the maximum time within which a system or process must be restored after an incident) and a Recovery Point Objective (RPO, the maximum time period during which data can be lost in case of an incident). In case of a severe business disruption that triggers a specific business continuity plan, financial institutions should prioritise business continuity actions using a risk-based approach, which can be based on the risk assessments carried out under section 4.3. For PSPs this may include for example, facilitating the further processing of critical transactions while remediation efforts continue.	For terms such as RTO and RPO, please consider re-using the definion as given in internationally established and widely used standards (i.e. ISO 22301): 1/ Align the definition of the **RTO** with ISO 22301: **"The period of time following an incident within which a product or service must be resumed, or activity must be resumed, or resources must be recovered."** 2/ Align the definition of the **RPO** (Recovery Point Objective) with ISO 22301: "**The point to which information used by an activity must be restored to enable the activity to operate on resumption"**.	The EBF suggests to facilitate application and avoid confusion by re-using established and well-known definitions from international standards when available, e.g. the ISO 22301 standard definitions for RTO and RPO.
4.7.3 Response and recovery plans **§91:** The plans should also consider alternative options where recovery may not be feasible in the short term because of	The plans should also consider alternative options where recovery may not be feasible in the short term because of cost, risks **or** logistics~~, **or unforeseen circumstances**~~.	The reference to "unforeseen circumstances" makes the perimeter of the Business Continuity Plan extremely broad.

cost, risks, logistics, or unforeseen circumstances.		
4.7.4 Testing of plans **§95a:** include an adequate set of severe but plausible testing scenarios including those considered for the development of the BCPs (including testing of services provided by third parties, where applicable). This should include the switch-over of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that it can run them for a sufficiently representative period of time, and that it can restore normal functioning afterwards;	[…]This ~~**should**~~ **could** include the switch-over of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that it can run them for a sufficiently representative period of time, and that it can restore normal functioning afterwards;	For flexibility in the execution of the Disaster Recovery (DR) tests.

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 3,500 banks - large and small, wholesale and retail, local and international - employing about 2 million people.

www.ebf.eu @EBFeu

For more information:

Alexandra MANIATI
Senior Policy Adviser
Cybersecurity & Social Affairs
a.maniati@ebf.eu

Iliana KOUTOULAKOU
Policy Adviser
Compliance, Tax & Security
i.koutoulakou@ebf.eu