EBA/CP/2018/15

13 December 2018

Consultation Paper

EBA draft Guidelines on ICT and security risk management

Contents

1. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper.

Comments are most helpful if they:

- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 13.03.2019. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found under the Legal notice section of the EBA website.

2. Executive Summary

Complexity of Information and Communication Technology (ICT) risks is increasing and frequency of ICT related incidents (including cyber incidents) is rising together with their potential significant adverse impact on financial institutions' operational functioning. Moreover, due to the interconnectedness between financial institutions, ICT related incidents risk causing potential systemic impact.

These guidelines set out how financial institutions should manage the ICT risks that they are exposed to. In addition, this guidance aims to provide the institutions to which the Guidelines apply with a better understanding of supervisory expectations for the management of ICT risks.

These guidelines build on, the requirements set out in the Guidelines on security measures for operational and security risks as mandated under Article 95 of Directive 2015/2366/EU (PSD2) – hereafter 'Guidelines on security measures'. Those Guidelines were addressed to PSPs and only for their payment services however their relevance was in fact for a broader set of institutions. For that reason, these guidelines have been formulated to be addressed to a broader range of institutions under the EBA's remit (namely to credit institutions who already fell into the scope of the Guidelines on security measures for their payment services but for whom these Guidelines will now apply for all activities) and for investment firms. These Guidelines continue to apply to PSPs for the payment services they provide, they will also extend to other activities of credit institutions and will apply to investment firms for all activities. Collectively, the Guidelines apply to financial institutions as set out in paragraph 9 under the Addressees section.

The term 'ICT risks' addresses the operational and security risks mandate of Article 95 PSD2. This term recognises that the operational risks for payment services refers predominantly to ICT risks because of the electronic nature of payment services (over ICT systems). For this reason, these guidelines refer to 'ICT risk' instead of 'operational risk' to avoid confusion with wider operational risk issues such as conduct risk, legal risk or reputational risk. Furthermore, security risks for payment services may stem from internal processes or external events but ultimately it is their impact on ICT systems that is relevant for payment services. For this reason the definition for 'ICT risk' is based on the definition in the EBA Guidelines on the Supervisory Review and Evaluation Process (EBA GL/2018/03) but includes additional details to clarify that it includes the impact deriving from security risks too.

These guidelines provide details on how institutions should comply with the following provisions in CRD and PSD2 namely:

(i) Article 74 of Directive 2013/36/EU (CRD) which strengthens the governance requirements for institutions including the requirements to have robust governance arrangements with a clear organisational structure with well-defined, transparent and consistent lines of responsibility, and effective processes to identify, manage, monitor and report the risk they are or might be exposed to; and

(ii) Article 95 of Directive 2015/2366/EU (PSD2) which contains explicit provisions for the management of operation and security risks requiring PSPs to have appropriate mitigation measures and control mechanisms to manage the operational and security risks and includes a mandate for the EBA to develop guidelines on this topic.

These Guidelines specify the above-mentioned requirements as follows:

Section 4.1 sets out the proportional application of these guidelines recognising the potential variation in size and complexity between financial institutions.

Section 4.2 of the Guidelines focuses on the management and mitigation of ICT risks through establishing sound internal governance and an internal control framework that sets clear responsibilities for financial institutions' staff including for the management bodies. It requires establishing the financial institutions' ICT strategy, and the management and mitigation of ICT risks through the three lines of defence, where applicable. The guidelines also remind financial institutions to ensure effectiveness of the risk mitigating measures, as defined by their risk management framework, when using third party providers. This should be set in contracts and service-level agreements. Nevertheless, financial institutions should monitor and seek assurance of the level of compliance.

Section 4.3 requires financial institutions to maintain an up-to-date inventory of their business functions, supporting processes and information assets, classify them in terms of criticality, and assess operational risks related to ICT risks that impact them. Financial institutions should determine what measures are required to mitigate identified risks.

Section 4.4 sets out requirements for information security to the extent that the information is held on ICT systems. This section defines requirements to implement a high degree of information security measures, including the establishment of an independent information security function; having an information security policy in place; testing information security measures; and establishing a training programme for all staff.

Section 4.5 specify high level principles on how ICT operations should be managed, including requirements to automate ICT operations, implement logging and monitoring procedures for critical ICT operations, maintain an updated inventory of their ICT assets, monitor and manage the lifecycle of ICT assets, and implement backup plans and recovery procedures. Financial institutions should also establish and implement an incident and problem management process.

Section 4.6 describes requirements for ICT project management, including the acquisition, development and maintenance of ICT systems and services. Financial institutions should ensure that changes to production systems are assessed, tested, approved and implemented in a controlled manner, with the aim of ensuring that ICT projects have appropriate governance and oversight and that development of applications is carefully monitored from test to production phase.

Section 4.7 specifies expectations with regard to business continuity management and developing response and recovery plans, including testing, and consequent update based on the testing results. Financial institutions should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders can be informed in a timely manner.

The last section 4.8 applies only to payment service providers (PSPs). It prescribes requirements for payment service users (PSUs) relationship management, including allowing PSUs to disable specific payment functionalities (where product functionality permits), receiving alerts on initiated and/or failed attempts to initiate payment transactions, and providing PSUs with assistance on questions and requests for support.

In implementing these guidelines, financial institutions should refer to existing standards and leading best practices.

The implementation of these guidelines should be done in accordance with the principle of proportionality taking into account the scale and complexity of operations, the nature of the activity

engaged in, the types of services provided and the corresponding ICT risks related to financial institutions' processes and services.

Next steps

The EBA will finalise these guidelines subsequent to the public consultation that will end by 13.03.2019. The EBA Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) will be repealed after these Guidelines come into force.

3. Background and rationale

1. Information and Communication Technology (ICT) risks can pose significant adverse prudential risks potentially compromising an institution's viability. For this reason, ICT risk management is fundamental for an institution to achieve its strategic, corporate, operational and reputational objectives.

2. The scope of application of the Guidelines covers PSPs for their payment services (any reference to 'payment services' includes 'issuing of electronic money'), credit institutions for all activities beyond their payment services, and also investment firms for all activities. Specifically, these guidelines are addressed to 1) PSPs as defined in Article 4 (11) of PSD2; 2) to institutions, meaning credit institutions and investment firms as defined in point 3 of Article 4(1) of Regulation (EU) No 575/2013; 3) to competent authorities as defined in point 40 of Article 4(1) of Regulation (EU) No 575/2013, including the European Central Bank with regards to matters relating to the tasks conferred on it by Regulation (EU) No 1024/2013, and to competent authorities under PSD2, as referred to in point (i) of Article 4(2) of Regulation (EU) No 1093/2010. For the purpose of these guidelines, the addressees in points 1 and 2 above are collectively referred to as 'financial institutions'.

3. These Guidelines integrate the 'Guidelines on security measures for operational and security risks of payment services' under Article 95 PSD2 which were published in December 2017 (EBA GL 2017/17) and elaborates further on certain topics that contribute to mitigating ICT risks in financial institutions. These Guidelines therefore contribute to a level-playing field for all financial institutions. The Guidelines also address the European Commission (EC) request set out in the EC FinTech Action Plan published in March 2018 which requests that European Supervisory Authorities develop Guidelines on ICT risk management and mitigation requirements in the EU financial sector[1].

4. The Guidelines address ICT risk including security risks which have increased in recent years. This is due to the increasing digitalisation of the financial sector and interconnectedness through telecommunications channels (internet, mobile and wireless lines, and wide area networks) and with other financial institutions and third parties. This renders financial institutions' operations vulnerable to external security attacks including cyber attacks therefore, recognising the need for preparedness for cybersecurity, this Guidelines implicitly cover the need for cyber security within the financial institution's information security measures. Whilst these guidelines recognise that cybersecurity should be undertaken as part of a financial institution's overall information security risk management it is worthwhile pointing out that cyber-attacks have some specific characteristics which should be taken into account in ensuring that the information security measures are adequate to mitigate cyber risks:

   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;

[1] European Commission FinTech Action Plan – https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109 - Box 8, point 2

ii) some cyber-attacks can render common risk management and business continuity arrangements ineffective (e.g. disaster recovery procedure) and they might in some instances fuel the propagation of malware and corrupted data to backup systems;

iii) third party service providers, vendors and vendors' products may become a channel to propagate cyber-attacks, therefore an interconnected institution having individual low relevance may become vulnerable and a source of risk propagation. Observing the weakest link principle, cyber-security should not only be a concern for major market participants or critical service providers.

5. The provisions of the 'Guidelines on the security measures for operational and security risks of payment services' (EBA/GL/2017/17) have been transposed and incorporated into these guidelines, with a wording that has been adapted to fit with the wider scope of addressees and with other provisions. As it was the case for the 'Guidelines on the security measures for operational and security risks of payment services', these guidelines should be applied in a manner that is proportionate to the nature, scope, complexity of the PSPs and institutions' business and the corresponding ICT risks. The 'Guidelines on the security measures for operational and security risks of payment services' (EBA/GL/2017/17) will therefore be repealed with effect from the date of application of these guidelines, which replace them in their entirety.

4. Guidelines

EBA/GL/20XX/XX

DD Month YYYY

Draft Guidelines on ICT and security risk management

Compliance and reporting obligations

Status of these guidelines

1. This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010[2]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.

2. Guidelines set the EBA view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/201x/xx'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3).

[2] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p.12).

Subject matter, scope and definitions

Subject matter

5. These guidelines build on the provisions of Article 74 of Directive 2013/36/EU (CRD) regarding internal governance and derive from the mandate to issue guidelines in Article 95 (3) of Directive (EU) 2015/2366 (PSD2).

6. These guidelines specify the risk management measures that institutions (as defined in paragraph 8 below) must take in accordance with Article 74 of CRD to manage their ICT risks for all activities; and that payment service providers (PSPs as defined in paragraph 8 below) must take, in accordance with Article 95 (1) of PSD2, to manage the operational and security risks (intended as 'ICT risks') relating to the payment services they provide. The guidelines include requirements for information security, including cybersecurity, to the extent that the information is held on ICT systems.

Scope of application

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.

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.

Addressees

9. These guidelines are addressed to financial institutions, which for the purposes of these guidelines refers to: 1) PSPs as defined in Article 4 (11) of PSD2; and 2) to institutions, meaning credit institutions and investment firms as defined in point 3 of Article 4(1) of Regulation (EU) No 575/2013. The guidelines also apply to competent authorities as defined in point 40 of Article 4(1) of Regulation (EU) No 575/2013, including the European Central Bank with regards to matters relating to the tasks conferred on it by Regulation (EU) No 1024/2013, and to competent authorities under PSD2, as referred to in point (i) of Article 4(2) of Regulation (EU) No 1093/2010.

Definitions

10. Unless otherwise specified, terms used and defined in 2013/36/EU (CRD), Regulation (EU) No 575/2013 (CRR) and Directive (EU) 2015/2366 (PSD2) have the same meaning in the guidelines. In addition, for the purposes of these guidelines, the following definitions apply:

ICT risk	Risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change IT within a reasonable time and costs when the environment or business requirements change (i.e. agility)[3]. This includes security risks resulting from inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security.
Management body	(a) For credit institutions and investment firms, this term has the same meaning of the definition in point (7) of Article 3(1) of Directive 2013/36/EU; (b) For payment institutions or electronic money institutions, this term means directors or persons responsible for the management of the payment institutions and electronic money institutions and, where relevant, persons responsible for the management of the payment services activities of the payment institutions and electronic money institutions; (c) For PSPs referred to in points (c), (e) and (f) of Article 1(1) of Directive (EU) 2015/2366, this term has the meaning conferred on it by the applicable EU or national law.
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, authenticity and/or continuity of ICT systems and services.
Senior management	(a) For credit institutions and investment firms, this term has the same meaning of the definition in point (9) of Article 3(1) of Directive 2013/36/EU; (b) For payment institutions and electronic money institutions, this term means natural persons who exercise executive functions within an institution and who are responsible, and accountable to the management body, for the day-to-day management of the institution;

[3] Definition from the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process of 19 December 2014 (EBA/GL/2014/13), amended by the EBA/GL/2018/03.

	(c) For PSPs referred to in points (c), (e) and (f) of Article 1(1) of Directive (EU) 2015/2366, this term has the meaning conferred on it by the applicable EU or national law.
Risk tolerance	The aggregate level and types of risk the PSPs and institutions are willing to assume within their risk capacity, in line with their business model, to achieve their strategic objectives.
Audit Function	(a) For credit institutions and investment firms, the audit function is as referred to in Section 22 of the EBA Guidelines on Internal Governance (EBA GL 2017-11) (b) For PSPs other than credit institutions, the audit function must be independent within or from the PSP and may be an internal and/or external audit function.
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.
Third party	An organisation that has entered into business relationships or contracts with an entity to provide a product or service[4].
Information asset	A collection of information, either tangible or intangible, that is worth protecting.
ICT asset	An asset of software and hardware that is found in the business environment.
ICT systems[5]	ICT set-up as part of a mechanism or an interconnecting network that support the operations of an institution.
ICT services[6]	Services provided by ICT systems to one or more internal or external users. Examples include data entry, data storage, data processing and reporting services, but also monitoring, business and decision support services.

Implementation

Date of application

11. These guidelines apply from dd.mm.yyyy […]

Repeal

12. The Guidelines on security measures for operational and security risks (EBA GL 2017/17) issued in 2017 will be repealed by these guidelines at the date that these Guidelines become applicable.

[4] Definition from G7 fundamental elements for third party cyber risk management in the financial sector
[5] Definition from Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) EBA GL/ 2017/05
[6] ibid

Guidelines on ICT and security risk management

4.1. Proportionality

1. All financial institutions should comply with the provisions set out in these Guidelines in such a way that is proportionate to, and takes into account of, the financial institutions' size, their internal organisation, the nature, scope, complexity and riskiness of the services and products that the financial institutions provide or intend to provide.

4.2. ICT governance and strategy

4.2.1. Governance

2. The management body should ensure that financial institutions have an adequate internal governance and internal control framework in place for their ICT risks. The management body should set clear roles and responsibilities on ICT functions, on information security risk management, and on business continuity, including those for the management body and its committees.
3. The management body should ensure that the quantity and skills of financial institutions' staff is adequate to support their ICT operational needs, their ICT risk management processes on an ongoing basis and to ensure the implementation of their ICT strategy. The management body should ensure that the budget allocated to fulfilling the above is appropriate and sustainable. Furthermore, financial institutions should ensure that staff members occupying key roles receive appropriate training, including information security on an annual basis, or more frequently if required.
4. The management body has overall responsibility for setting, approving and overseeing the implementation of financial institutions' ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT risks.

4.2.2. Strategy

5. The ICT strategy should be aligned with financial institutions' overall business strategy and should define:
    a) how financial institutions' ICT should evolve to effectively support their business strategy, including the evolution of the organisational structure, ICT system changes and key dependencies with third parties;
    b) the planned strategy and evolution of the reference architecture of ICT, including third party dependencies; and

c) clear information security objectives, focusing on ICT systems and ICT services, people and processes.

6. Financial institutions should establish a set of action plans to support the ICT strategy, which should be communicated to all relevant staff (including third party providers where applicable and relevant). The action plans should be periodically reviewed to ensure their relevance and appropriateness. Financial institutions should also establish a process to monitor and measure the effectiveness of the implementation of the ICT strategy.

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.
8. Financial institutions should ensure that contracts and service level agreements with the provider (outsourcing provider, group entity, or third party provider) include the following:
    a) 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;
    b) service level agreements, to ensure continuity of ICT services and ICT systems and performance targets under normal circumstances as well as those provided by contingency plans in the event of service interruption; and
    c) operational and security incident handling procedures including escalation and reporting.
9. Financial institutions should monitor and seek assurance on the level of compliance of these providers with their security objectives, measures and performance targets.

4.3. ICT risk management framework

4.3.1. Organisation and objectives

10. Financial institutions should identify and manage their ICT risks according to the three lines of defence model. PSPs other than credit institutions may use an equivalent internal risk management and control model, to identify and manage these risks. Financial institutions should ensure that their internal control function has sufficient authority, independence, resources, expertise and direct reporting lines to the management body.
11. Where the three lines of defence model is applied, the ICT function(s) in 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).

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.

13. The ICT risk management framework should include processes in place to:

    a) determine the risk tolerance for ICT risks, in accordance with the risk tolerance of financial institutions;
    b) identify and assess the ICT risks to which financial institutions are exposed;
    c) define mitigation measures, including controls, to mitigate ICT risks;
    d) monitor the effectiveness of these measures as well as the number of reported incidents, affecting the ICT related activities, and taking actions to correct the measures where necessary;
    e) report to the management body on the ICT risks and controls.

14. Financial institutions should ensure that the ICT risk management framework is documented, and updated with documented 'lessons learned' during its implementation and monitoring.

15. The ICT risk management framework 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.

4.3.2. Identification of functions, processes and assets

16. Financial institutions should identify, establish and regularly update a mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT risks.

17. Additionally, financial institutions should identify, establish and regularly update a mapping of the information assets supporting their business functions and supporting processes, such as ICT systems, people, third parties and dependencies on other internal and external systems and processes, to be able to, at least, manage the information assets that support their critical business functions and processes.

4.3.3. Classification and risk assessment

18. Financial institutions should classify the identified business functions, supporting processes and information assets in terms of criticality (paragraphs 16 and 17).

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.

20. Financial institutions should review the adequacy of the classification of the information assets and relevant documentation, when risk assessment is performed.

21. Financial institutions should identify the ICT risks, that impact the identified and classified business functions, supporting processes, and information assets, according to their criticality. This risk assessment should be carried out and documented, annually or at shorter intervals if required. Such risk assessments should also be performed on any major change of infrastructure, process or procedures affecting the business functions, supporting processes or information assets and consequently update the current risk assessment of financial institutions.

22. Financial institutions should ensure that they continuously monitor threats and vulnerabilities relevant to their business processes, supporting functions and information assets and regularly review the risk scenarios impacting them.

4.3.4. Risk mitigation

23. Based on the risk assessments, financial institutions should determine which measures are required to mitigate identified ICT risks to acceptable levels and whether changes are necessary to the existing business processes, control measures, and ICT systems and ICT services. Financial institutions should consider the time required to implement these changes and the time to take appropriate interim mitigating measures to minimise ICT and/or security risks to stay within the financial institution's ICT risk tolerance.

24. Financial institutions should define and implement the measures to mitigate identified ICT risks and protect information assets in accordance with their classification.

4.3.5. Reporting

25. Risk assessment results should be reported to the management body in a timely manner. Additionally, PSPs should provide competent authorities with an updated and comprehensive risk assessment as laid down in Article 95(2) of Directive (EU) 2015/2366.

4.3.6. Audit

26. Financial institutions' governance, systems and processes for its ICT risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT risks and in payments (for payment service providers) to provide independent assurance of their effectiveness to the management body. The auditors should be independent within or from the institution. The frequency and focus of such audits should be commensurate with the relevant ICT risks.

27. Financial institutions' management body should approve the audit plan, including any ICT audits, and any material modifications thereto. The audit plan and its execution, including the audit frequency, should reflect and be proportionate to the inherent ICT risks in financial institutions, be updated regularly.

28. A formal follow up process including provisions for the timely verification and remediation of critical security related audit findings should be established.

4.4. Information security

4.4.1. Information security policy

29. Financial institutions should develop and document an information security policy which should define the high-level principles and rules to protect the confidentiality, integrity and availability of financial institutions' and their customers' information. For PSPs this policy should be in line with Article 5 (1j) of Directive (EU) 2015/2366. The information security policy should be in line with financial institutions' information security objectives, and based on the relevant results of the risk assessment process.

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 and to third parties used by financial institutions, as applicable, and should apply to all employees.

31. Based on the information security policy, financial institutions should establish and implement security measures to mitigate the ICT risks that they are exposed to. These measures should include:

    a) independent information security function (Section 4.4.2)
    b) logical security (Section 4.4.3)
    c) physical security (Section 4.4.4)
    d) ICT operations security (Section 4.4.5)
    e) security monitoring (Section 4.4.6)
    f) information security reviews, assessment and testing (Section 4.4.8)
    g) information security training and awareness (Section 4.4.7)

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). In accordance with financial institutions' internal governance structure, financial institutions should ensure that the information security function is not responsible for any internal audit. The function should report directly to the management body.

33. The information security function should at a minimum:

    a) be responsible for the information security policy for financial institutions and control its deployment;
    b) monitor the implementation of the information security measures through key risk indicators;
    c) report and advise the management body regularly, and on an ad hoc basis as needed, on the status of information security management and risks to financial institutions;
    d) ensure that the information security requirements are adhered to when using third parties; and
    e) ensure that all employees and third parties accessing information and systems are adequately informed of the information security policy, for example through information security training and awareness sessions.

4.4.3. Logical security

34. Financial institutions should define, document and implement procedures for logical access control (identity and access management). These procedures should be implemented, enforced, monitored and periodically reviewed. The procedures should also include controls for monitoring anomalies. These procedures should, at a minimum, implement the following elements, where the term 'user' also comprises technical users:

    (a) **Need-to-Know, Least Privilege and Segregation of Duties**: financial institutions should manage access rights to information assets and their supporting systems on a 'need-to-know' basis, including for remote access. Users should be granted minimum access rights that are strictly required to execute their duties (principle of 'least privilege') i.e. to prevent unjustified access to a large set of data or that the allocation of combinations of access rights may be used to circumvent controls (principle of 'segregation of duties').
    (b) **User accountability:** financial institutions should limit, as much as possible, the usage of generic and shared user accounts and ensure that users can be identified for the actions performed in the ICT systems.
    (c) **Privileged access rights:** financial institutions should implement strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements (e.g. administrator accounts). In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems should be granted only on a need-to-know basis and when strong authentication solutions are used.
    (d) **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.

(e) **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.

(f) **Access recertification:** access rights should be periodically reviewed to ensure that users do not possess excessive privileges and that access rights are removed when no longer required.

(g) **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).

35. Electronic access by applications to data and ICT systems should be limited to a minimum required to provide the relevant service.

4.4.4. Physical security

36. Financial institutions' physical security measures should be defined, documented and implemented to protect its premises, data centres and sensitive areas from unauthorised access and from environmental hazards.

37. Physical access to ICT systems should be permitted only for authorised individuals. Authorisation should be assigned in accordance with the staff's tasks and responsibilities, limited to individuals who are appropriately trained and monitored. Physical access should be regularly reviewed to ensure that unnecessary access is promptly revoked when not required.

38. Adequate measures to protect from environmental hazards should be commensurate with the importance of the buildings and the criticality of the operations or ICT systems located in these buildings.

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:

a) identify potential vulnerabilities which should be evaluated and remediated by ensuring software and firmware are up to date, including the software provided by financial institutions to its internal and external users, by deploying critical security patches or by implementing compensating controls;

b) secure configuration baselines of critical network components such as core routers or switches should be implemented;

c) network segmentation, data leakage prevention systems or the encryption of network traffic should be implemented;

d) 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;
e) financial institutions should ensure that integrity-checking mechanisms are in place to verify the integrity of software, firmware, and information;
f) encryption of 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.

4.4.6. Security monitoring

41. Financial institutions should establish and implement policies and procedures to detect anomalous activities that may impact financial institutions' information security, and to respond to these events appropriately. As part of this continuous monitoring, financial institutions should implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets. The continuous monitoring and detection processes should cover:

a) relevant internal and external factors, including business and ICT administrative functions;
b) transactions to detect misuse of access by third parties or other entities and internal misuse of access; and
c) potential internal and external threats.

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.

43. The security monitoring process should also help financial institutions to understand the nature of operational or security incidents, to identify trends and to support the organisation's internal investigations.

4.4.7. Information security reviews, assessment and testing

44. Financial institutions should perform a variety of different information security reviews, assessments and testing, so as to ensure effective identification of vulnerabilities in its ICT systems and ICT services. Specifically, financial institutions may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, the institution should foster source code reviews, penetration tests, or red team exercises.

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.

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.

47. Financial institutions should ensure that tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed internet facing critical applications.

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.

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.

50. For PSPs, the testing framework should also encompass the security measures relevant to (i) payment terminals and devices used for the provision of payment services, (ii) payment terminals and devices used for authenticating the PSU and (iii) devices and software provided by the PSP to the PSU to generate/receive an authentication code.

51. Based on the security threats observed and the changes made, testing should be performed to incorporate scenarios of relevant and known potential attacks.

4.4.8. Information security training and awareness

52. Financial institutions should establish a training programme for all staff to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss. Financial institutions should ensure that the training programme provides training for staff members at least annually.

53. Financial institutions should ensure that staff members occupying key roles receive targeted information security training at least annually.

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.

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.

56. To increase the efficiency of financial institutions' ICT operations, financial 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.

57. Financial institutions should implement logging and monitoring procedures for critical ICT operations to allow for detection, analysis and correction of errors.

58. Financial institutions should maintain an updated inventory of their ICT assets (including IT systems, network devices, databases, etc). The ICT asset inventory should document the configuration of the ICT assets and the links and interdependencies between the different ICT assets to enable a proper configuration and change management process.

59. The ICT asset inventory should be sufficiently detailed to enable the prompt identification of an ICT asset, its location, security classification, and ownership. Interdependencies between assets should be documented to help in the response to security and operational incidents, including cyber-attacks.

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.

61. Financial institutions should implement performance and capacity planning and monitoring process to prevent, detect and respond to important performance issues of ICT systems and ICT capacity shortages in a timely manner.

62. Financial institutions should define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required. The scope and frequency of backups should be set in line with business recovery requirements and the criticality of the data and the ICT systems, assessed according to the performed risk assessment. Testing of the backup and restoration procedures should be undertaken on a periodic basis.

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.

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.

65. To minimise the impact of adverse events and enable timely recovery, financial institutions should establish appropriate processes and organisational structures to ensure the consistent and integrated monitoring, handling and follow-up of operational and security incidents to ensure that the root causes are identified and eliminated preventing the occurrence of repeated incidents. The incident and problem management process should establish:

    a) the procedures to identify, track, log, categorise and classify incidents according to a priority based on business criticality and service agreements;
    b) the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber-attacks);
    c) 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;
    d) effective internal communication plans, including incident notification and escalation procedures - covering also security-related customer complaints - to ensure that:
        i) incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the relevant senior management and ICT senior management;
        ii) the management body is informed on an ad-hoc basis in case of significant incidents and at least, informed of the impact, reaction and additional controls defined because of the incidents.
    e) an incident response procedure to mitigate the impacts related to the incidents and to ensure that the service becomes operational and secure in a timely manner;
    f) specific external communication plans for critical business functions and processes
        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.

4.6. ICT Project and Change management

4.6.1. ICT project management

66. Financial institutions should implement a governance process with an adequate project implementation leadership to effectively support the implementation of the ICT strategy through ICT projects.

67. Financial institutions should appropriately monitor and mitigate risks deriving from the portfolio of ICT projects, considering also risks that may result from interdependencies between different projects and from dependencies of multiple projects on the same resources and/or expertise.

68. Financial institutions should establish and implement an ICT project management policy which defines the phases of each project and includes at a minimum:

    a) project objectives;
    b) roles and responsibilities;
    c) project risk assessment;
    d) project plan, timeframe and steps;
    e) procurement management;
    f) key milestones;
    g) and change management requirements.

69. The policy should ensure that information security requirements are analysed and approved by a function that is independent from the development function through all phases of an ICT project.

70. Financial institutions should ensure that all areas impacted by an ICT project are represented in the project team and that the project team has an adequate knowledge required to ensure secure and successful project implementation.

71. The responsibilities of the project team members should be defined and documented in the project plan and approved by the project implementation leader.

72. Establishment and progress of ICT projects and their associated risks should be reported to the management body, individually or aggregated, depending on the importance and size of the ICT projects, regularly and on an ad hoc basis as appropriate. Financial institutions should include project risk in their risk management framework.

4.6.2. ICT systems acquisition and development

73. Financial institutions should develop and implement a process governing the acquisition, development and maintenance of ICT systems. This process should include:

    a) setting objectives during the development phase;
    b) technical implementation (including secure coding/programming guidelines);
    c) quality assurance standards; and

d) testing, approval and release, irrespective of whether the development is done in house or externally by a third party.

74. Financial institutions should ensure that before any acquisition or development of ICT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined. In addition, this should include provisions for technical specifications and test plans which are approved by the relevant business management as well as ICT management.

75. Financial institutions should ensure that measures are in place to prevent unintentional alteration or intentional manipulation of the ICT systems during development.

76. Financial institutions should have a methodology in place for testing and approval of ICT systems prior to their first use. When applicable, regression testing should be performed to ensure that new ICT systems perform in the same way as previously developed and tested systems. They should also use test environments that adequately reflect the production environment so that the behaviour of the ICT systems in the production environment can be predicted and sufficiently tested.

77. Financial institutions should test ICT systems, ICT services and information security measures to identify errant coding practices and systems vulnerabilities that could lead to security weaknesses, violations and incidents.

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 from development, testing and other non-production environments.

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.

80. Financial institutions' processes for acquisition and development of ICT systems should also apply to ICT systems developed or managed by the business function's end users outside of the ICT organisation (e.g. business managed applications or end user computing applications) in a risk based manner. The financial institutions should maintain a register of these applications that support critical business functions or processes (e.g. business managed applications and EUCs).

4.6.3. ICT change management

81. Financial institutions should establish and implement an ICT change management process to ensure that all changes to ICT systems are assessed, tested, approved and implemented in a controlled manner. The ICT change management process should contain at least the following elements:

a) a process for recording all change requests to ICT systems;
b) an evaluation, testing, and approval process for all change requests to ICT systems - specifically financial institutions should evaluate the impact of the proposed changes and the potential implementation risks. Following approval, and based on the outcome of the evaluation, the process should include a formal acceptance of any new residual risks;
c) testing and independent validation processes of ICT systems' changes for possible compatibility and security implications prior to deployment to production environment;
d) an authorisation process, only after which ICT changes move to production. This authorisation process should be undertaken by responsible personnel in such a way so that a rollback can be performed in case of a malfunction;
e) 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; and
f) a process to update ICT systems' documentation to reflect the changes carried out, where necessary.

82. Financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate the risk involved. These changes should be part of financial institutions' formal change management process, which should ensure that changes are properly planned, tested, documented and authorised.

4.7. Business continuity management

83. Financial institutions should establish a sound business continuity management (BCM) process to maximise their abilities to provide services on an on-going basis and to limit losses in the event of severe business disruption

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.

85. Financial institutions should ensure that their ICT systems and ICT services are designed and aligned with their BIA, for example with redundancy of certain critical components to prevent disruptions caused by events impacting those components.

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 external stakeholders, as appropriate, during the establishment of these plans.

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.

88. Financial institutions should consider a range of different scenarios in their BCPs, including extreme but plausible ones, to which they might be exposed, including a cyber - attack scenario, and assess the potential impact that such scenarios might have. Based on these scenarios, financial institutions should describe how continuity of ICT systems and services, as well as financial institutions' information security, is ensured.

4.7.3. Response and recovery plans

89. Based on the BIA (paragraph 86) and plausible scenarios (paragraph 87), financial institutions should develop response and recovery plans. These plans should specify what conditions may prompt activation of the plan and what actions should be taken to ensure the availability, continuity and recovery of, at least, financial institutions' critical ICT systems and ICT services. The response and recovery plans should aim to meet the recovery objectives of financial institutions' operations.

90. The response and recovery plans should consider both short-term and long-term recovery options. The plans should:

    a) focus on the recovery of the operations of critical business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of financial institutions, the financial system, including on payment systems and on payment service users, and to ensure execution of pending payment transactions;
    b) be documented and made available to the business and support units and readily accessible in case of emergency; and

c) be updated in line with lessons learned from incidents, tests, new risks identified and threats, and changed recovery objectives and priorities.

91. The plans should also consider alternative options where recovery may not be feasible in the short term because of cost, risks, logistics, or unforeseen circumstances.

92. Furthermore, as part of the response and recovery plans, financial institutions should consider and implement continuity measures to mitigate failure of third party providers, which are of key importance for financial institutions' ICT service continuity (in line with the provisions of EBA Guidelines on outsourcing arrangements EBA GL/2019/XX regarding business continuity plans).

4.7.4. Testing of plans

93. Financial institutions should test their BCPs, and ensure that the operation of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties) are tested at least annually. The testing activities period and/or test duration should be performed in a way to ensure minimum disruption to normal business operations.

94. BCPs should be updated at least annually, based on testing results, current threat intelligence and lessons learned from previous events. Any changes in recovery objectives (including RTO and RPO) and/or changes in business functions, supporting processes, and information assets, should also be considered, where relevant, as a basis for updating the BCPs .

95. Financial institutions' testing of their BCPs should demonstrate that they are able to sustain the viability of the business until critical operations are re-established. In particular they should:

a) 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;
b) be designed to challenge the assumptions on which BCPs rest, including governance arrangements and crisis communication plans; and
c) include procedures to verify the ability of their staff, ICT systems and ICT services to respond adequately to the scenarios defined in 95(a).

96. Test results should be documented and any identified deficiencies resulting from the tests should be analysed, addressed and reported to the management body.

4.7.5. Crisis communications

97. In the event of a disruption or emergency, and during the implementation of the BCPs, financial institutions should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including the competent authority when required by national regulation, and also relevant external service providers, are informed in a timely and appropriate manner.

4.8. Payment service user relationship management

98. PSPs should establish and implement processes to enhance PSUs' awareness of security risks linked to the payment services by providing PSUs with assistance and guidance.

99. The assistance and guidance offered to PSUs should be updated in the light of new threats and vulnerabilities, and changes should be communicated to the PSU.

100. Where product functionality permits, PSPs should allow PSUs to disable specific payment functionalities related to the payment services offered by the PSP to the PSU.

101. Where, in accordance with Article 68(1) of Directive (EU) 2015/2366, a PSP has agreed with the payer spending limits for payment transactions executed through specific payment instruments, the PSP should provide the payer with the option to adjust these limits up to the maximum agreed limit.

102. PSPs should provide PSUs with the option to receive alerts on initiated and/or failed attempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their account.

103. PSPs should keep PSUs informed about updates in security procedures which affect PSUs regarding the provision of payment services.

104. PSPs should provide PSUs with assistance on all questions, requests for support and notifications of anomalies or issues regarding security matters related to payment services. PSUs should be appropriately informed about how such assistance can be obtained.

5. Accompanying documents

5.1. Draft cost-benefit analysis / impact assessment

As per Article 16(2) of Regulation (EU) No 1093/2010 (EBA Regulation), any guidelines and recommendations developed by the EBA shall be accompanied by an Impact Assessment (IA), which analyses 'the potential related costs and benefits'.

This section presents a cost-benefit analysis of adopting the Guidelines described in this Consultation Paper by financial institutions. Given the nature and the scope of the guidelines, the IA is high-level and qualitative in nature.

A. Problem identification

Complexity of Information and Communication Technology (ICT) risks is increasing and frequency of ICT related incidents (including cyber incidents) is rising together with their potential significant adverse impact on the financial institutions' operational functioning. Moreover, due to the interconnectedness between financial institutions, ICT related incidents risk causing potential systemic impact.

For PSPs, ICT plays an important role in the efficient functioning of payment systems. A recent risk analysis exercise conducted by the EBA and the ECB identified various threats and vulnerabilities to which PSPs are currently exposed when providing their payment services. The most common risks are:

i. inadequate protection of communication channels used for payments;
ii. inadequately secured IT systems used for payments;
iii. unsafe behaviour of users and PSPs; and
iv. technological advancements and tools that are available to potential fraudsters or malicious attackers.

For institutions, ICT is a key resource in developing and supporting banking services; ICT systems are not only key enablers of institutions' strategies, forming the backbone of almost all banking processes and distribution channels, but they also support the automated controls environment on which core banking data is based. ICT systems and services also represent material proportions of institutions' costs, investments and intangible assets. Furthermore, technological innovation plays a crucial role in the banking sector from a strategic standpoint, as a source of competitive advantage, as it is a fundamental tool to compete in the financial market with new products as well as through facilitating the restructuring and optimisation of the value chain. As a result of the increasing importance of ICT in the banking industry, some recent trends include:

i. the emergence of cyber risks together with the increased potential for cybercrime; and

ii. the increasing reliance on third parties for ICT services and products, often in the form of diverse packaged solutions resulting in manifold dependencies and potential constraints and concentration risks.

In view of the growing importance and increasing complexity of ICT risk for financial institutions, and based on the mandates set out for the EBA, the EBA has published:

a) Guidelines on the assessment of ICT risk as part of the SREP, addressed to competent authorities (EBA/GL/2017/05); and

b) Guidelines on security measures for operational and security risks of payment services, addressed to PSPs (EBA GL 2017/17).

The guidelines above in point (b) set out very important requirements for PSPs for the provision of their payment services but, for credit institutions, which are PSPs the existing Guidelines do not address ICT risks from their other activities. Furthermore the Guidelines in point (b) do not apply to investment firms. The new Guidelines on ICT and security management aim to address the European Commission request[7] for Guidelines for all institutions regarding their ICT security and governance. The aim is to ensure sound ICT and security management in the EU financial sector and to ensure a level playing field for all institutions. The new Guidelines integrate the existing text of the Guidelines on security measures for operational and security risks and broaden the scope of addressees, namely covering all activities for credit institutions and investment firms. Furthermore, the new Guidelines build on the existing requirements in the Guidelines on security measures but are more explicit, clarifying in more detail how institutions can ensure adequate management of their ICT and security.

B. Policy objectives

The main objective of the Guidelines is to establish harmonised requirements for ICT and security across PSPs (for payment services) and institutions (for credit institutions and investment firms this extends to all activities). In return, this is expected to contribute to better management of risks arising to market integrity, consumers and the viability of institutions and PSPs from ICT.

Operationally, the Guidelines aim to integrate all provisions on ICT and security management in a single legal text for all financial institutions and to a wider range of activities.

C. Baseline scenario

The status quo should constitute the baseline scenario. It entails maintaining the current regulatory framework, which includes two legislations related to ICT risk management:

[7] European Commission FinTech Action Plan: For a more competitive and innovative European financial sector, 8 March 2018, COM (2018) 109 final.

i. Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) (EBA/GL/2017/05): These Guidelines are addressed to competent authorities and are intended to promote common procedures and methodologies for the assessment of the Information and Communication Technology (ICT) risk under the supervisory review and evaluation process (SREP). The Guidelines set out the requirements that competent authorities should apply in their assessment of ICT on the general provisions and application of scoring as part of the SREP assessment of risks to capital, assessment of institutions' governance and strategy on ICT, and the assessment of institutions' ICT risk exposures and controls.

ii. Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) (EBA GL 2017/17): These Guidelines set out the requirements that payment service providers (PSPs) should implement in order to mitigate operational and security risks derived from the provision of payment services which in practice relates to the impact of the operational and security risks on their ICT systems.

D. Options considered

Scope

Option 1a: Develop a separate set of Guidelines on ICT risk management addressed only to credit institutions and investment firms, and maintaining the Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) for PSPs.

Option 1b: Develop a single set of Guidelines on ICT and security management addressed to PSPs for their payment services and to credit institutions and investment firms (for all activities), integrating (and consequently repealing) the Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2).

Level of detail in prescribed requirements

Option 2a: Set out detailed and prescriptive requirements on ICT and security management

Option 2b: Set out high-level principle-based requirements on ICT and security management

E. Cost-Benefit Analysis and preferred options

Scope

Option 1a would mean a new set of Guidelines on ICT and security management for credit institutions and investments firms, for all activities and services. However, given that most of the requirements that apply for security of payment services (i.e. those already within the published Guidelines on security measures) are also applicable for security of other services and activities, the two set of Guidelines would have significant overlap and would create confusion for credit institutions who already apply the Guidelines on security measures for their payment services. This means then that the benefits of having two different Guidelines are limited.

Option 1b would ensure that the same requirements are set across PSPs for payment services (i.e. not extending beyond the PSD2 mandate), and for all institutions for all services, creating a level playing field. The mandate for security measures for operational and security risks in payment services, in practice refers to security measures for operational and security risks on ICT systems. As suchIt would also reduce the compliance burden for institutions, which will then need to refer to a single legal text for their requirements on ICT risk management, irrespective of the service they provide. In addition, it can still take into account any specificities in the ICT risk management for PSPs, by setting exclusive requirements for payment services.

Option 1b is retained.

Level of detail in prescribed requirements

Option 2a to include a detailed and prescriptive requirements on ICT risk management could increase comparability and level playing field across financial institutions. However, it risks that the requirements become obsolete very quickly due to the ever-changing nature of ICT risks. Financial institutions would be unable to ensure that their ICT risk management properly mitigates ICT risks in an ecosystem in which new threats are evolving continuously.

Option 2b on the other hand would allow financial institutions to adapt their risk management to new challenges and developments. As such, this option reflects financial institutions' need to anticipate and mitigate unknown types of ICT risks.

Option 2b is retained.

5.2. Views of the Banking Stakeholder Group (BSG) [PLACEHOLDER]

5.3. Feedback on the public consultation and on the opinion of the BSG [PLACEHOLDER]