cssf

Commission de Surveillance
du Secteur Financier

Circular CSSF 20/750

Requirements regarding information and communication technology (ICT) and security risk management

Commission de Surveillance du Secteur Financier

In case of discrepancies between the French and the English text, the French text shall prevail.

Circular CSSF 20/750

Re: Requirements regarding information and communication technology (ICT) and security risk management

Luxembourg, 25 August 2020

To all credit institutions and to all PFS

To all payment institutions and and to all electronic money institutions

Ladies and Gentlemen,

This circular implements the Guidelines of the European Banking Authority EBA/GL/2019/04 on ICT and security risk management (hereinafter "ICT Guidelines").

Moreover, the circular specifies that the content of the ICT Guidelines also reflects the expectations of the CSSF as regards the risk management measures and the control and security arrangements referred to in the Law of 5 April 1993 on the financial sector ("LFS") and in the Law of 10 November 2009 on payment services ("LPS").

Commission de Surveillance du Secteur Financier

1. Requirements regarding information and communication technology (ICT) and security risk management

Implementation of the Guidelines of the European Banking Authority EBA/GL/2019/04

1. By way of this circular, the CSSF, in its capacity as competent authority, complies with and applies the Guidelines (hereinafter "ICT Guidelines") of the European Banking Authority (hereinafter "EBA") on ICT and security risk management (reference: EBA/GL/2019/04). Consequently, the CSSF has integrated the ICT Guidelines into its administrative practice and regulatory approach with a view to promote supervisory convergence in this field at European level.

Risk management measures and control and security arrangements

2. The CSSF considers that the content of the ICT Guidelines reflects its expectations as regards risk management measures and control and security arrangements as referred to in Articles 5(1a), 17(1a), 36(1) and 37-1(4) of the LFS and in Articles 11(2) and 105-1 of the LPS.

3. The CSSF expects thus from all entities authorised under the LFS and the LPS - whether they fall or not within the scope of the ICT Guidelines - to implement the content of these ICT Guidelines in order to manage their ICT and security risks.

Clarifications regarding the content of the ICT Guidelines

4. For the purpose of this circular, the following terms used in the ICT Guidelines are to be understood as follows:

   a. "Management body" used in paragraph 50 of Guideline "3.5. ICT operations management" means "management body or authorised management as defined by the management body".

   b. "Senior management" used in point 60(d)(i) of Guideline "3.5.1. ICT incident and problem management" means "management".

2. Amendment of Circular CSSF 12/552

5. This circular amends Circular CSSF 12/552, as amended[1], as follows:

   a. In Chapter 2 of Part II, the 4th paragraph of point 9 is replaced by the following: "*The second line is formed by the support functions, including the financial and accounting function (Section 5.2.2 of this circular), and the compliance and risk control functions (Sub-chapter 6.2 and Sections 6.2.5 and 6.2.6 of this circular and guideline 3.3 implemented by Circular CSSF 20/750 on the information and communication technology (ICT) and security risk management framework) which contribute to the independent risk control.*"

   b. In Chapter 5 of Part II:

      i. point 85 of Section 5.2.3 is replaced by the following: "*Institutions shall organise their IT function so as to have control over it and to ensure robustness, effectiveness, consistency and integrity pursuant to point 12. For those purposes, they shall comply with the requirements of Circular CSSF 20/750 on requirements regarding information and communication technology (ICT) and security risk management*".

      ii. point 86 of Section 5.2.3 is deleted.

3. Repeal and replacement of Circular CSSF 19/713

6. The ICT Guidelines implemented via this circular repeal Guidelines EBA/GL/2017/17 on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2). Consequently, this circular repeals and replaces Circular CSSF 19/713 which implemented Guidelines EBA/GL/2017/17.

7. It is furthermore reminded that the term "ICT and security risks" covers the operational and security risks referred to in Article 105-1 of the LPS.

[1] *By Circulars CSSF 13/563, CSSF 14/597, CSSF 16/642, CSSF 16/647 and CSSF 17/655.*

Commission de Surveillance du Secteur Financier

4. Additional requirement for payment service providers (PSPs)[2]

8. As provided for in paragraph 24 of Guideline "3.3.5. Reporting" and in accordance with Article 105-1(2) of the LPS, PSPs are required to provide the CSSF with an updated and comprehensive risk assessment related to payment services (hereafter "PSP ICT Assessment").The CSSF has developed a standardised form for the PSP ICT Assessment to be used by all PSPs.

   The objective of this standardised PSP ICT Assessment form is to give guidance to the PSPs on the CSSF's expectations on the information to be provided via the PSP ICT Assessment, and hence achieve a certain level of harmonisation and comparability among the PSPs' ICT Assessments.

   Concerning the scope of the PSP ICT Assessment, the following is to be highlighted:

   - Institutions whose business model does not include the provision of payment services (as defined in article 1(38) of the LPS), do not have to provide the PSP ICT Assessment. As soon as the business model of an institution includes the provision of payment services, it shall submit to the CSSF for that calendar year a PSP ICT Assessment.
   - EEA Branches established in Luxembourg, which offer payment services, do not have to provide the CSSF with a PSP ICT Assessment. On the other hand, Luxembourg based PSPs which have established branches in other EEA countries, which provide payment services, have to include those branches in their PSP ICT Assessment. In the event the ICT and security risk assessment for these branches deviates from that of the PSP, it should be made clear in the PSP ICT Assessment[3].

   All PSPs must submit the duly completed PSP ICT Assessment form on an annual basis to the CSSF **no later than 31 March each year and covering the previous calendar year**.

   The PSP ICT Assessment form is published in the CSSF's eDesk portal which is available at:

[2] *As defined in Article 1(37) of the LPS.*

[3] *see EBA Q&A ID number 2018_4176*

https://edesk.apps.cssf.lu/

The PSP ICT Assessment shall be validated by the Management body of the PSP, i.e. at least by the member of the Management body responsible for the ICT function. This validation shall be specified in the respective section of the PSP ICT Assessment.

The duly completed and validated PSP ICT Assessment shall be submitted annually by a member of the Management body to the CSSF exclusively via the CSSF's eDesk portal.

5. Entry into force

9. This circular enters into force on 25 August 2020.

10. The guidelines are attached to this circular and are available on the EBA website: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

EBA/GL/2019/04

29 November 2019

FINAL REPORT

EBA Guidelines on ICT and security risk management

Contents

1. Executive summary

The complexity of information and communication technology (ICT) and security risks is increasing and the frequency of ICT and security-related incidents (including cyber incidents) is rising, together with their potential significant adverse impact on financial institutions' operational functioning. Moreover, due to the interconnectedness of financial institutions, ICT and security-related incidents risk causing potential systemic impacts. The EBA has responded to this by detailing how supervisors should cover ICT and security risks within supervision (EBA/GL/2017/05), by detailing how financial institutions should manage outsourcing (EBA/GL/2019/02) and by describing the expectations for ICT and security risk management for the financial institutions in these guidelines.

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

These guidelines integrate and are built on the requirements set out in the 'Guidelines on security measures for operational and security risks of payment services' (hereafter 'Guidelines on security measures'), which were published in December 2017 (EBA/GL/2017/17) and which have applied since January 2018 in fulfilment of the mandate in Article 95(3) of Directive 2015/2366/EU (PSD2). Those guidelines were addressed to payment service providers (PSPs), and only applied to their payment services; however, they were in fact relevant to a broader set of institutions. For that reason, these guidelines have been formulated to be addressed to a broader range of financial institutions under the EBA's remit (namely to credit institutions which already fell within the scope of the guidelines on security measures for their payment services, but for which these guidelines will now apply for all activities) and to investment firms. These guidelines continue to apply to PSPs for the payment services they provide; they extend to other activities of credit institutions and also 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 and security risks' addresses the operational and security risks mandate of Article 95 of the revised Payments Services Directive (PSD2). This term recognises that the operational risks for payment services refer predominantly to ICT and security risks because of the electronic nature of payment services (over ICT systems). For this reason, these guidelines refer to 'ICT and security risk' instead of 'operational and security risk' to avoid confusion with wider operational risk issues, such as conduct risk, legal risk and reputational risk. Furthermore, security risks may stem from inadequate or failed internal processes or external events, but ultimately it is their impact on systems and data that is relevant. The definition of 'ICT and security risk' is based on the definition in the EBA Guidelines on the revised common procedures and methodologies for the supervisory review and evaluation process and supervisory stress testing (EBA/GL/2018/03); thus, it encompasses data integrity risk but includes additional details to clarify that it covers the impact deriving from security risks.

These guidelines provide details on how financial institutions should comply in order to address ICT and security risks, with the following provisions in the Capital Requirements Directive (CRD) and PSD2:

(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;

(ii) Article 95 of Directive 2015/2366/EU (PSD2), which contains explicit provisions for the management of operation and security risks that require 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 3.1 sets out the proportionate application of these guidelines, recognising the potential variation in size, complexity, internal organisation, nature, scope and riskiness of the services and products between financial institutions.

Section 3.2 of the guidelines focuses on the management and mitigation of ICT and security 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 the establishment of the financial institutions' ICT strategy, which should be aligned with their overall business strategy. The guidelines also remind financial institutions to ensure the effectiveness of the risk-mitigating measures, as defined by their risk management framework, when outsourcing or using third party providers. This should be set out in contracts and service level agreements. Nevertheless, financial institutions should monitor and seek assurance of the level of compliance.

Section 3.3 requires financial institutions to manage and mitigate ICT and security risks through an independent and objective control function, appropriately segregated from ICT operations processes and not responsible for any internal audit, and an independent internal audit function. It requires financial institutions to maintain updated mapping of their business functions, supporting processes and information assets and to classify them in terms of criticality, based on the confidentiality, integrity and availability of data. Based on this, financial institutions should assess the operational risks related to ICT and the security risks that impact them and should determine what measures are required to mitigate the identified risks.

Section 3.4 sets out requirements for information security to the extent that the information is held on ICT systems. This section defines requirements to implement effective information security measures, including having an information security policy in place; establishing, implementing and testing information security measures; and establishing a training programme for all staff and contractors.

Section 3.5 specifies high-level principles on how ICT operations should be managed, including requirements to improve, when possible, the efficiency of ICT operations; implement logging and monitoring procedures for critical ICT operations; maintain an up

-to-date inventory of their ICT assets; monitor and manage the life cycle of ICT assets; and implement data and ICT systems backup and restoration procedures. Financial institutions should also establish and implement incident and problem management processes.

Section 3.6 describes requirements for ICT project and change 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 the development of applications is carefully monitored from the test phase to the production phase.

Section 3.7 specifies expectations with regard to business continuity management and developing response and recovery plans, including testing, and their consequent updating based on the test 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 ICT business continuity management processes are an integral part of the overall financial institution's business continuity management process and should not be separated.

The last section, Section 3.8, applies only to PSPs for their provision of payment services. 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. The EBA stresses the importance of ensuring transparency, such that PSUs are always aware of which PSP is responsible for providing them with the payment service.

In implementing these guidelines, financial institutions should refer to existing standards and leading best practices. These guidelines intend to be technology and methodology agnostic.

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 and security risks related to financial institutions' processes and services.

These guidelines complement and should be read in conjunction with the supervisory assessment to the applicable institutions in the EBA Guidelines on ICT risk assessment under the Supervisory Review and Evaluation Process (EBA/GL/2017/05), which are addressed to supervisors, as well as other relevant guidelines such as the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02).

Next steps

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.

2. Background and rationale

1. ICT risks can pose significant adverse prudential risks, potentially compromising a financial institution's viability. For this reason, ICT and security risk management is fundamental for a financial 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; and (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 regard 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, unless specified otherwise, 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 of PSD2, which were published in December 2017 (EBA/GL/2017/17), and elaborate further on certain topics that contribute to mitigating ICT and security risks in financial institutions. These guidelines therefore contribute to a level playing field for all financial institutions. The guidelines also address the European Commission (the Commission) request set out in the Commission's financial technology (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 and security risks that have increased in recent years. This is due to the increasing digitalisation of the financial sector and the increasing 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, these guidelines implicitly cover the need for cybersecurity within the financial institution's information security measures. While 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

[1] European Commission's FinTech action plan — https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109 — Box 8, point 2.

cyber-attacks have some specific characteristics that 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 is difficult to determine.

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

iii) Third party service providers, vendors and vendors' products may become channels to propagate cyber-attacks; therefore, an interconnected financial institution that has individual low relevance may become vulnerable and a source of risk propagation. Observing the weakest link principle, cybersecurity should not only be a concern for major market participants and critical service providers.

5. The guidelines are compatible with the three lines of defence model, with the ICT operational units being the first line of defence. The guidelines focus in particular on the responsibilities of the management body and the second line of defence (which usually includes the information security function), and, following the public consultation, the structure of the guidelines has been revised to better reflect this focus. It is further clarified that cross-references to the EBA Guidelines on internal governance (EBA/GL/2017/11) are intended to incorporate in these guidelines governance requirements that are (objectively) valid for the purposes of these guidelines. For the avoidance of doubt, references do not change or expand the scope of application of the EBA Guidelines on internal governance.

6. 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 and complexity of the PSPs' and institutions' businesses and the corresponding ICT and security 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.

3. Guidelines

EBA/GL/2019/04

28 November 2019

EBA 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 out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how European Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 and 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 whether they comply or intend to comply with these guidelines, or otherwise, with reasons for non-compliance, by 04/05/2020. 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/2019/04'. 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 the 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 financial institutions (as defined in paragraph 9 below) must take in accordance with Article 74 of the CRD to manage their ICT and security risks for all activities and that payment service providers (PSPs as defined in paragraph 9 below) must take, in accordance with Article 95(1) of PSD2, to manage the operational and security risks (intended as 'ICT and security 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 and security risks within financial institutions (as defined in paragraph 9). For the purposes of these guidelines, the term ICT and security risks addresses the operational and security risks of Article 95 of PSD2 for the provision of payment services.

8. For PSPs (as defined in paragraph 9) these guidelines apply to their provision of payment services, in line with the scope and mandate of Article 95 of PSD2. For institutions (as defined in paragraph 9) these guidelines apply to 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 regard 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 and security 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 information technology (IT) within a reasonable time and with reasonable 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 as 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 event or a series of linked events unplanned by the financial institution that has or will probably have an adverse impact on the integrity, availability, confidentiality and/or authenticity of services.
Senior management	(a) For credit institutions and investment firms, this term has the same meaning as 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 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 appetite	The aggregate level and types of risk that 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 an external audit function.
ICT projects	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.
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 either software or hardware that is found in the business environment.
ICT systems[5]	ICT set-up as part of a mechanism or an interconnecting network that supports the operations of a financial 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, and business and decision support services.

Implementation

Date of application

11. These guidelines apply from 30 June 2020.

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

3.1. 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 account of, the financial institutions' size, their internal organisation, and the nature, scope, complexity and riskiness of the services and products that the financial institutions provide or intend to provide.

3.2. Governance and strategy

3.2.1. Governance

2. The management body should ensure that financial institutions have adequate internal governance and internal control framework in place for their ICT and security risks. The management body should set clear roles and responsibilities for ICT functions, information security risk management, and 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 and their ICT and security risk management processes on an ongoing basis and to ensure the implementation of their ICT strategy. The management body should ensure that the allocated budget is appropriate to fulfil the above. Furthermore, financial institutions should ensure that all staff members, including key function holders, receive appropriate training on ICT and security risks, including on information security, on an annual basis, or more frequently if required (see also Section 3.4.7).
4. The management body has overall accountability 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 and security risks.

3.2.2. 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 and participate in 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 architecture of ICT, including third party dependencies;

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

6. Financial institutions should establish sets of action plans that contain measures to be taken to achieve the objective of the ICT strategy. These should be communicated to all relevant staff (including contractors and 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 processes to monitor and measure the effectiveness of the implementation of their ICT strategy.

3.2.3. Use of third party providers

7. Without prejudice to the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) and Article 19 of 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 of any activity are outsourced, including to group entities, or when using third parties.
8. To ensure continuity of ICT services and ICT systems, financial institutions should ensure that contracts and service level agreements (both for normal circumstances as well as in the event of service disruption — see also Section 3.7.2) with providers (outsourcing providers, group entities, or third party providers) include the following:
    a) appropriate and proportionate information security-related objectives and measures including requirements such as minimum cybersecurity requirements; specifications of the financial institution's data life cycle; any requirements regarding data encryption, network security and security monitoring processes, and the location of data centres;
    b) 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 the security objectives, measures and performance targets of the financial institution.

3.3. ICT and security risk management framework

3.3.1. Organisation and objectives

10. Financial institutions should identify and manage their ICT and security risks. The ICT function(s) in charge of ICT systems, processes and security operations should have appropriate processes and controls in place to ensure that all risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the financial institution's risk appetite and that the projects and systems they deliver and the activities they perform are in compliance with external and internal requirements.
11. Financial institutions should assign the responsibility for managing and overseeing ICT and security risks to a control function, adhering to the requirements of Section 19 of the EBA Guidelines on internal governance (EBA/GL/2017/11). Financial institutions should ensure the

independence and objectivity of this control function by appropriately segregating it from ICT operations processes. This control function should be directly accountable to the management body and responsible for monitoring and controlling adherence to the ICT and security risk management framework. It should ensure that ICT and security risks are identified, measured, assessed, managed, monitored and reported. Financial institutions should ensure that this control function is not responsible for any internal audit.

The internal audit function should, following a risk-based approach, have the capacity to independently review and provide objective assurance of the compliance of all ICT and security-related activities and units of a financial institution with the financial institution's policies and procedures and with external requirements, adhering to the requirements of Section 22 of the EBA Guidelines on internal governance (EBA/GL/2017/11).

12. Financial institutions should define and assign key roles and responsibilities, and relevant reporting lines, for the ICT and security 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 and security risk management framework should include processes in place to:

    a) determine the risk appetite for ICT and security risks, in accordance with the risk appetite of the financial institution;
    b) identify and assess the ICT and security risks to which a financial institution is exposed;
    c) define mitigation measures, including controls, to mitigate ICT and security risks;
    d) monitor the effectiveness of these measures as well as the number of reported incidents, including for PSPs the incidents reported in accordance with Article 96 of PSD2 affecting the ICT-related activities, and take action to correct the measures where necessary;
    e) report to the management body on the ICT and security risks and controls;
    f) identify and assess whether there are any ICT and security risks resulting from any major change in ICT system or ICT services, processes or procedures, and/or after any significant operational or security incident.

14. Financial institutions should ensure that the ICT and security risk management framework is documented, and continuously improved, based on 'lessons learned' during its implementation and monitoring. The ICT and security risk management framework should be approved and reviewed, at least once a year, by the management body.

3.3.2. Identification of functions, processes and assets

15. Financial institutions should identify, establish and maintain updated mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT and security risks.

16. In addition, financial institutions should identify, establish and maintain updated mapping of the information assets supporting their business functions and supporting processes, such as ICT systems, staff, contractors, 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.

3.3.3. Classification and risk assessment

17. Financial institutions should classify the identified business functions, supporting processes and information assets referred to in paragraphs 15 and 16 in terms of criticality.

18. 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. There should be clearly assigned accountability and responsibility for the information assets.

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

20. Financial institutions should identify the ICT and security 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 changes in infrastructure, processes or procedures affecting the business functions, supporting processes or information assets, and consequently the current risk assessment of financial institutions should be updated.

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

3.3.4. Risk mitigation

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

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

3.3.5. Reporting

24. Financial institutions should report risk assessment results to the management body in a clear and timely manner. Such reporting is without prejudice to the obligation of PSPs to provide competent authorities with an updated and comprehensive risk assessment, as laid down in Article 95(2) of Directive (EU) 2015/2366.

3.3.6. Audit

25. A financial institution's governance, systems and processes for its ICT and security risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks and in payments (for PSPs) to provide independent assurance of their

effectiveness to the management body. The auditors should be independent within or from the financial institution. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.

26. A financial institution's 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 and security risks in the financial institution and should be updated regularly.

27. A formal follow-up process including provisions for the timely verification and remediation of critical ICT audit findings should be established.

3.4. Information security

3.4.1. Information security policy

28. Financial institutions should develop and document an information security policy that should define the high-level principles and rules to protect the confidentiality, integrity and availability of financial institutions' and their customers' data and information. For PSPs this policy is identified in the security policy document to be adopted in accordance with Article 5(1)(j) of Directive (EU) 2015/2366. The information security policy should be in line with the financial institution's information security objectives and based on the relevant results of the risk assessment process. The policy should be approved by the management body.

29. The policy should include a description of the main roles and responsibilities of information security management, and it should set out the requirements for staff and contractors, processes and technology in relation to information security, recognising that staff and contractors at all levels have responsibilities in ensuring financial institutions' information security. The policy should ensure the confidentiality, integrity and availability of a financial institution's critical logical and physical assets, resources and sensitive data whether at rest, in transit or in use. The information security policy should be communicated to all staff and contractors of the financial institution.

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

    a) organisation and governance in accordance with paragraphs 10 and 11;
    b) logical security (Section 3.4.2);
    c) physical security (Section 3.4.3);
    d) ICT operations security (Section 3.4.4);
    e) security monitoring (Section 3.4.5);
    f) information security reviews, assessment and testing (Section 3.4.6);
    g) information security training and awareness (Section 3.4.7).

3.4.2. Logical security

31. 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 includes 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 to prevent the allocation of combinations of access rights that may be used to circumvent controls (principle of 'segregation of duties').
    (b) **User accountability:** financial institutions should limit, as much as possible, the use 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 accounts 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:** at a minimum, all activities by privileged users 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 Section 3.3.3, without prejudice to the retention requirements set out in EU and national law. A financial institution should use this information to facilitate the identification and investigation of anomalous activities that have been detected in the provision of services.
    (e) **Access management:** access rights should be granted, withdrawn or modified in a timely manner, according to predefined approval workflows that involve the business owner of the information being accessed (information asset owner). In the case of termination of employment, access rights should be promptly withdrawn.
    (f) **Access recertification:** access rights should be periodically reviewed to ensure that users do not possess excessive privileges and that access rights are withdrawn 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, information or the process being accessed. This should, at a minimum, include complex passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk.

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

3.4.3. Physical security

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

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

35. 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.

3.4.4. ICT operations security

36. Financial institutions should implement procedures to prevent the occurrence of security issues in ICT systems and ICT services and should minimise their impact on ICT service delivery. These procedures should include the following measures:

    a) identification of potential vulnerabilities, which should be evaluated and remediated by ensuring that software and firmware are up to date, including the software provided by financial institutions to their internal and external users, by deploying critical security patches or by implementing compensating controls;
    b) implementation of secure configuration baselines of all network components;
    c) implementation of network segmentation, data loss prevention systems and the encryption of network traffic (in accordance with the data classification);
    d) implementation of protection of endpoints including servers, workstations and mobile devices; financial institutions should evaluate whether endpoints meet the security standards defined by them before they are granted access to the corporate network;
    e) ensuring that mechanisms are in place to verify the integrity of software, firmware and data;
    f) encryption of data at rest and in transit (in accordance with the data classification).

37. Furthermore, on an ongoing 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.

3.4.5. Security monitoring

38. 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;
c) potential internal and external threats.

39. Financial institutions should establish and implement processes and organisation structures to identify and constantly monitor security threats that could materially affect their abilities 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, for instance to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and should check for corresponding new security updates.

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

3.4.6. Information security reviews, assessment and testing

41. Financial institutions should perform a variety of information security reviews, assessments and testing to ensure the effective identification of vulnerabilities in their ICT systems and ICT services. For instance, 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 consider good practices such as source code reviews, vulnerability assessments, penetration tests and red team exercises.

42. Financial institutions should establish and implement an information security testing framework that validates the robustness and effectiveness of their information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and ICT and security risk assessment process.

43. 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 who are not involved in the development of the information security measures;
b) include vulnerability scans and penetration tests (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems.

44. Financial institutions should perform ongoing and repeated tests of the security measures. For all critical ICT systems (paragraph 17), these tests should be performed at least on an annual basis and, for PSPs, they will be part of the comprehensive assessment of the security risks

related to the payment services they provide, in accordance with Article 95(2) of PSD2. Non-critical systems should be tested regularly using a risk-based approach, but at least every 3 years.

45. 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.

46. Financial institutions should monitor and evaluate the results of the security tests and update their security measures accordingly without undue delays in the case of critical ICT systems.

47. For PSPs, the testing framework should also encompass the security measures relevant to (1) payment terminals and devices used for the provision of payment services, (2) payment terminals and devices used for authenticating the payment service users (PSU), and (3) devices and software provided by the PSP to the PSU to generate/receive an authentication code.

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

3.4.7. Information security training and awareness

49. Financial institutions should establish a training programme, including periodic security awareness programmes, for all staff and contractors 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 and how to address information security-related risks. Financial institutions should ensure that the training programme provides training for all staff members and contractors at least annually.

3.5. ICT operations management

50. Financial institutions should manage their ICT operations based on documented and implemented processes and procedures (which, for PSPs, include the security policy document in accordance with Article 5(1)(j) of PSD2) that are approved by the management body. This set of documents should define how financial institutions operate, monitor and control their ICT systems and services, including the documenting of critical ICT operations and should enable financial institutions to maintain up-to-date ICT asset inventory.

51. Financial institutions should ensure that performance of their ICT operations is aligned to their business requirements. Financial institutions should maintain and improve, when possible, efficiency of their ICT operations, including but not limited to the need to consider how to minimise potential errors arising from the execution of manual tasks.

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

53. Financial institutions should maintain an up-to-date inventory of their ICT assets (including ICT systems, network devices, databases, etc.). The ICT asset inventory should store 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.

54. 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.

55. Financial institutions should monitor and manage the life cycles of ICT assets, to ensure that they continue to meet and support business and risk management requirements. Financial institutions should monitor whether their ICT assets are supported by their external or internal vendors and developers and whether all relevant patches and upgrades are applied based on documented processes. The risks stemming from outdated or unsupported ICT assets should be assessed and mitigated.

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

57. 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 out in line with business recovery requirements and the criticality of the data and the ICT systems and evaluated according to the performed risk assessment. Testing of the backup and restoration procedures should be undertaken on a periodic basis.

58. Financial institutions should ensure that data and ICT system backups are stored securely and are sufficiently remote from the primary site so they are not exposed to the same risks.

3.5.1 ICT incident and problem management

59. Financial institutions should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and to enable financial institutions to continue or resume, in a timely manner, critical business functions and processes when disruptions occur. Financial institutions should determine appropriate criteria and thresholds for classifying events as operational or security incidents, as set out in the 'Definitions' section of these guidelines, as well as early warning indicators that should serve as alerts to enable early detection of these incidents. Such criteria and thresholds, for PSPs, are without prejudice to the classification of major incidents in accordance with Article 96 of PSD2 and the Guidelines on major incident reporting under PSD2 (EBA/GL/2017/10).

60. To minimise the impact of adverse events and enable timely recovery, financial institutions should establish appropriate processes and organisational structures to ensure a consistent and integrated monitoring, handling and follow-up of operational and security incidents and to make sure that the root causes are identified and eliminated to prevent 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;

b) the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber-attacks);
c) problem management procedures to identify, analyse and solve the root cause behind one or more incidents — a financial institution should analyse operational or security incidents likely to affect the financial institution that have been identified or have occurred within and/or outside the organisation and 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 — also covering 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 the event of significant incidents and, at least, informed of the impact, the response and the additional controls to be defined as a result of the incidents.
e) incident response procedures 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 in order to:
    i) collaborate with relevant stakeholders to effectively respond to and recover from the incident;
    ii) provide timely information to external parties (e.g. customers, other market participants, the supervisory authority) as appropriate and in line with an applicable regulation.

3.6. ICT project and change management

3.6.1. ICT project management

61. A financial institution should implement a programme and/or a project governance process that defines roles, responsibilities and accountabilities to effectively support the implementation of the ICT strategy.

62. A financial institution should appropriately monitor and mitigate risks deriving from their portfolio of ICT projects (programme management), considering also risks that may result from interdependencies between different projects and from dependencies of multiple projects on the same resources and/or expertise.

63. A financial institution should establish and implement an ICT project management policy that includes as a minimum:

    a) project objectives;

    b) roles and responsibilities;

    c) a project risk assessment;

    d) a project plan, timeframe and steps;

e) key milestones;

f) change management requirements.

64. The ICT project management policy should ensure that information security requirements are analysed and approved by a function that is independent from the development function.

65. A financial institution should ensure that all areas impacted by an ICT project are represented in the project team and that the project team has the knowledge required to ensure secure and successful project implementation.

66. The establishment and progress of ICT projects and their associated risks should be reported to the management body, individually or in aggregation, 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.

3.6.2. ICT systems acquisition and development

67. Financial institutions should develop and implement a process governing the acquisition, development and maintenance of ICT systems. This process should be designed using a risk-based approach.

68. A financial institution 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 and approved by the relevant business management.

69. A financial institution should ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.

70. Financial institutions should have a methodology in place for testing and approval of ICT systems prior to their first use. This methodology should consider the criticality of business processes and assets. The testing should ensure that new ICT systems perform as intended. They should also use test environments that adequately reflect the production environment.

71. Financial institutions should test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.

72. A financial institution should implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Specifically, a financial institution should ensure the segregation of production environments from development, testing and other non-production environments. A financial institution should ensure the integrity and confidentiality of production data in non-production environments. Access to production data is restricted to authorised users.

73. Financial institutions should implement measures to protect the integrity of the source codes of ICT systems that are developed in-house. They should also document the development, implementation, operation and/or configuration of the ICT systems comprehensively to reduce any unnecessary dependency on subject matter experts. The documentation of the ICT system should contain, where applicable, at least user documentation, technical system documentation and operating procedures.

74. A financial institution's 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 the ICT organisation (e.g. end user computing applications) using a risk-based approach. The financial institution should maintain a register of these applications that support critical business functions or processes.

3.6.3. ICT change management

75. Financial institutions should establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner. Financial institutions should handle the changes during emergencies (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards.

76. Financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require the adoption of additional measures to mitigate the risks involved. These changes should be in accordance with the financial institutions' formal change management process.

3.7. Business continuity management

77. Financial institutions should establish a sound business continuity management (BCM) process to maximise their abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption in line with Article 85(2) of Directive 2013/36/EU and Title VI of the EBA Guidelines on internal governance (EBA/GL/2017/11).

3.7.1. Business impact analysis

78. As part of sound business continuity management, financial institutions should conduct business impact analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (e.g. third party provider data relevant to a business process or publicly available data that may be relevant to the BIA) and scenario analysis. The BIA should also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies, in accordance with Section 3.3.3.

79. 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.

3.7.2. Business continuity planning

80. Based on their BIAs, financial institutions should establish plans to ensure business continuity (business continuity plans, BCPs), which should be documented and approved by their management bodies. 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.

81. Financial institutions should put BCPs in place to ensure that they can react appropriately to potential failure scenarios and that they are able to recover the operations of their critical business activities after disruptions 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 it is acceptable for data to be lost in the event of an incident). In cases of severe business disruption that trigger specific business continuity plans, financial institutions should prioritise business continuity actions using risk-based approach, which can be based on the risk assessments carried out under Section 3.3.3. For PSPs this may include, for example, facilitating the further processing of critical transactions while remediation efforts continue.

82. A financial institution should consider a range of different scenarios in its BCP, including extreme but plausible ones to which it might be exposed, including a cyber-attack scenario, and it should assess the potential impact that such scenarios might have. Based on these scenarios, a financial institution should describe how the continuity of ICT systems and services, as well as the financial institution's information security, are ensured.

3.7.3. Response and recovery plans

83. Based on the BIAs (paragraph 78) and plausible scenarios (paragraph 82), financial institutions should develop response and recovery plans. These plans should specify what conditions may prompt activation of the plans 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.

84. 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 and on 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 the event of an emergency;
    c) be updated in line with lessons learned from incidents, tests, new risks identified and threats, and changed recovery objectives and priorities.

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

86. Furthermore, as part of the response and recovery plans, a financial institution should consider and implement continuity measures to mitigate failures of third party providers, which are of key importance for a financial institution's ICT service continuity (in line with the provisions of

the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) regarding business continuity plans).

3.7.4. Testing of plans

87. Financial institutions should test their BCPs periodically. In particular, they should ensure that the BCPs of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually, in accordance with paragraph 89.

88. 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 RTOs and RPOs) and/or changes in business functions, supporting processes and information assets, should also be considered, where relevant, as a basis for updating the BCPs.

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

    a) include testing of an adequate set of severe but plausible scenarios including those considered for the development of the BCPs (as well as 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 they can be run in this way for a sufficiently representative period of time and that normal functioning can be restored 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 and contractors, ICT systems and ICT services to respond adequately to the scenarios defined in paragraph 89(a).

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

3.7.5. Crisis communications

91. 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 authorities when required by national regulations, and also relevant providers (outsourcing providers, group entities, or third party providers) are informed in a timely and appropriate manner.

3.8. Payment service user relationship management

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

93. 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.

94. 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.

95. 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.

96. 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 accounts.

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

98. 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.

4. Accompanying documents

4.1. 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 are to 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

The complexity of ICT risks is increasing and the frequency of ICT-related incidents (including cyber incidents) is rising, together with their potential significant adverse impacts on the operational functioning of financial institutions. Moreover, due to the interconnectedness of financial institutions, ICT-related incidents risk causing potential systemic impacts.

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 European Central Bank (ECB) identified various threats and vulnerabilities that PSPs are currently exposed to when providing their payment services. The most common risks are:

i. inadequate protection of communication channels used for payments;
ii. inadequately secured ICT systems used for payments;
iii. unsafe behaviour of users and PSPs;
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 are 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 for competing in the financial market through 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;
ii. the increasing reliance on third parties for ICT services and products, often in the form of diverse packaged solutions and resulting in manifold dependencies and potential constraints and concentration risks.

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

a) Guidelines on ICT risk assessment under the supervisory review and evaluation process (SREP), addressed to competent authorities (EBA/GL/2017/05);

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 that are PSPs the existing guidelines do not address ICT and security risks from their other activities. Furthermore, the guidelines in point (b) do not apply to investment firms. The new Guidelines on ICT and security risk 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' 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 for 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 pieces of legislation related to ICT and security risk management:

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 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

[7] European Commission's FinTech action plan: for a more competitive and innovative European financial sector, 8 March 2018, COM(2018) 109 final.

the general provisions and application of scoring as part of the SREP assessment of risks to capital, assessment of institutions' governance and strategies on ICT, and the assessment of institutions' ICT and security 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 PSPs should implement to mitigate operational and security risks derived from the provision of payment services, which in practice relate 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 and security risk management addressed only to credit institutions and investment firms, and maintain 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 to the 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 sets of guidelines would have significant overlap and would create confusion for credit institutions which already apply the Guidelines on security measures for their payment services. This then means 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. Therefore, it would also reduce the compliance burden for institutions, which will then need to refer to a single legal text for their requirements on ICT and security risk management, irrespective

of the service they provide. In addition, it can still take into account any specificities in the ICT and security 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 detailed and prescriptive requirements on ICT and security risk management could increase comparability and create a level playing field across financial institutions. However, this option risks requirements becoming obsolete very quickly due to the ever-changing nature of ICT and security risks. A financial institution would be unable to ensure that its ICT and security risk management properly mitigates ICT and security 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 processes to new challenges and developments. Therefore, this option reflects financial institutions' needs to anticipate and mitigate unknown types of ICT and security risks.

Option 2b is retained.

4.2. Feedback on the public consultation

Summary of responses to the consultation and the EBA's analysis

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
General comment — implementation	One respondent commented on the implementation of the guidelines, suggesting to add to Section 'background and rationale'[8], about how the supervision of the implementation of the guidelines is envisaged (e.g. possible role for the competent authorities). One respondent expressed concerns relating to the impact of these guidelines on third party providers (TPPs), given the open banking facility in PSD2. Their concerns relate to how each competent authority will comply with these guidelines, as a possible restrictive interpretation could introduce barriers to entry, impact the number of TPPs and negatively affect the growth of open banking. Moreover, it was noted that the guidelines can be interpreted liberally or restrictively by competent authorities. This could result in new entrants requesting authorisation and licence from jurisdictions with a less restrictive interpretation of the guidelines for the provision of their cross-border services. Consequently, consumers may be exposed to different ICT security levels and risks. The need for a more legally binding text (i.e. a level 1 text) was also proposed by the same respondent. The respondent noted the possibility of the 'deceptive' implementation of the guidelines by institutions and therefore called for sanctions to enforce the implementation of the guidelines. This is to avoid a situation where, in a potential fraud case caused by a TPP, consumers may blame the banks for exposing them to loss of reputation and credibility, as the banks hold the client relationship. Sanctions could be a useful tool for supervisors to protect customers and financial services. They also suggested introducing and applying industry standards (such as an open	In line with EBA standard practice, the guidelines do not cover implementation aspects in detail. Any practical questions can be addressed through the EBA Single Rulebook Q&A facility or through bilateral discussions with competent authorities. The EBA guidelines are principle based. Any specification of details would create a situation in which one size does not fit all institutions. Furthermore, the EBA guidelines are technology and methodology neutral, with an expectation for institutions to focus on their security, based on a robust process (Section 3.3), instead of on detailed compliance aspects.	No change.

[8] Section numbers and paragraph numbers in this column relate to the numbering in the draft guidelines.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	application programming interface (API)) and industry solutions (such as the PSD2 hub), which can embrace technology and ensure adequate security, while maintaining minimum security standards acceptable to the industry.		
General comment — principles vs rules in the guidelines	A few comments were received on the guidelines being principle based versus being rules based. Some respondents supported and encouraged the EBA's use of the principle-based approach, commenting that this is essential and should be maintained as far as possible. Specifically the focus on outcomes that allow firms to demonstrate capabilities was cited as increasing consistency. This approach ensures that the guidelines can be implemented with proportionality in mind. Principle-based guidance also provides the flexibility required for the continuously evolving nature of technology risks and avoids prescriptive and detailed requirements that may become obsolete over time. This would increase consistency and alignment with the Bank for International Settlements (BIS) Committee on Payments and Market Infrastructures (CPMI) International Organisation of Securities Commissions (IOSCO) guidance 'Cyber resilience for financial market infrastructures'. Where more detailed guidance is provided, the EBA should consider separating these out as examples or use cases, such as how the three lines of defence could be implemented to provide examples of how the requirements could apply or be interpreted. Other respondents considered that some requirements in the guidelines are too prescriptive and too detailed and are thereby limiting the risk management options available to financial institutions (such as governance structures, internal controls and other security-related measures). This was considered to put at risk the ability of the guidelines to withstand the rapid nature of changes in the ICT and information security risk landscape in the years to come. It might also ultimately limit	The EBA agrees with a principle- based approach, and the guidelines are drafted with this explicit intention. The EBA intends to ensure that the guidelines are principle based and flexible enough to facilitate their application to all the relevant institutions in the sector. Furthermore, it is important to ensure that the guidelines remain valid in the continuously evolving technological environment. The EBA's aim is not to be overly prescriptive but to cover the main important areas of ICT and security risk management. In several parts the detailed points are drafted as examples to be considered. That said, a number of specific points have been amended based on the current supervisory insights for future developments in ICT and security risk management maturity.	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	financial institutions' abilities to innovate within the information and cybersecurity domain. One respondent noted that a departure from the existing recognised standards increases regulatory complexity and requires resources to be diverted from other activities, inhibiting firms from focusing their efforts on the identification of and protection against technological risks, thus increasing the amount of firms' resources that are focusing on compliance rather than on technological security. This respondent recommended the international harmonisation of ICT rules in the EU and globally, as diverging regulatory requirements will significantly increase operating costs and will introduce risks of regulatory arbitrage.	The guidelines do not aim to promote one set of standards over another. The EBA agrees with the need to harmonise regulatory requirements and finds that these guidelines are sufficiently principle based that they do not contradict existing standards.	No change.
General comment — risk-based approach	One respondent suggested that a risk-based approach should be adopted in these guidelines, especially where controls are mentioned.	This is taken on a case-by-case basis throughout the guidelines; however, in general the guidelines are to be applied proportionately, taking into account the risks that the financial institutions are exposed to.	Changes made on a case-by-case basis.
Standardisation of all ICT guidelines	One respondent commented that the guidelines seem to separate the 'business' and 'IT' functions within an organisation, thus not taking into account new configurations, represented particularly by FinTech start-ups. It was further commented that new developments in ICT seem to be ignored, such as cloud computing and distributed ledger technology (DLT), along with the issues of end-to-end data encryption in the course of data processing; access to data, which conflicts with banking confidentiality (General Data Protection Regulation, GDPR), management of ICT security in the form of internal outsourcing, etc. The same respondent understood that the objective of these guidelines was to integrate and standardise all ICT guidelines (in force and under implementation), taking into account relevant national guidelines.	The guidelines cover ICT from a holistic business point of view, using the overall business strategy and business processes as a starting point. If new entrants are primarily technology driven, business strategy and ICT strategy will coincide, but this does not change the expectations on formulating and approving such strategies. The guidelines are technology agnostic. It is up to an institution to ensure that appropriate security measures are implemented, e.g. by using new technologies or by leveraging more traditional technologies. The EBA cannot specify all details or all technologies.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		The guidelines do not replace any ICT-relevant guidelines from EU law, but they clarify and harmonise the supervisory expectations following from CRD IV, Article 74, and PSD2, Article 95 (1). Some issues are not addressed in these guidelines because there already exist EU-level regulations and guidelines on these topics (e.g. data-related questions are regulated in the GDPR, and cloud security is also handled in the EBA Guidelines on outsourcing).	
Reference to international standards	Some respondents proposed that the guidelines are linked — where relevant — to European and international practices/requirements/standards/regulations relating to ICT risk management that are already in place. Examples include (1) the Financial Stability Board (FSB) Cyber Lexicon, (2) the Basel Committee's 'Principles for the sound management of operational risk', (3) the FSB's 'Guidance on arrangements to support operational continuity in resolution, (4) the EBA's 'Guidelines on outsourcing', (5) the ECB's 'Cyber resilience oversight expectations for financial market infrastructures', and (6) International Organization for Standardization (ISO) 27001/2 for controls and ISO 27005 for risk management. Without an explicit reference or a gap analysis, it is currently not clear how the guidelines overlap or complement the existing standards in place. In addition, overly general guidelines are open to interpretation both by organisations and by supervisors in each Member State, and references to existing standards will ease harmonisation across Member States and provide assistance in the consistent interpretation of requirements. One respondent commented that the guidelines do not mention any international standard and appear to be a stand-alone best practice for the whole sector. However, much of the guidelines work should be (or should already have been) taken from international standards (e.g. ISO)	The aim of EBA was to ensure that these guidelines are technology and methodology agnostic and do not prescribe any particular international standards or stand-alone good practices. It would not be feasible for the EBA to mention all the existing standards and regulations in the text of the guidelines. However, in the executive summary, the EBA highlights the two main regulations (PSD2 and CRD IV) as these guidelines elaborate how to comply with their requirements. Furthermore, the executive summary has been amended with references to the existing EBA guidelines. The ECB cyber resilience oversight expectations for financial market infrastructures are aligned with these guidelines, but the main difference is in their scope, as the ECB cyber resilience oversight expectations specify details for financial market infrastructures, while these guidelines apply to institutions. The EBA considers that keeping these guidelines principle based allows them to be applied by all kinds	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	and tailored to the financial institution environment. This respondent considers that this would have allowed a more tailored, thorough, consistent, tested and adopted approach to have been defined for financial institutions, which would have less difficulty in the adoption and implementation of these guidelines.	of institutions in the sector. However, this means that institutions and supervisors need to interpret and tailor the guidelines for a specific case.	
Reference to existing EBA guidelines	A few respondents requested an explanation of the relationship between the Guidelines on ICT risk assessment under the supervisory review and evaluation process (EBA/GL/2017/05) and these draft guidelines (preferably with a mapping between the requirements if possible). A request was made to reference the existing guidelines in these new guidelines.	The EBA has amended the executive summary with references to existing EBA guidelines that are relevant to these guidelines. The Guidelines on ICT risk assessment under the supervisory review and evaluation process (EBA/GL/2017/05) are addressed to competent authorities, while these guidelines are addressed to financial institutions. For these guidelines to add value it was agreed not to do a direct mapping of the requirements but to word them in a way that makes it easier for the financial institutions to read over and apply them. These guidelines are directed at financial institutions and cover ICT and security risk management from a holistic perspective. In particular, the definition of ICT and security risk details that this covers data confidentiality, integrity and availability. This is also found in other definitions, such as of incidents, and is included in processes such as the classification and risk assessment process. The aspect of data integrity, therefore, is fully integrated into the entire guideline, instead of being dealt with as a specific risk type. In contrast, the EBA/GL/2017/05 guidelines are directed at supervisors. Since the supervisory	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		assessment depends on information provided by financial institutions, data integrity has been highlighted as a specific topic, not because data integrity is more important or specific as a risk type, but because of the impact on the subsequent assessment of all risks (including data confidentiality and data availability).	
	Another respondent highlighted that these draft guidelines do not address the data Integrity risk from EBA/GL/2017/05. Even if all financial institutions are not subject to the Basel Committee on Banking Supervision's principles for effective risk data aggregation and risk reporting (BCBS 239 principles), this is a key risk for financial institutions. The respondent requested clarification on why this theme/risk is not within the scope of the draft guidelines.	The EBA agrees with the importance of data integrity risks; therefore, the EBA has amended the document to include the data integrity risk as one of the risks that institutions should manage.	The guidelines have been amended.
Section 1: responding to the consultation — data protection	One respondent suggested that this section should be replaced with the new regulation, Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.	This comment has been accommodated; however, this section has been removed from the final guidelines, as it was used only for the consultation.	The guidelines have been amended.
Compliance and reporting obligations — reporting requirements	One respondent proposed that the guidelines should better clarify the difference between compliance and intent/intention to comply. Intention to comply does not equal compliance. Also, there is a typo: 'intend' should be 'intent'.	Compliance and intent to comply are mentioned in the EBA Regulation, Regulation (EU) No 1093/2010. Further information can be found here: https://eba.europa.eu/about-us/legal-framework/compliance-with-eba-regulatory-products. We expect that competent authorities giving intention to comply should provide a date by which they will comply. There is no typo.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Subject matter, scope of application and definitions	Paragraphs 6, 7, 8 should be amended to reflect the correct paragraph number that they reference '… as defined in paragraph 9 …' (instead of paragraph 8).	The final guidelines have been updated with the final accurate references.	The guidelines have been amended.
Subject matter, scope and definitions — addressees	A question was received on the addressees about why these guidelines (EBA/CP/2018/15) are addressed to institutions related to PSD2, while the Guidelines on ICT risk assessment under the supervisory review and evaluation process (EBA/GL/2017/05) have a broader scope. If an entity is not related to PSD2, will the EBA/GL/2017/05 guidelines continue to apply? If an entity is related to PSD2, are both guidelines going to apply, or only this last one (EBA/CP/2018/15)?	The addressees of the EBA guideline — the subject of the consultation (EBA/CP/2018/15) — are not only the institutions related to PSD2, but a broader range of institutions under the EBA remit (e.g. investment firms and other activities of the credit institutions). These guidelines do not repeal the Guidelines on ICT risk assessment under the supervisory review and evaluation process (EBA/GL/2017/05), so they both should be applied according to their scope/addressees. Note that EBA/GL/2017/05 is intended for supervisors, not financial institutions. The EBA expects that if financial institutions implement the Guidelines on ICT and security risk management, providing supervisors with the input required for EBA/GL/2017/05 should not lead to undue burdens.	No change.
Definitions — general	A few comments were received recommending that the definitions are aligned as far as possible with the definitions within international publications on technology and cybersecurity risks such as the FSB Cyber Lexicon and the ECB cyber resilience oversight expectations (CROE) or to use standard definitions (e.g. from control objectives for information and related technology (COBIT), ISO, etc.) where possible.	The comments regarding each of the definitions have been taken on a case-by-case basis and are described for each definition below.	See below.
Definitions	ICT risk – one respondent recommended applying the concept of probability, as there is a likelihood of any kind of impact.	The current definition mentions expected loss, which is the result of the probability of loss times the expected impact. Furthermore, this definition brings together	

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		the existing definition from the EBA Guidelines on common procedures and methodologies for SREP and stress testing (EBA/GL/2014/13 consolidated version) and the definition of security risk from the EBA Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) (EBA/GL/2017/17); therefore, no change is required.	No change.
	Another respondent asked for clarification of the use of the terms ICT risk, security risk and cyber risk in the document. In particular, when ICT risk is meant to include security/cyber risk.	As specified in the scope of these guidelines (paragraph 7), for the purposes of these guidelines, the term ICT and security risk addresses the operational and security risks of Article 95 of PSD2 (including cyber risk).	No change.
Definitions	Management body — one respondent commented that the definition could be supplemented with a reference to paragraph 8 of the Guidelines on internal governance (EBA/GL/2017/11). Other respondents commented that there are different management body structures and responsibilities in the EU jurisdictions and that the definition should be clarified if this refers to the Board of Directors or the executive management of the bank.	The definition of 'management body' references level 1 legislation and the EBA does not consider that there is a need to specify this further.	No change.
Definitions	Operational or security incident — a few respondents suggested using just the word 'incident', which would allow it to be aligned with the FSB Cyber Lexicon definition of 'incident'. A further comment was received that the current wording describes a risk and not an operational or security incident. Another comment suggested revising the wording, as 'continuity' is already included in the definition of 'availability' and is therefore considered redundant. Another respondent suggested deleting the text '~~*…systems and…*~~' from the definition, as 'ICT system continuity' has been covered by	The wording 'operational or security incident' is purposefully used to address the requirements of Article 95 of PSD2, and also 'incident' has a wider meaning in the financial sector. The definition describes an event not a risk. The terms has been revised to be in line with the definition used in the EBA Guidelines on security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) (EBA/GL/2017/17).	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	'availability' mentioned one line above, whereas 'ICT services continuity' can refer to third party providers' services outsourced by the financial institutions.	The EBA concurs that the word continuity is redundant.	The guidelines have been amended.
Definitions	Risk tolerance — some respondents suggested using 'risk appetite', which is more common. The use of 'risk appetite' would also be consistent with other EBA guidelines (e.g. SREP, internal governance). Furthermore, one respondent explained that risk tolerance is understood as the variability regarding the established risk appetite that the organisation can accept under some circumstances. They commented that risk appetite can consider the aggregate level of risk as a medium value of the addition of risks in the organisation, and not only their addition. One suggestion to overcome this was to add this term into the text (hence, risk tolerance or risk appetite). Another respondent commented that, in relation to paragraph 13a), 'risk tolerance' is a term used in connection with the investments, whereas the whole document is about ICT-related risks, so they suggested providing more details relating to ICT in the definition.	The EBA agrees to change the definition to 'risk appetite', to coincide with the use of this in the EBA Guidelines on internal governance (EBA/GL/2017/11), the Guidelines on the revised common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing (EBA/GL/2014/13) and the Guidelines on security measures for operational and security risks (EBA/GL/2017/17).	The guidelines have been amended.
Definitions	ICT projects — comments suggested that the definition should refer to ICT projects' 'end of life' or 'removal' as part of wider ICT and business transformation programmes, while a suggestion was received to add the word 'dismissed' to refer to this same notion, as the removal of ICT systems should be treated with the same caution as that given to their change, replacement or implementation. Another respondent commented that the definition is too wide and suggested shortening it to 'Any project where ICT systems and services are changed, replaced or implemented. ICT projects can be part of wider ICT or business transformation programmes.'	The EBA considers that shortening the definition would adversely impact the intention of the definition; however, it is reasonable to add the phrase 'dismissed' to the definition. Adding this completes the definition.	The guidelines have been amended.
Definitions	Information asset — revised wording was suggested, as it is difficult to know what is worth protecting, so it would be better explained using		

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	the following definition: '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.'** A further comment was received in which it was suggested that the wording 'that is worth protecting' should be the outcome of the risk analysis, as an information asset may be significantly relevant for the functioning of the organisation but not worth protecting due to the cost of implementing security measures (tangible or intangible costs). Another respondent suggested changing the definition to 'information, data and tools required for the processing thereof, which can either belong to the company or be stored under bailment (e.g. personal data).' The respondent considers that mentioning 'tools' is significant, as all measures taken on the protection of information are tightly related to the tools (e.g. user rights), while leaving the definition only as 'pure data' makes things philosophical and removes the connection to reality, where data does not exist by itself but is always under the management of some tools. Another respondent suggested harmonising this definition with the wording in paragraph 17.	The definition of 'information asset' derives from the definition of 'asset' in the FSB Cyber Lexicon, but is clarified to refer specifically to 'information assets', as both 'information' and 'ICT assets' are defined in these guidelines, whereas the FSB Cyber Lexicon was not specific.	No change.
Definitions	ICT asset — a proposal was received to consider the use of the similar definition of 'asset' from the FSB Cyber Lexicon reference. Another suggestion was received to clarify the wording to 'an asset **either** ~~of~~ software ~~and~~ **or** hardware, that is found in the business environment'.	See the above explanation regarding 'information asset'. The explanation has been clarified in accordance with the comment received.	The guidelines have been amended.
New definitions suggested		The EBA considers that all definitions used follow existing legislation and industry standards as appropriate. However the aim of the EBA is to ensure that these guidelines are technology and methodology	

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		agnostic and do not prescribe any particular international standards or stand-alone good practices. In particular:	
	New definitions were suggested for the following: 1) 'structured data' to include in the guideline: 'Structured data are information that is structured systematically, which typically includes information within IT applications and database records structured according to a data model, as for example a relational or hierarchical schema'. 2) 'project implementation leadership' — paragraph 66. 3) 'adequate knowledge' — paragraph 70. 4) 'information security function' to clarify if this means the chief information security office (CISO) (paragraph 32). 5) 'information security standards' in paragraph 44. 6) 'business-managed applications' in paragraph 80. 7) 'urgent or emergency ICT changes' in paragraph 81(e). 8) 'asset owner' in paragraph 19, because entities/institutions' complexities can be very different.	1) As this phrase is not used anywhere in the guidelines, there is no need for the definition. Furthermore, the guidelines deal with structured and unstructured data; therefore, the EBA considers it inappropriate to single out structured data. 2) 'Project implementation leadership' is used in the text in its general meaning. There is no need to specify its meaning. 3) 'Adequate knowledge' has no special meaning in this text. The knowledge should be proportionate to what it relates to. 4) 'Information security function' has already been made clear in the text from the context and the responsibility associated with it. The intention is not to be too prescriptive about the roles and responsibilities for this function; therefore, the EBA does not want to explicitly link it to the CISO. After considering all feedback received, paragraphs 32 and 33 have been removed. 5) 'Information security standards' refers to any applicable and relevant information security standards. The EBA does not see the need to list specific standards. 6) 'Business-managed applications' were mentioned in paragraph 80 only as an example. The EBA does not want to explain and define the examples that are used	No change. No change. No change. The guidelines have been clarified. No change. The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		to support the understanding of the guidelines; therefore, the EBA deleted this example from the text. 7) 'Urgent or emergency ICT changes' has been removed from the guidelines (paragraph 81); therefore, there is no need to define it in the text. 8) 'Asset owner' has been removed from the text. In paragraph 18 the text has been amended and updated to '*There should be clearly assigned accountability and responsibility for the information assets*.'	The guidelines have been amended. The guidelines have been amended.
Proportionality	One respondent asked that additional wording be added in order to be clear on the obligation of all addressees to comply with the new guidelines. This new wording should set out that proportionality cannot be understood as grounds for exemption and that all addressees should address and manage their ICT and security risks. One respondent asked that proportionate application or implementation according to the individual risk situation should be made possible. One respondent commented that, although appropriate, the principle of proportionality may lead to financial institutions excluding the implementation of security controls, based solely on cost factors. The principle of proportionality must be closely monitored by the management bodies (or even the regulator) that will issue the relevant guidelines. Hence, the respondent suggested considering the amendment of Section 4.1 and its association with Section 4.2.1. Another respondent suggested including a more comprehensive set of principles governing the proportionate application, or a differentiation between minimum requirements and those that could be applied proportionately, in order for institutions to achieve compliance with competent authorities' needs.	All EBA guidelines must be applied proportionately by all those to whom these guidelines are addressed (see 'Addressees'). Proportional application is specified in paragraph 1 of the guidelines (see Section 3.1). Compliance with the provisions will be monitored by competent authorities. The basis of proportionality is specified in this paragraph. Competent authorities have the responsibility of monitoring proportionate application. In line with paragraph 1 the EBA expects that competent authorities take into account the institution's risk profile.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	Another suggested that 'proportionality' is better expressed as 'a graded approach' according to the specific context, objectives, conditions and needs of financial institutions. The respondent suggested that it is appropriate to set minimum criteria (factors) to be taken into account and proposed the following for paragraph 4.1: ***'The management body should apply the graded approach to comply with the provisions set out in these guidelines in such a way that is proportionate to, and takes account of, at least the following factors: a) security significance of the financial institution and its parts, b) the financial institution's size and complexity, c) internal organisation, d) the nature, scope, complexity and riskiness of the services and products that the financial institutions provide or intend to provide, e) the strategy and the goals. The factors used to grade the development and application of the guidelines shall be documented.'***	These are principle-based guidelines that, as explained in paragraph 1 of the guidelines (see Section 3.1), should be applied by all institutions in a proportionate manner. The application of these guidelines is not for competent authorities' needs but for institutions to ensure that they manage their ICT and security risks proportionately. Furthermore using a graded approach would limit the implementation of principle-based guidelines and it is the right of the management body to establish proportionate application.	
	Another respondent commented that adapting to the requirements in the guidelines could be a significant problem for organisations operating on a small scale, such as cooperative banks, payment services institutions and FinTech start-ups. The application of the principle of proportionality should be clarified to specify which aspects are important for these organisations and which are not. This applies particularly to countries where 'gold-plating' occurs. This can lead to other negative outcomes, such as the migration of payment institutions to more 'liberal' countries.	These guidelines will be applied for more services and by more addressees than the Guidelines on security measures for operational and security risk under PSD2 (EBA/GL/2017/17). It is important that the guidelines are 'size neutral' and are applicable to all addressees. All institutions must apply all the guidelines in a proportionate manner based on paragraph 1 (see Section 3.1).	
4.2. ICT governance and strategy	Some respondents commented on the management body's roles, specifically requesting that it is specified that the executive function of the management body deals with the ICT function and strategy but that the accountability of the executive function (the Executive Board) should focus on risk strategy and risk appetite and should challenge decisions of the ICT function. Therefore, the Executive Board's	The guidelines intend to place the responsibility and accountability with the management body, in particular regarding strategy and governance due, which is in line with paragraphs 23(a) and 23(b) of the EBA Guidelines on internal governance (EBA/GL/2017/11).	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	responsibilities should be amended in the guidelines (in paragraph 4) to permit delegation where appropriate, e.g. in implementing processes. The need for the management body to approve specific risk-type policies should also be reconsidered. One respondent elaborated concerns that the drafting would significantly expand the management body's obligations to include the day-to-day activities regarding the design and implementation of ICT governance and strategy. This level of granularity is not considered necessary, given that the management body discharges its obligation to ensure that an adequate control framework is in place, as detailed in paragraph 2. Another respondent proposed replacing 'management body' with 'senior management body', making reference to governance and mentioning the activity of 'ensuring'. The respondent suggested promoting a view of ICT corporate governance and, by definition, that the responsibility of governance belongs to the Executive Board while the responsibility of management belongs to the management body. Another respondent suggested that the management body should have at least one expert in the information security/ICT risks field in order to properly execute governance.	Paragraph 4 states that the oversight of implementation is for the management body, which is in line with paragraph 23 of the EBA Guidelines on internal governance (EBA/GL/2017/11). In addition, the EBA does not state that the management body should formulate and draft the policies but considers that the general ICT and security risk management framework and information security framework is of such particular importance that it should be approved periodically at the highest level. The term management body is used in line with the EBA Guidelines on internal governance (EBA/GL/2017/11). The guidelines do not prescribe the composition (or part of it) of the management body. The EBA does not see a need to promote and define the ICT corporate governance into the management body. The guidelines allow for implementation by all institutions (according to their size or mandate).	
4.2.1. ICT governance	Paragraph 2 specifies that the management body is required to set roles and responsibilities for information security risk and business continuity, not only for ICT risks. The question is rather what chapter 4.2.1 covers and should the chapter title reflect this, i.e. is it only ICT risk or also information security risk and business continuity?	Business continuity and information security are addressed in the guidelines in the context of ICT. This is specified in the wording in Section 3.2.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	One respondent suggested deleting the requirement for a sustainable budget for setting an adequate internal governance and control framework (paragraph 3). The respondent fully supported supervisors' expectations to ensure an appropriate budget for an institution to meet its requirements on ICT governance and also agreed on having an overall sustainable budget, which is, in their understanding, to maintain the ability for an institution to (1) meet its current as well as expected future financial obligations and (2) sustain growth, both primarily through current or past income. Nevertheless, the respondent questioned the requirement for having a sustainable budget for such a limited scope as ICT governance, particularly as the support of operational needs and the implementation of risk management processes is associated with costs and not directly related to income.	The comment has been accepted.	The guidelines have been amended.
4.2.1. Governance	The concept of 'key roles' in paragraph 3 is considered vague by some respondents, as it relates to training, and all staff should receive information security training. One respondent commented that the wording contradicts the principle in paragraph 30 of chapter 4.4.1, where it states that the information security policy should apply to all employees, and in paragraph 52 of chapter 4.4.8, where training applies to all employees. Others wanted to receive more detail about what are considered 'staff members occupying key roles'. One respondent suggested clarifying that the requirement for quantity and skills of staff specifies that it is for relevant staff, as, in banks, only part of the staff is responsible for performing the tasks listed. Heightening the awareness of all staff is already addressed in, for example, paragraph 54. The new wording suggested is ' …the quantity and skills of financial institutions' **relevant** staff is adequate …'	The EBA agrees with the need for information security training for all staff members and in particular for key function holders in the institution. The guidelines have been updated to state that training is necessary for all staff including key function holders. Key function holder has a meaning as set out in the EBA Guidelines on internal governance (EBA/GL/2017/11). Furthermore, financial institutions should ensure that on an annual basis, or more frequently if required, all staff members including key function holders receive appropriate training on ICT and security risks, including on information security.	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
4.2.1. Paragraph 4	One respondent suggested drafting changes to paragraph 4, as the obligations set out cover a level of activity that would in their view reasonably be approved and overseen at a level below the management body: 'The management body has overall **accountability** ~~responsibility~~ for **ensuring an effective risk management framework for ICT risks is in place, including ensuring there is an identified individual or forum within the organisation is responsible** for setting, approving and overseeing the implementation of that framework. ~~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.~~ Another respondent suggested after *'management of ICT risks'* adding the following new text: '**as the integral part of overall business risk management process**.'	The EBA agrees with the suggestion that the management body is accountable for and not responsible for ensuring the effective risk management framework. The text has been amended. Other wording in this paragraph remains the same in order to remain in line with the EBA Guidelines on internal governance (EBA GL/2017/11).	The guidelines have been amended.
4.2.1. Governance	One respondent commented that some requirements related to ICT security operating models (roles, responsibilities, reporting lines and mechanisms) could be included.	The intention is to stay 'size neutral' and allow proportional application; therefore, such a level of detail is not necessary.	No change.
4.2.2. Strategy Paragraph 5(a)	One respondent suggested adding 'compliance with applicable laws and regulations' as a further component of the ICT strategy, as non-compliance signifies a business risk (and associated provisions in the business strategy). Another respondent suggested adding in the first line 'to effectively support **and participate in their business strategy**'. This reflects the role of ICT as an integral part of processes, not only as a support function	The EBA does not see a need to prescribe the need for compliance with applicable laws and regulations in these guidelines, as it is already prescribed in all of the laws and regulations. The EBA agrees that it is important to highlight the importance and functions of ICT on creating and implementing a company's business strategy.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	that is involved in the late stages of already established processes and procedures.	Therefore the EBA has amended the text according to the suggestion.	The guidelines have been amended.
4.2.2. Strategy Paragraph 5(c) — components of ICT strategy	One respondent commented that there should be room for a separate information security strategy as long as there is a clear connection to the ICT strategy — this relates to paragraph 5(c) where it is specified that the ICT strategy should contain information security objectives. Another respondent asked if ICT assets should be added here (i.e. software and hardware — for example licences, redundant hardware, up-to-date software and hardware, etc.) Another respondent suggested adding at the end of the sentence '**in line with general security and governance policies established in organisation**'. The text should also include the alignment of the ICT strategy with innovation, to avoid disruption and to support lean digital transformation that is based on ICT architecture. It should also include the proper portfolio of changes to align ICT transformation in accordance with business transformation.	The guidelines do not prohibit the establishment of a separate information security strategy; they state only that there must be information security objectives in the company's ICT strategy. According to this, the guidelines do not mention the issue of the separate information security strategy, so there is a possibility for any institution to have a separate information security strategy, as long as it is in line with the information security objectives of the ICT strategy. All ICT assets are covered by the current wording; therefore, there is no need to specifically mention them at this point. According to the EBA, it is important that the security policies and ICT strategy must be aligned with each other and with any innovation. This suggestion is covered in paragraph 4, which mentions 'ICT strategy as part of their overall business strategy'. Therefore, there is no need to introduce the suggested text in the guidelines again.	No change. No change. No change.
4.2.2. Strategy Paragraph 6 — action plans to support the ICT strategy	Two comments were received on the concept of 'action plans' in paragraph 6, which are said to support the ICT strategy. One respondent said that the term 'action plans' seems vague, and there is a request to clarify what is meant by 'action plans' and the associated expectations. Could they be articulated as either initiatives, projects, programmes or an implementation programme supported by an action plan (priorities, deadlines, resources, etc.)? Another respondent suggested the	The EBA agrees that the previous wording was a little inaccurate and that a detailed, clarified text could help institutions to implement the guidelines. Therefore the comments regarding action plans have been accommodated, to clarify the intention.	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	following wording: 'Financial institutions should establish a set of **measures to be taken to achieve the objectives of** ~~action plans to support~~ the ICT strategy,... ~~The action plans~~ **These measures** should be periodically reviewed to ensure their relevance….'.		
	One respondent commented that instead of 'should be periodically reviewed', the review should be performed and validated on a management committee level to ensure alignment with the overall business strategy.	The EBA does not consider this proposal too detailed or unnecessary.	No change.
4.2.3. Use of third party providers (reference to the EBA Guidelines on outsourcing arrangements)	One respondent commented that addressing requirements across two different sets of guidelines (these and the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)) could create uncertainty about the applicable requirements or lead to differences in the interpretation by different competent authorities about how each document is translated and implemented. Other respondents suggested leaving this section out, partially or completely, to avoid any confusion with the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) and to avoid fragmentation of requirements and inconsistencies across the services, activities and functions being outsourced. Another respondent requested a clear alignment with the requirements set out in the EBA Guidelines on outsourcing arrangements, as it remains unclear if it is necessary to differentiate between parent entities based in another Member State and parent entities based in a third country. Another respondent requested clarification on the relation (if any) between the concept of 'appropriate and proportionate security objectives and measures' in these guidelines and the classification of outsourcing (as critical or not critical) proposed by the EBA Guidelines on outsourcing.	The guidelines specify some requirements that address the specificities of ICT and security risk when outsourcing and using third parties and complement the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02); therefore, this section is deemed to add value by giving information about security requirements. The requirements apply to the addressees of the EBA Guidelines for any outsourcing or use of third parties, regardless of where the parent entity is. There is no contradiction or particular relation between these guidelines and the distinction of critical or	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		important functions in the EBA Guidelines on outsourcing arrangements.	
4.2.3. Use of third party providers	One respondent asked for consistency in requirements across the sectors because 'intragroup' would include insurance companies, and in the event that a financial institution's ICT serves multiple subsidiaries, it would be complex to have different security controls on different subsidiaries.	To create the necessary requirements for other sectors, is the responsibility of the other European Supervisory Authorities (ESAs). Therefore, it is not possible for the EBA to define cross-sectoral requirements that must be applied in all of the sectors. However the ESAs liaise closely on this topic in order to be aligned in their approaches.	No change.
Paragraph 7	A question was received asking if the measures set out in these guidelines should be included in the outsourcing risk assessments whenever the outsourced service is related to payment services. One respondent proposed the following changes to clarify that the provision of services by third parties should not trigger the EBA Guidelines on outsourcing arrangements: *'[…] including the measures set out in these guidelines, when* ***important*** *operational functions of payment services and/or ICT services and ICT systems are outsourced, including to group entities****, or when using third parties****.'.* With regard to the wording *'financial institutions should ensure the effectiveness of the risk-mitigating measures as defined by their risk management framework',* one respondent suggested that the risk management framework of each institution could be enhanced through a common risk management framework, such as the one already established by the ECB — i.e. risk assessment questions of the ECB for outsourcing providers. This common framework will help to ensure consistency among all institutions. There was a request to clarify that group entities are covered only to the extent applicable in line with current vendor risk obligations and	The EBA considers that the measures in these guidelines should be included in the outsourcing risk assessments, as these general principles need to be applied when outsourcing. The scope of the EBA Guidelines on outsourcing arrangements is clearly specified in those guidelines. The intention of this section is to ensure that ICT and security risks are covered not only when outsourcing but also when using third parties. The EBA does not support the suggested modification in the wording. The option of using third parties is an important issue, and it is important to keep it in this point. The intention is not to specify one risk management framework over another. The guidelines are principle based.	No change. No change. No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	intragroup service controls, i.e.: 'ICT systems, are outsourced, including, **to the extent applicable,** to group entities…')	The requirements of the guidelines must be applied to any intragroup outsourcing, without any limitation or lightening; therefore, the EBA considers there is no need to specify or clarify the text.	No change.
Paragraphs 7 and 8	Requests for clarification were received for the specific use of the wording 'critical or important' in both paragraphs 7 and 8, to align with the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02), i.e. 'when critical or important operational functions…'. In particular, one respondent suggested limiting paragraph 8 to (critical or important) outsourcing of ICT services and ICT systems, as otherwise the principle of proportionality and the draft guidelines' objective to focus on risk might be contradicted. This is because they consider that the minimum contractual content outlined in paragraph 8 is too extensive for the entirety of the potential ICT-related services or systems procured from third parties. Rather, the assessment of the necessity for specific contractual requirements should be within the responsibility of the institution, whereas, in line with the principle of proportionality, necessity should be risk based.	The suggested wording (to add 'critical or important' operational functions) is not necessary, as the guidelines apply for any outsourced service or system, and it is the company's right to determine whether it is critical or important, based on its proportionality. The guidelines are risk based and proportionality is already specified in the guidelines. Furthermore the Guidelines on outsourcing arrangements set out the guidance for critical and important outsourcing.	No change. No change.
Paragraph 8	The following requests for clarification on paragraph 8 were received: (i) Paragraph 8: suggested rewording to clarify the sentence '…ensure that contracts ~~and service level agreements~~ with the provider (**third party** outsourcing provider **or** group entity~~, or third party provider)~~…' (ii) Paragraph 8(a): 'appropriate and proportionate information security-**related** ~~objectives and~~ measures, including requirements such as minimum cybersecurity requirements'. The wording 'information security-related objectives' is not clear, so the respondent suggests using 'measures' alone. Also 'appropriate and proportionate information security objectives, **ICT risks** and measures […]'	(i) The EBA considers that it is important to keep service level agreement (SLA) in the text; however, the wording has been clarified. (ii) The EBA agrees with the suggestion.	No change. The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	(iii) Paragraph 8(a): the terms 'minimum cybersecurity requirements' and 'data life cycle' are considered to be vague, and there was also a suggestion that these terms should be removed and that the first part of this section is enough: 'appropriate and proportionate information security objectives and measures...'.	(iii) 'Minimum cybersecurity requirements' and 'data life cycle' already exist in other ICT standards, so no change is needed.	No change.
	(iv) Paragraph 8(b): one respondent commented that service level agreements are currently only available on continuity, but there should also be agreements on vulnerability management/patching, as well as on release management of system security items such as antivirus patterns/engines. Another proposed redrafting was 'Service-level agreements, **key performance indicators, reporting or other adequate measures** to ensure continuity of **business-critical** ICT services and ICT systems and performance targets under normal circumstances as well as those provided by **business continuity or** contingency plans…'.	(iv) The suggested supplement is not necessary, as the current text covers all of the suggestions on other points: patching and vulnerability management in paragraph 8(a), key performance indicator (KPI) in paragraph 8(a), and reporting in paragraph 8(c) and paragraph 9. The text has been amended by moving part of paragraph 8(b) into paragraph 8.	The guidelines have been amended.
	(v) One respondent suggested including a new paragraph 8(d): '**The right to audit the provider to validate compliance of the requirements established in the contract.**'	(v) The EBA considers that it is not necessary to add the new paragraph, as this is included in the EBA Guidelines on outsourcing.	No change.
Paragraph 8	One respondent suggested that the use of KPIs to monitor compliance of the outsourcing provider to the SLA provisions, as well as key risk indicators (KRIs) for outsourcing provider evaluation purposes could benefit financial institutions. Generic KPIs and KRIs could be provided to ensure consistency among financial institutions, at least to a certain degree, since other laws and regulations may impose diverse requirements. Such generic KRIs could include certifications of the outsourcing provider against ISO 27001:2013, the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) and/or STAR certification (for cloud providers). This will also assist the implementation of paragraph 9 below *('Financial institutions should monitor and seek assurance on the*	There is no intention to prescribe the use of KPIs and KRIs to monitor compliance, as this would be too detailed. Therefore, the EBA aims to keep the text as it is and retain the opportunity for institutions to decide how they want to fulfil the guidelines.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	level of compliance of these providers with their security objectives, measures and performance targets.').		
	One respondent provided a second sentence to clarify the wording in paragraph 9: '**For the avoidance of doubt, contractual obligations concerning intragroup service relationships can be satisfied by binding group information security policies applicable to the servicing group entity covering such requirements.'**	The suggestion is considered too prescriptive. The addition of the suggested new sentence would limit the regulation, and it would be necessary to apply this provision also to intragroup service relationships.	No change.
Paragraph 9	Another respondent commented that the particular assurance is better to be specified. For the security measures, a system and organisation controls (SOC)2 type II security attestation by an independent assessor could be provided. Without explicitly stating compliance assurance, service providers can never move in the right direction. Similarly, another respondent suggested mentioning some examples of internationally accepted standards and certifications (e.g. certifications to standards in the ISO/International Electrotechnical Commission (IEC) 27000 family and the International Standard on Assurance Engagements (ISAE) 3402 type II certification).	The EBA does not consider that there is a need to specify such standards (e.g. SOC2), as the guidelines are principle based.	No change.
Paragraph 9	One respondent suggested limiting the applicability of paragraph 9 to 'where considered appropriate in terms of related risks', i.e. in the case of (material) outsourcings, as it considered the requirement to 'seek assurance on the level of compliance of ICT service or system providers with their security objectives, measures and performance targets' too prescriptive and inexpedient. Monitoring and potential assurance of compliance should be appropriate to the service or system's relevance and the risk it poses, whereas the assessment of associated risks is conducted by means of various mandatory risk assessments, e.g. outsourcing risk assessments, vendor risk assessments and information security risk assessments. The costs associated with a mandatory assurance of compliance of the entirety of ICT service or system	The EBA considers that the guidelines follow a risk-based approach and therefore consider that this is already included.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	providers, irrespective of their relevance and risk, are excessive, compared with the potential associated benefits of such mandatory assurance of compliance.		
Paragraph 9	One respondent suggested at the end of the sentence to add '**on a regular basis with remediation plans created and implemented based on findings obtained by monitoring and testing**'.	The EBA expects that monitoring is done on a regular basis. The general concept is already in the text, so it is already expected that an institution would act based on its findings.	No change.
4.2.3. Use of third party providers	The use cloud services and related specific governance (CSA, etc.), taking into account the different implementation models (SaaS, PaaS, public cloud, hybrid, etc.) and assurance mechanisms, should be highlighted in this chapter as being increasingly important third party service providers.	This is already included and regulated in the EBA Guidelines on outsourcing, so there is no need to have this specification here also.	No change.
4.2.3. Third party providers — data centres	One respondent suggested that data centres supporting financial institution operations should possess or adhere to internationally recognised certifications, controlled by independent auditors. There are a number of standards that greatly contribute to data centre security and that could be included in the text: a minimum tier 3 level of redundancy of the data centre infrastructure ensures the continuity of operations; the ISO 27001 standard certifies the quality of an information security management system, guaranteeing the confidentiality and availability of data; the ISO 14001 standard specifies requirements for an effective environmental management system; the ISO 9001 standard ensures effective quality management, providing a systematic approach to maintaining and improving customer experience; ISAE 3000 type 2 and ISAE 3402 type 2 reports ensure adequate risk management, quality and reliability of internal processes; ISAE 3000 focuses on operational management; and ISAE 3402 focuses on financial reporting.	The EBA agrees with the concept and points that were suggested, but these would be too detailed for the general purpose of these guidelines.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	Furthermore, the respondent recommended applying the following criteria to enhance the physical security of data centres: a safe location; the use of a minimum of two data centres, connected to different power grids to diversify risks; data servers to be stored separately from any other customers; and a controlled access system to the data centre needs to be in force that requires identity verification.		
4.3.1. Organisation and objectives	One respondent suggested the adoption of a well-recognised security management framework.	The adoption of a well-recognised security management framework is too limiting with regard to the ICT and security risk management of financial institutions.	No change.
4.3.1. Organisation and objectives relating to ICT risk management framework	Comments were received on the specification in the text of the three lines of defence (3LoD) model, with a request that the model for implementation should not be specified, particularly as this is considered to move away from the guidelines being 'principle based'. The focus should be on ensuring an effective internal risk management and control model. This would be, for example, just a clear description of what duties and responsibilities reside with the respective lines of defence, on an overall level. This description should be in line with EBA/GL/2017/11 Guidelines on internal governance under Directive 2013/36/EU. One respondent also highlighted that there is no consistent industry standard for the 3LoD model, whereby the model is implemented by institutions in accordance with their size, structure and complexity. This has resulted in the allocation of information security roles to the first or second line of defence not being consistent in industry. The view was also that the objectives of the guidelines are met without the need to disrupt the existing enterprise risk management practices. One respondent said that banks should not be forced to manage ICT risks differently from the rest of their risks. Others said that this guidance may be deemed useful for smaller, less mature institutions but not for well-established institutions that already meet existing	Financial institutions have to manage their ICT and security risks according to their general obligations on risk management set forth in EBA/GL/2017/11 Guidelines on internal governance under Directive 2013/36/EU. Based on the feedback received, the guidelines have been amended to follow the 'principle-based' approach. Paragraphs 10 and 11 have been revised to ensure appropriate segregation of ICT operations, control, and internal audit functions, while paragraphs 32 and 33 have been removed. The revised guidelines do not explicitly refer to the 3LoD model and do not prescribe to financial institutions how to implement the 3LoD model for ICT and security risk management purposes. These guidelines do not assign specific roles to each of the three lines of defence, but describe the responsibilities of each. The EBA considers that these guidelines are now compatible with the 3LoD model, with the ICT	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	regulations. Meanwhile another respondent commented that the 3LoD requirement can be difficult for smaller companies to meet, as they may not have enough people with adequate technical skills or the information security background outside ICT support teams (second line). One of these respondents suggested the following wording in paragraph 10: 'Financial institutions should identify and manage their ICT risks according to ~~**the three lines of defence model**~~ **an effective internal risk management and control model, including an independent risk control function, to identify and manage these risks**.' One respondent proposed changes in paragraph 11: '… in charge of ICT systems, processes and security operations, **which could be** acting 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) One respondent suggested consistently using the term 'financial institutions' throughout these guidelines, instead of mentioning the appropriate department or level (including the 3LoD) where the responsibility for a specific requirement lies. In addition, the respondent suggested adjusting the wording for the three lines of defence in paragraphs 11, 13, 27, 32 and 33, as the three lines of defence are not described clearly and consistently.	operational units being the first line of defence. The guidelines now focus in particular on the responsibilities of the management body and the second line of defence control function (which usually includes the information security function). Cross-references to the EBA Guidelines on internal governance (EBA/GL/2017/11) added to paragraphs 10 and 11 are intended to incorporate in these guidelines governance requirements that are (objectively) valid for the purposes of these guidelines. For the avoidance of doubt, references do not change or expand the scope of the application of the EBA Guidelines on internal governance. Based on the feedback received, reference to the 3LoD model has been removed. Instead paragraphs 10 and 11 have been revised to ensure the appropriate segregation of ICT operations, control, and internal audit functions. Based on the feedback received, the guidelines have been amended to follow the 'principle-based' approach. The text has been amended for clarification and alignment with the EBA/GL/2017/11 Guidelines on internal governance under Directive 2013/36/EU — paragraphs 10 and 11 have been revised to ensure the appropriate segregation of ICT operations, control, and internal audit functions. The revised guidelines do not explicitly refer to the 3LoD model — they do not assign specific roles to each of the three lines of defence, but describe the responsibilities of each.	The guidelines have been amended. The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 10	One respondent commented that the distinction in the requirements between financial institutions and PSPs is incomprehensible. PSPs should also follow the 3LoD model and an appropriate internal control function. Another respondent requested clarification of paragraph 11, as in paragraph 10 the use of the 3LoD model is a mandatory requirement, while paragraph 11 seems to leave it optional to manage the ICT risks under this model, using the term 'where the three lines of defence is applied'. However, the respondent requested wording that suggests that the 3LoD model is used but, for reasons of proportionality in small financial institutions, risk management can be done as effectively as necessary under a different approach. It should be more important to create a robust ICT risk management with an independent internal control function than to formally stick to a model. This approach would be especially valuable in situations where, due to head count, the implementation of all three lines of defence would prove to be difficult.	The EBA considers that financial institutions have to manage their ICT and security risks according to their general obligations on risk management set forth in EBA/GL/2017/11 Guidelines on internal governance under Directive 2013/36/EU. Based on the feedback received, the guidelines have been amended to follow the 'principle-based' approach, and paragraphs 10 and 11 have been revised to ensure appropriate segregation of ICT operations, control and internal audit functions. The revised guidelines do not explicitly refer to the 3LoD model and do not prescribe to financial institutions how to implement the 3LoD model for ICT and security risk management purposes.	The guidelines have been amended.
Paragraph 11	One respondent suggested changing the wording in paragraph 11 to 'internal control function should take responsibility of the control of ICT risks'. Currently, according to paragraph 11, an internal control function in the second line of defence should 'take responsibility for the management of ICT risks', but this was considered unclear. The suggestion is to ensure that it is the same as the requirements defined in EBA/GL/2017/11 Guidelines on internal governance under Directive 2013/36/EU, paragraphs 174 to 180 on the risk management function's role in identifying, measuring, assessing, managing, mitigating, monitoring and reporting on risks. Another respondent suggested that where it is mentioned that the second line of defence should take 'responsibility' for the management of ICT risks, this should be replaced with 'accountability', since the responsibility of managing ICT risks during the daily tasks is the first line	Based on the feedback received, the text has been revised and aligned with the wording of the EBA/GL/2017/11 Guidelines on internal governance under Directive 2013/36/EU. The control function should adhere to the requirements of Section 19 of the EBA Guidelines on internal governance (EBA/GL/2017/11). The EBA considers that such change would not be in line with the EBA/GL/2017/11 Guidelines on internal governance under Directive 2013/36/EU.	The guidelines have been amended. No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	of defence. The second line would have an internal control function, but not the responsibility for the daily risk management. Another respondent commented that the internal control function should be in the information security and operational risk management departments, as it is not clear how one single department can manage ICT risks alone. Another respondent commented that the internal control function should be allowed to be organisationally situated outside the ICT department in order to ensure independence and to avoid conflicts of interests.	The EBA considers that one single department does not have to manage ICT and security risks alone. Following the feedback received, the wording of these guidelines has been revised to clarify that the assignment of the responsibilities for managing and overseeing ICT and security risks should adhere to the requirements of Section 19 of the EBA/GL/2017/11 Guidelines on internal governance under Directive 2013/36/EU. The EBA considers that the independence of the control function as the second line of defence is ensured.	The guidelines have been amended. No change.
	Another respondent suggested moving this paragraph to an annex as an example of a potential model framework for certain institutions with less mature risk management functions. Some rewording was suggested here for this purpose: '…acting as the first line of defence, should operate under the ~~**supervision**~~ **oversight** of an internal control function acting as a second line of defence. This internal control function should ~~**take responsibility for the**~~ **independently challenge the first line of defence's** management of ICT risks'. One respondent commented that there may be room to add a fourth level that is provided by a regular external audit — both passive (e.g. SOC2) and active (e.g. red teaming).	Following the feedback received, these guidelines have been revised and the wording of paragraphs 10 and 11 aligned with the wording of the EBA/GL/2017/11 Guidelines on internal governance under Directive 2013/36/EU. The EBA does not recognise a fourth level of defence.	The guidelines have been amended. No change.
Paragraph 12	To ensure consistency when referring to the ICT organisational structure, one respondent suggested that the wording in this paragraph be amended to align with Section 4.2.1 and Section 4.3.2, to include any interdependencies to ICT risks within the organisation. The following wording was suggested: 'this framework should be fully integrated into, and aligned with, financial institutions' overall risk management processes, **including any interdependencies related to the ICT risk**'. A	As the guidelines already mention 'fully integrated', this should also include the interdependencies between areas of risk. The ICT and security risk management framework should be fully integrated into the financial institutions' overall risk management processes.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	request was received to clarify what kind of integrations are expected (e.g. advanced measures approaches — capital reserve, risk appetite framework, etc.).		
Paragraph 13	One respondent recommended that paragraphs 13 and 14 regarding risk management should follow the identification of functions, processes and assets (Section 4.3.2), as business requirements drive risk management actions, and to be in line with Section 4.3.3 paragraphs 21 and 22.	Paragraph 14 specifies documentation requirements in the area of the ICT and security risk management framework. As these requirements are normally specified at the end of the relevant subsection, a change of order is not deemed appropriate	No change.
Paragraph 13(a)	A question was received about what details/criteria are required to determine the risk tolerance to ICT risks. One respondent also suggested providing a list of common risks that should be considered in risk assessment/risk mitigation processes, for instance the unavailability of key staff of financial institutions; the unavailability of data centre facilities (fire, power outage, power from city grid unavailable for 4, 8 or 24 hours); cyber-attack (distributed denial-of-service (DdoS), ransomware); and data leakage (inside job, external attack). (Some of the risks are listed in paragraph 39 in Section 3.2.1, review of the institutions' ICT risk profile in EBA/GL/2017/05).	Risk appetite is already further defined (see section on definitions, page 13). ICT and security risk is defined in the section on definitions. Further guidance is not deemed necessary due to the principle-based approach embedded in the guidelines. In addition, factors for risk tolerance can depend on business process particulars; therefore, the EBA does not intend to provide such details.	No change. No change.
	Another respondent suggested switching paragraphs 13(a) and 13(b) to first identify and assess, and then determine, risk tolerance. Another respondent suggested considering rephrasing paragraph 13(a) as follows: *'a) enable the management to determine an appropriate risk tolerance for ICT risks, […]'.* The respondent stated that paragraph 13 provided a non-exhaustive list of processes to be implemented as part of the ICT risk management framework, including processes for determining the risk tolerance for ICT risk. The respondent noted that the institution's risk management framework contains processes to determine the institution's risk-bearing capacity, based on which the institution's management has to decide on its risk tolerance. The	The EBA agrees that further clarification is appropriate regarding the requirement in paragraph 13(a). Please see also comments above and below.	Paragraph 13(a) has been amended to replace 'tolerance' with 'appetite'.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	respondent argued that the risk framework as such cannot determine the actual risk tolerance. Another respondent commented that the level of risk tolerance or risk threshold defined by the institution could be difficult to determine at this early phase, before measuring the residual (or net) risk level for the institution's ICT risks. It is advisable to define it at the risk mitigation phase (Section 4.3.4) with the pertaining risk acceptance announcement, signed by senior management, on tolerating the residual risk items below the risk tolerance threshold.	See comment above.	
Paragraph 13(c)	One respondent requested the definition of controls compared with mitigation measures, i.e. of the mitigation measures, which ones are considered controls.	Further guidance is not deemed necessary due to the principle-based approach embedded in the regulations.	No change.
Paragraph 13(f)	One respondent suggested that in order to account for a timely mitigation of the risks identified, as well as to track the implementation of mitigating measures, the guidelines should include an additional item (i.e. paragraph 13(f)) to address the aforementioned aspects.	New paragraph 13(f) added: *'identify and assess whether there are any ICT and security risks resulting from any major change in ICT system or ICT services, processes or procedures, and/or after any significant operational or security incident.'*	The guidelines have been amended.
Paragraph 14	One respondent commented that the need for firms to update their ICT risk management framework with 'lessons learned' is fully appreciated. However, the way firms decide to do this may vary. The respondent sought clarification on the implementation of a continuous improvement process. The respondent considered that this is subject to different interpretations, as 'lessons learned' documentation could be inferred as being part of the project closure documentation or being the lessons learned from ICT incidents and outages. In addition, they request clarification on the level of documentation and the level of criticality of the incidents that should be captured in the 'lessons	The EBA sees no need for further clarification on 'lessons learned' and its documentation, due to the overall proportionality principle.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	learned' documentation. Another respondent questioned if the lessons learned should be gathered explicitly in a specific document for that purpose, or if it is enough to add them to the different appropriate documents in an implicit way. Another respondent requested a definition of 'lessons learned' in the ICT risk management framework background.		
Paragraph 15	One respondent considered that the second sentence in paragraph 15 belongs to the list of activities in the ICT risk management framework in paragraph 13.	As this is indeed a role of the ICT and security risk management framework; the guidelines have been amended to include a new paragraph 13 (f).	The guidelines have been amended.
	Furthermore, one respondent commented that the 'ICT risk management framework' contains requirements that are more of an operational nature and do not require approval by the management body. The respondent suggested the revised wording: 'The ICT risk management framework should be ~~approved and~~ reviewed, at least once a year~~, by the management body.~~' This would be in line with EBA Guidelines on internal governance (see Section 17). Another suggested 'The **management body should ensure that the** ICT risk management framework ~~should be~~ **is** approved and reviewed, at least once a year, by the **individual or forum with delegated responsibility for ICT risks.** ~~appropriate management body.'~~ Another respondent stated that an approval is only necessary if there are changes to the ICT risk management framework, as an approval of an unchanged ICT risk management framework is inexpedient.	The first sentence moved under paragraph 14 but with no changes: '*The ICT and security risk management framework should be approved and reviewed, at least once a year, by the management body*.'	The guidelines have been amended.
		The EBA sees no inconsistency with the current text.	No change.
		The EBA sees no inconsistency with the current text.	No change.
	Some respondents commented on the wording 'major change', with one asking for clarification and another asking whether the intention is that the risk evaluation of major changes/information security incidents has to be done formally in the general risk management process and reported to those owners, or whether risk evaluation in the change or information security incident management process is sufficient?	Clarification on 'major changes' is not deemed necessary.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	One respondent suggested that the second sentence be separated out and moved to Section 4.6.3 on ICT change management: **'Financial institutions should …. from this change or incident'.**	The EBA would like to clarify that the first example/option described is in line with the requirement in this guideline.	No change.
	One respondent asked if the ICT risk management framework is one single framework, as there are separate information security and operational risk management frameworks and consolidating the two could create operational inconsistencies.	Risks resulting from these changes are being addressed, therefore it should not be moved to Section 4.6.3.	No change.
		The EBA considers that the term is used as an 'umbrella' term, and that financial institutions can have a few frameworks.	No change.
4.3.2. Identification of functions processes and assets Paragraphs 16 and 17	One respondent commented that the guidelines could refer to the topic of operational resilience to make it consistent with Basel work.	As the work of the Basel Committee on Banking Supervision has not yet been finalised, the EBA prefers not to use this term at the current time.	No change.
	Another respondent suggested that guidance for risk tolerance (thresholds) be specified for mapping business functions, roles and processes, which would lead to a critical or significant ICT risk based on acceptable risk thresholds. However, regarding such thresholds, they recommend that in paragraph 17 only information assets that, when not available, would cause a significant client or sector impact should be required to be mapped. The principle of proportionality and guidance for risk tolerance should be followed.	Further guidance is not deemed necessary due to the principle-based approach embedded in these guidelines.	No change.
	Another respondent suggested mentioning the holistic view of an organisation detailed on an appropriate enterprise architecture to control changes and impacts. They also suggested mentioning data governance to capture and control metadata information in a corporate view that explains and describes organisation data and related risk.	Further guidance is not deemed necessary due to the principle-based approach embedded in the regulations.	No change.
	Another respondent commented that the provision on the minimum and maximum frequency of the review of processes, functions and resources should be elaborated, or a new provision should be added, to	All risk management activities need to be reviewed on a regular basis then only make specific time references when there is a specific reason to do so. Paragraph 14 makes the general statement that this applies to the actual implementation of these procedures. The	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	the effect that such a review is necessary if there are significant changes in resources, infrastructure, systems or processes.	guidelines have been updated to require financial institutions to 'identify, establish and ***maintain updated mapping***'.	
Paragraph 16	One respondent asked whether instead of 'roles', 'information assets' was meant to be used. In addition, it requested a more detailed explanation of the mapping referred to.	'Information assets' was not meant to be used. See also comment below.	No change.
Paragraph 16	There was a suggestion to add that a risk-based approach should be used for the mapping, and that it should leverage language in existing regulations with a potential focus on materiality: 'Financial institutions should identify, establish and regularly update a mapping of their business functions, roles and supporting processes — **using a risk-based approach —** to identify...'. The requirement as it stands would be a challenge and probably not sustainable.	The mapping should include all of a financial institution's business functions, roles, etc. and not use a risk-based approach.	No change.
	One respondent suggested that financial institutions should also make statements concerning the importance of the identification of ICT risks in their organisations. The institutions should then do the mapping of business functions, roles and supporting processes and ICT infrastructures and link these to the ICT risks.	The mapping of the ICT infrastructures is a part of the next step (as in information asset), see paragraph 18.	No change.
Paragraph 17	One respondent suggested that the mapping is done every 3 years. The mapping requirements in the EBA's current drafting seem to indicate that it would be expected of firms to complete a mapping of all functions, across all jurisdictions and legal entities. The respondent therefore also recommends that the EBA clarifies the scope and expectation of firms, to ensure that this is realistically completed, in line with business criticality and firms' risk appetites.	The current wording about the regular update of the mapping is sufficient and provides the proportionality needed. In regard to the information assets there is no differentiation between inter-group or other outsourcing arrangements.	No change.
	With regard to third parties, it is not clear to the respondent if the requirements are in addition to the EBA Guidelines on outsourcing arrangements, in particular relating to inter-group arrangements or fourth parties.	These guidelines and the EBA Guidelines on outsourcing arrangements coexist (see paragraph 7 of these guidelines).	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	Another respondent suggested that ICT assets (software and hardware) and physical necessities (such as buildings, workplaces), both internally provided/owned and from third parties, should be included.	The ICT assets are included in the ICT systems.	No change.
	One respondent suggested that the word 'people' should be replaced by 'organisational function'.	Based on the suggestion and according to EBA/GL/2017/11, 'people' will be replaced by 'staff'.	The guidelines have been amended.
4.3.3. Classification and risk assessment - Paragraph 18	One respondent commented that paragraph 41 of the EBA Guidelines on ICT risk assessment under the supervisory review and evaluation process (EBA/GL/2017/05) outlines conditions for identifying critical ICT systems and services, whereas currently no reference to those guidelines is made. Clarification on this point is also relevant for further paragraphs where criticality is mentioned, such as paragraph 49. Furthermore, the respondent was of the opinion that the costs associated with the classification of supporting processes and information assets in addition to the business functions clearly exceed the potential benefits. It therefore suggested limiting the classification in terms of criticality to business functions only and, if considered necessary, to major supporting processes related to critical business functions. Another respondent requested clarification on the classification of criticality of business functions with reference to areas such as their key roles in the financial statement, the decision-making process, 24/7 customer service (e.g. e-channels), cash withdrawal, money transfer and payment services, risk or compliance-related areas and strategic planning.	Each financial institution needs to define their own level of criticality; therefore, the definition depends on the financial institution. The EBA considers that the result of the classification is to know different levels of criticality; therefore, the lower levels should not be excluded upfront.	No change.
4.3.3. Classification and risk assessment	Some respondents suggested that criticality is defined by regulations/standards, e.g. the payment card industry, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system and	Adding that the regulation requirements is to be considered is too generic. Next to that, regulatory requirements can place expectations/burdens but be not at the same level.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 19	GDPR, and therefore suggested the wording 'consider the confidentiality, integrity, ~~and~~ availability **and regulation** requirements'. One respondent commented that this section should focus on structured data, with the proposed wording '...consider the confidentiality, integrity and availability requirements on structured data'. The respondent also proposed that a definition of 'structured data' should be included in the guidelines (see comments for definitions).	The EBA does not consider this addition necessary.	No change.
Paragraph 20	One respondent did not consider that a review of the classification of the information assets and relevant documentation should be done every time a risk assessment is performed, as this task should be included in other activities. In their view, when a risk assessment takes place, the classification already assigned by the owner of the asset or documentation should be considered to directly determine the possible impact that a risk event could produce.	Such a review needs to be done while the risk assessment is performed.	No change.
Paragraph 21	One respondent was of the opinion that carrying out risk assessments, i.e. classification in terms of criticality, on supporting processes and information assets is generally inappropriate and in particular is too prescriptive. Consequently, the respondent asked that the guidelines limit the applicability of paragraph 21, in particular in the case of the classification of supporting processes and information assets and also for business functions where risk assessments of the aforementioned subjects should be reviewed using a risk-based approach. In line with this, major changes as listed in the second sentence in paragraph 21 or changes in the underlying ICT risks and related ICT systems should trigger a reassessment of risks. One respondent requested that 'business function' is defined. It also suggested that this point should be less restrictive so that different risk management methodologies can be implemented depending on the	See also the comment on paragraph 18. The criticality assessment is done by the financial institution and needs to include the supporting processes and information assets. The work needs to be done extensively for each process. However, if the risk assessment of a particular process shows that the process is not vital/critical, then the supporting information assets can be evaluated in a risk-based process as well. A more extensive risk assessment needs to be done for more important information assets.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	characteristics of the organisation. For a very complex and big organisation, determining the ICT risks to every business function or information asset could be difficult to maintain and is not practical.	The current wording is more general. Defining 'business function' is too restricting in terms of using different risk management methodologies	No change.
	Two respondents asked for the requirement for updates to be more frequent than 1 year to be deleted, i.e. 'This risk assessment should be carried out and documented, annually ~~or at shorter intervals if required~~'. The view was that assessments of ICT risks once a year are sufficient, since a new assessment takes place anyway during the course of the year if there are major changes. Further assessments during the year are not appropriate.	If there is a major change, the risk assessment needs be carried out sooner.	No change.
	Another respondent asked for clarification of or confirmation that this paragraph covers a risk-based approach, referring to 'annually or at shorter intervals, if required'.	The risk assessment for periods of less than a year should be risk based (see also paragraph 1).	No change.
Paragraph 22	A request was received to clarify how financial institutions are expected to monitor threats, as there are many different ways to assess ICT risks, including scenario analysis and the evaluation of threats and controls against information assets. This request was complemented with a suggestion to replace 'risk scenarios impacting them' with '**the ICT risk framework'.**	It is not intended to limit financial institutions in their approaches; therefore, no further clarification is needed.	No change.
	Another respondent suggested additional wording at the end: '**and establish actions and activities in relation to newly discovered risk vectors**'.	The EBA sees no inconsistencies. The mentioned scenarios should be reviewed.	No change.
4.3.4. Risk mitigation	Two respondents suggested that in addition to providing guidance on risk mitigation in the form of a risk mitigation plan the guidelines should clarify the three other 'T's of risk mitigation: transfer (by insurance), tolerate (risk acceptance) and terminate (stop doing the business or ICT process altogether).	No further guidance is needed; this depends on the risk appetites of the different financial institutions.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	One respondent proposed mentioning the role of business process controls to risk mitigation.	No further guidance is deemed necessary, since in the guidelines the business strategy and processes drive the ICT strategy and processes (see paragraph 4).	No change.
4.3.5. Reporting Paragraph 25	Some respondents asked that reporting should be done on an aggregated level on the total ICT risk picture for the financial institution to the management body. The view was that requiring individual risk assessments to be reported to the management body is in many cases irrelevant (the information is too detailed) and would demand disproportionate resources, compared with the outcome.	The level of reporting is not specified and depends on the financial institution.	No change.
	Another respondent said that the management body should have the ability to delegate to an individual or forum, to ensure that its time is not dedicated to reading individual risk reports: '*Risk assessment results should be reported to the* ***~~management body~~*** ***individual or forum with the delegated responsibility for ICT risks*** *in a timely manner.'*	This is not to be delegated.	No change.
	One respondent said that ICT risk reporting should take place as part of a broader risk report to the management body and should not be separated out, as, if it is a top risk, it will be identified.	Paragraph 24 does not require a separated ICT and security risk report.	No change.
	The timely reporting was commented on and it was suggested that it should be set to a specific threshold, as otherwise it leads to subjective implementation (e.g. quarterly or semi-annually), and the reporting to competent authorities should be set to annually. One respondent suggested adding the word '**documented**' before 'reported'.	The requirement to document risk assessment is set in paragraph 20.	No change.
	Furthermore, two comments were received about deleting the second sentence, as the requirement is already dealt with comprehensively by Article 95(2) of Directive (EU) 2015/2366. Double regulation should be avoided.	Because of the scope of these guidelines (PSPs and credit institutions), there is no double regulation.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
4.3.6. Audit Paragraph 26	One respondent suggested that quantitative requirements concerning the minimum and maximum audit frequency should be imposed, provided that the bracket is sufficiently wide (for example, from once a year to once every 3 years), in order to accommodate the specific nature of the operations of any given organisation.	The frequency of such audits is not specified and depends on the financial institution (see paragraph 26).	No change.
	One respondent requested clarification of whether the requirement that *'The auditors should be independent within or from the institution'* excludes the internal audit function. The respondent commented that internal audit is considered as being independent in financial institutions (by any applicable corporate governance model) and should be part of the audit. An external auditor will provide an unbiased opinion; nevertheless, this must also be part of the internal audit responsibilities.	The requirement is based upon the internal audit requirements of the relevant regulations and is deemed sufficient.	No change.
	One respondent considered that the methodology should be periodically updated, to guarantee that it covers requirements related to new trends and changes in the payment ecosystem (cloud platforms, big data, new technologies, new actors in the payment ecosystem, etc.). Therefore, the respondent proposed adding the following sentence: '**The methodology should be periodically updated, to guarantee it considers requirements related to new trends and changes in the payment ecosystem**'.	The requirement is based upon the internal audit requirements of the relevant regulations. Therefore, an amendment is not deemed necessary.	No change.
	One respondent asked for the final sentence ('The frequency and focus of such audits should be commensurate with the relevant ICT risks.) to be replaced by: '**The scope and frequency of the audits should be based on a risk assessment that takes into account the ICT assets supporting the critical business processes, the identified ICT risks, and the prior outcome of ICT and security audits or management reviews**.'	Due to the principle-based approach of the guidelines, a rewording of the last sentence does not seem necessary. It would actually be limiting, since it focuses only on the critical business processes, whereas the audit universe should be more holistic.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 27	One respondent asked to substitute 'approve the audit plan' by '**be informed on the audit plan**', as the audit committee is an independent body within the organisation.	The financial institution's management body's overall responsibility requires an approval of the audit plan. Please refer in this regard also to the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2017/11), paragraph 206.	No change.
Paragraph 28	Two respondents asked that the wording 'security-related' be deleted and stated that the remediation extends to all critical ICT findings, not just to those that are security related, i.e. '..remediation of critical ICT ~~security related~~ audit findings should be established'.	***'**…remediation of critical ICT **~~security related~~** **audit findings** should be established**.'***	The guidelines have been amended.
4.4.1. Information security policy Paragraph 29	One respondent commented that it is unclear on what level in the organisation the information security policy should be ratified. This should be clarified in the requirement.	The guidelines have been clarified and changed to: '***The policy should be approved by the management body***.'	The guidelines have been amended.
	Some respondents said that the wording 'and based on the relevant results of the risk assessment process' should be deleted, since the information security policy establishes the information security objectives and the security framework of the financial institution. These objectives will determine the risk tolerance and how to manage the results of the risk assessment. However, the information security policy is not based on the relevant results of the risk assessment process, as stated in these guidelines. One respondent considered that the wording in paragraph 29 should be changed by adding at the end: ***'It shall take into account regulatory and legal requirements for financial institutions and other legal provisions that affect ICT in general***.'	The EBA considers that the mentioned sentence is essential in order to highlight the interconnectedness of ICT and security risk management and information security.	No change.
	Another respondent suggested removing this paragraph, as this is already covered by Article 5 of Directive 2015/2366 (PSD2), which prescribes the conditions to obtain a licence. One of which is the development of an information and security policy. It further noted that the responsibility for fraud scenarios lies with fraud operations.	As these guidelines are within the scope of the relevant regulations (see section on 'subject matter, scope and definitions'), such a clarification is not deemed necessary. The EBA does not see any inconsistencies.	No change. No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 30	A few respondents requested that the information security policy is not communicated to third parties, with the suggested rewording: *'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 to all employees **of the financial institutions**.'*	Based on the suggestion, the guidelines have been revised in the following manner: *'The information security policy should be communicated **to all staff and contractors of the financial institution** ~~within of the financial institutions and to third parties used by financial institutions, as applicable, and should apply to all employees.~~'*	The guidelines have been amended.
	A suggestion was made to clarify that the components of the policy should be in accordance with the risk tolerance of the financial institution: '[…]*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 EBA considers that components of the policy should be in accordance with the risk appetite and that the proposed rewording is not deemed necessary.	No change.
Paragraph 31	One respondent suggested adding an incident response/management process (see Section 4.5.1)	The EBA considers that the incident response/management process is part of the ICT operations management and is, therefore, covered in these guidelines by Section 3.5.1 ICT incident and problem management.	No change.
	Similarly a comment was received that change and configuration management is one of the major factors affecting information security. It was recommended that change management becomes a separate point in Section 4.4.1, paragraph 31 and that it is linked to Section 4.6.	The EBA considers that the ICT change management is part of ICT project and change management and is, therefore, covered in these guidelines by Section 3.6.3 'ICT change management'.	No change.
Paragraph 31(f) and 31(g)	The order of the last two subsections should be reversed and their section numbers should be adjusted in accordance with the section numbering on pages 22 and 23.	The references have been revised.	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
4.4.2. Information security function Paragraphs 32 and 33	Further to the comments on Section 4.3.1 (paragraph 11), a number of comments were received on the three lines of defence referenced here and called for less prescription in the text, citing examples where the current wording would not be appropriate. Respondents suggested that the idea of clearly segregated lines of defence should remain but without assigning specific roles to each one of them. Specifically the guidelines could include a clear description (in line with EBA/GL/2017/11 Guidelines on internal governance) of what duties and responsibilities reside with the respective lines of defence, on an overall level. Some examples were given by respondents to illustrate their concerns: there are cases where an information security function/unit also includes security operations that are independent from the rest of ICT operations (e.g. firewall administration vs network administration). This segregation ensures that information security is fully independent (in terms of governance, organisation and technology) and cooperates very closely with ICT, but, as an operating model, it effectively creates an overlap between the first and second lines as regards 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. Paragraph 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 and for monitoring its implementation and reporting 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 paragraphs 10 and 11. A revised wording for paragraph 32 was put forward: 'Financial institutions should establish an information security function, with the responsibilit~~ies~~**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~~	Based on the feedback received, the guidelines have been amended to follow a 'principle-based' approach by removing paragraphs 32 and 33, and revising paragraphs 10 and 11. The revised guidelines do not prescribe to financial institutions how to implement the 3LoD model for ICT and security risk management purposes. The EBA considers that these guidelines are now compatible with the 3LoD model, with the ICT operational units being the first line of defence. The guidelines now focus in particular on the responsibilities of the management body and the second line of defence (which usually includes the information security function) and, following the public consultation, the structure of the guidelines has been revised to better reflect this focus. The cross-references to the EBA Guidelines on internal governance (EBA/GL/2017/11) added to paragraphs 10 and 11 are intended to incorporate in these guidelines governance requirements that are (objectively) valid for the purposes of these guidelines. The guidelines have been revised and now do not assign specific roles to each of the three lines of defence but describe the responsibilities of each. Furthermore, the revised guidelines do not explicitly require the establishment of an information security function, with the responsibilities assigned to a designated person, but a reference to the information security function is made in the background section. Based on the feedback received, paragraphs 32 and 33 have been removed. Paragraphs 10 and 11 have been	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	~~the three lines of defence model is applied, this function should be the second line of defence function — see Section 4.3.1~~).' The first change reflects the fact that the accountability of the security function can be assigned to a single person but not all the responsibilities under the security function (some require a role/team). The second change is because it is considered to be too prescriptive to impose a specific operational or organisational model, given that these may vary significantly across financial institutions. The respondents then proposed that if 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 deleted, clarification should be made of the new role of the information security function in relation to the other second level of defence roles.	revised to ensure the appropriate segregation of ICT operations, and control and internal audit functions.	
	Another respondent requested that the requirements in the guidelines (and specifically paragraph 32), for an information security function should focus on its required level of independence rather than on the organisational structure of the financial institution. One respondent requested clarification of the reference to *'… this function should be the second line of defence function'.* The respondent commented that the information security function, in the best case, could be part of the second line of defence but is not the only component of the second line of defence. The respondent also asked if the operational day-to-day activities related to information security would be part of the first line of defence. In addition, the respondent requested clarification of what person (the CISO?) was referenced in *'…with the responsibilities assigned to a designated person'*?	Reference to the information security function in the guidelines has been removed. It is only included in the background section.	The guidelines have been amended.
	Another respondent proposed that the control function should monitor and control the information security function and hence that this person must be located independently of the control function.	Based on the feedback received, paragraphs 32 and 33 have been removed. Paragraphs 10 and 11 have been revised to ensure the appropriate segregation of ICT operations, and control and internal audit functions. Based on the feedback received, paragraphs 32 and 33 have been removed. Paragraphs 10 and 11 have been	The guidelines have been amended. The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	One respondent suggested clarifying that internal audits may be carried out by the second line of defence (information security management system (ISMS) audits) but that they are separate from the internal audit function: 'In accordance with financial institutions' internal governance structure, financial institutions should ensure that the information security function **is not part of the internal audit function**. ~~is not responsible for any internal audit.~~.'	revised to ensure the appropriate segregation of ICT operations and of control and internal audit functions. The EBA considers that the control function should not carry out any internal audit, whereas different kinds of security reviews (penetration testing, etc.) are not meant here.	No change.
	One respondent was of the view that the tasks listed in paragraph 33 should be performed by the first line of defence and that the second line should independently control and report on the effective implementation of those tasks. For instance, awareness and training, risk monitoring controls and reporting are first-line tasks. The second line can complement these through independent monitoring, control and assurance reviews, but it should not diffuse the responsibility of the first line in these areas. Another way to put this is that the second line of defence should perform its required activities also in the risk area of ICT and security risk.	Based on the feedback received, paragraphs 32 and 33 have been removed. Paragraphs 10 and 11 have been revised to ensure the appropriate segregation of ICT operations, control and internal audit functions.	The guidelines have been amended.
4.4.2. Security function Paragraph 32	One respondent commented that having an information security officer as a measure to secure robust ICT risk management is interpreted more as a function that can be carried out by a team representing the information security function as the second line of defence; it should not necessarily mean the appointment of an information security individual. It should be clarified that, with the appointment of an information security officer, the information security function is established. According to proportionality it may be necessary for the information security officer to have a team, but this should be a question of size and the level of risk exposure of the individual financial institution. Another comment suggested that the word 'person' is replaced by 'role, that can be performed by a team or person'.	Based on the feedback received, paragraphs 32 and 33 have been removed. Paragraphs 10 and 11 have been revised to ensure the appropriate segregation of ICT operations, control and internal audit functions.	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 33	One respondent commented that the first line (operational) and second line (information security function) of defence are not described separately and are unclear. For example, in their view, the activity in paragraph 33(d) belongs to the first line of defence (operational management) and is not the responsibility of the information security function. The respondent suggested adjusting the wording of this paragraph to ensure that third party adherence to security requirements is not difficult/infeasible to enforce.	Based on the feedback received, paragraphs 32 and 33 have been removed. The EBA considers that the requirement set in paragraph 33(d) to adhere to the information security requirements when using third parties is covered by Section 3.2.3 'Use of third party providers', paragraph 7.	The guidelines have been amended.
	Another respondent suggested adding a new paragraph 33(f) '**Be involved in all ICT initiatives and projects from their early stages**'. It should also mention software security controls and data masking in the non-production environment.	Based on the feedback received, paragraphs 32 and 33 have been removed. However, the EBA considers that adding such a general task for the information security function might cause conflicts of interest with respect to the monitoring task of the information security functions and its control function.	The guidelines have been amended.
4.4.3. Logical security Paragraph 34	A comment was received to amend paragraph 34 to include that the procedures can be designed according to the criticality of data/systems: 'Financial institutions should define, document and implement procedures for logical access control (identity and access management), **according to the criticality of the information assets and systems**. ….These procedures should, **in principle** ~~at a minimum~~, implement the following elements …'.	Logical access controls have to be implemented, including the elements stated in paragraph 34(a) to (g).	No change.
	Paragraph 34(c): Privileged access rights: A suggestion was received to delete the example, as granting privileged access rights depends on protection needs 'with elevated system access entitlements (~~e.g. administrator accounts~~)'.	The example is intended to provide clarity but is not obligatory.	No change.
	Paragraph 34(d): Logging of user activities: one respondent asked that this paragraph specify what type of privileged user activities should be logged. The objective should be logging of exceptional activities (e.g.	The EBA considers that all privileged user activities should be logged and monitored. Proposed clarification: '***at a minimum, all activities by privileged users*** […]'	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	failed logins, reconciliation breaks) and should distinguish between interactive and non-interactive privileged activities.		
	In paragraph 34(d) there is a reference to retention requirements set out in EU and national law with regard to the period of time for retaining access logs. One respondent suggested that this should be clarified and that the data safeguard requirements should be in line with other regulations that give guidance on retention periods at EU level, e.g. GDPR. Paragraph 34(d): Change to '***F***~~*f*~~*inancial institutions'*.	The EBA considers that no change is needed because retention requirements are set out in EU and national laws.	No change.
	Paragraph 34(e): Access management: new wording was suggested, as access rights are withdrawn, not removed: 'access rights should be granted, ~~removed~~ **withdrawn** or modified in a timely manner'.	The comment has been accommodated.	The guidelines have been amended.
	Paragraph 34(e): one respondent asked for clarification of the definition of 'information asset owner'. Depending on circumstances, an 'information asset owner' could be a person, a tool or a system. The question was raised whether any of these definitions can be accepted. In addition, the respondent asked if the definition in the guidelines was consistent with the definition used in the GDPR. In order to make it easier to understand and create relationships and controls at scale, the respondent suggested using the standardised terminology across legislation (e.g. the GDPR and PSD2).	The comment has been accommodated. The EBA would like to clarify that these guidelines specify requirements for financial institutions, based on the CRD and PSD2. On the contrary, the GDPR concerns the protections of personal data. Consequently, the EBA does not see the necessity for a standardisation of terms in this respect.	The guidelines have been amended. No change.
	34 (e) One respondent suggested additional the wording: *'Access management: access rights should be granted, removed or modified in a timely manner, according to predefined approval workflows involving* ***either the applicant's immediate leader (subject-based approach) and/or*** *the business owner of the information being accessed (information asset owner* ***in an object-based approach****).'*		
	Paragraph 34(f): with regard to *'access rights should be periodically reviewed'* one respondent suggested that the security function can only	Adding this wording would be too detailed and therefore not in line with the principle-based approach	

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	oversee this process, as this will be the responsibility of each business owner.	of these guidelines. The current wording was deemed sufficient.	No change.
	Para 34 (g): Authentication methods: new wording was suggested to avoid multiple interpretations: '[…] This ~~may~~ **should at a minimum** include password complexity requirements ~~and/~~or other authentication methods, based on relevant risk'.	See comment above.	No change.
	Paragraph 34(g): mandatory two-factor authentication to access critical systems is too burdensome and it was suggested to remove it. The respondent agreed that it is more secure, but argued that it should not be mandatory if an adequate privileged access management process is implemented, e.g. New York Department of Financial Services (NYDFS) 23 and New York Codes, Rules and Regulations (NYCRR) 500: 'Based on its risk assessment, each covered entity shall use effective controls, which may include multifactor authentication'. It also questioned whether the two controls for network access are needed for the server and especially with a check against policy. A question was raised about whether the server will lose network connectivity if it is not compliant any more. The respondent suggested that this control should only be applicable for systems in non-secured areas, e.g. clients.	Following feedback received, the guidelines have been amended to reflect a risk-based approach, and two-factor authentication is used as an example: '***This should, at a minimum include complex passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk.***' 'Stronger authentication methods' are not to be confused with 'strong customer authentication (SCA) under PSD2' to be applied by PSPs when carrying out remote electronic transactions. SCA is defined as 'authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.'	The guidelines have been amended.
	Another respondent commented that the provision for password complexity is vague, which could lead to multiple interpretations and therefore that this should be clearer in the text. One respondent suggested the additional wording: '*This may include password **length**, complexity**, password lockout (both time-based and failed attempts-based) policy and expiration period** requirements and/or other authentication methods, based on relevant risk […]*'		

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		The EBA considers that further description would be unduly burdensome and would not be principle based.	No change.
4.4.3. Logical security, 4.4.4. Physical security, 4.4.5. ICT operations security	One respondent appreciated that the requirements on logical security, physical security and ICT operational security follow the content of generally accepted standards such as ISO 27001/02 or the National Institute of Standards and Technology (NIST) cybersecurity framework, as this contributes to harmonising applicable requirements. However, the respondent commented that the draft guidelines deviate from the structure of the aforementioned standards and therefore recommended further alignment to the standards mentioned and structuring them according to security domains or functions to enhance readability.	These guidelines are explicitly intended to be technology and methodology agnostic to allow institutions to leverage on various industry practices. The EBA considers that reference to specific standards is not appropriate.	No change.
4.4.4. Physical security	One respondent suggested a change in title: *'4.4.4. Physical **and environmental** security'*	Physical security encompasses protective measures against environmental hazards; therefore, a change is not deemed necessary.	No change.
4.4.4. Physical security Paragraph 37	There was a suggestion from one respondent to clarify that access to non-public ICT systems should be permitted only for authorised individuals: 'Physical access to **non-public** ICT systems should be permitted only for authorised individuals.' Users of public ICT systems (e.g. automated teller machines (ATMs), information terminals and account statement printers) have physical access to these.	The EBA considers the proposed differentiation not necessary, as it would be an additional source of complexity.	No change.
Data centres	One respondent suggested that data centres that support financial institution operations should possess or adhere to internationally recognised certifications, controlled by independent auditors. These were listed in a comment on Section 4.2.3.	These are interesting security points for data centres, but the EBA considers that such requirements would be too detailed for the purpose of these guidelines.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
4.4.5. ICT operations security Paragraph 39	One respondent commented that this paragraph should encompass a risk-based approach. Furthermore, it recommend prescribing the goals instead of the activities in this paragraph.	The goal of these measures is the prevention of security issues in ICT systems and ICT services and minimising their impact on ICT serve delivery. Therefore, a change as suggested is not deemed necessary.	No change.
	One respondent noted that the chapter starts with an ambition to 'identify potential vulnerabilities' but then continues to describe a set of best practices for ICT security. It recommended that there must be a clearer connection between the identification of the potential vulnerabilities and the actions that must be taken as a consequence of the identified potential vulnerabilities.	The EBA would like to highlight that this paragraph describes measures for implementing procedures to prevent the occurrence of security issues in ICT systems and ICT services. Therefore, the EBA sees the listed measures as appropriate to accomplish these requirements.	No change.
	Another respondent found the list too prescriptive and suggested the revised wording: 'These procedures, **following a risk-based approach,** ~~should~~ **could** include, **for example**, the following measures'. Another respondent provided suggested wording for paragraph 39, specifically: 'Financial institutions should implement procedures to prevent the occurrence of security issues, **particularly** in **critical** ICT systems and ICT services and should minimise their impact on ICT service delivery.'	The EBA does not consider the list as examples but as necessary measures.	No change.
		Due to the interconnectedness of all ICT systems and ICT services, there is a need to observe all security issues.	No change.
	One respondent asked that the wording in paragraph 39(a) is revised and suggested splitting what should be achieved (the outcome) and how it should be achieved (the measures). Suggested wording: 'a) **evaluate and remediate vulnerabilities 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**'. Their view was that currently the wording in paragraph 39(a) on the desired outcome to 'identify potential vulnerabilities' that starts this section is	Vulnerabilities have to be identified before they can be evaluated and remediated; therefore, the EBA considers that no change is needed.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	not addressed in the text that follows. Instead it addresses the remediation of known vulnerabilities. Another said that the critical security patches should be deployed by no later than 1 month.	The EBA considers that the timing of the security patches' deployment depends on their criticality; therefore, no specific time should be prescribed.	No change.
Paragraph 39(b)	From a network security perspective, one respondent said that it might be counterproductive to only require security baselines for certain 'critical network components'. Instead, there should be a framework in place that defines the level or type of security baseline for any given network device, in a risk-based manner. Suggested wording: 'b) secure configuration baselines of all network components such as core routers or switches should be implemented in a risk-based manner;' Another respondent considered that secure configuration baselines should be established not only for critical network components, but also for system components (servers, databases, etc.). Therefore, they proposed adding the following reference: '*Secure configuration baselines of critical network components […]* ***and system components, such as servers and databases***'.	The EBA agrees with the comment and that platform aspects (such as operating systems and databases) should be included. For clarification, the guidelines are revised to include: '*implementation of secure configuration baselines of all network components*'.	The guidelines have been amended.
Paragraph 39(c)	Rewording was suggested to replace 'leakage' with 'loss', as this derives from '*data loss prevention' (DLP) not 'leakage'*, and to add '**detection and response**' to 'data leakage prevention systems'. In addition, a comment was received to say that this requirement seems to indicate that it would be expected of firms to complete this blanket control across all activities and therefore a request was received for clarification of the scope and what was expected of firms. Another respondent commented that this point contains a mixture of different security measures with different purposes. To make this paragraph clearer, they suggest an outcome-based approach, e.g. what is it that should be achieved with network segmentation, DLP and encryption, respectively?	In line with the suggestion 'leakage' has been replaced with 'loss'. This requirement has to be implemented in a proportional manner. Therefore no change is necessary. The goal of the measures is the prevention of security issues in ICT systems and ICT services and minimising	The guidelines have been amended. No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	Another suggested that, because of its utmost importance as being the basis of network defence, 'network encryption' should come first in the list and the 'or' should be changed to 'and', because the combination of all these elements are necessary for an in-depth and multilayer defence mechanism. The wording suggested is *'**the encryption of network traffic,** network segmentation **and** data leakage prevention systems should be implemented;'*	their impact on ICT serve delivery. Therefore, a change as suggested is not deemed necessary. Based on the suggestion, the wording has been changed from '~~or~~' to '**and**'.	No change. The guidelines have been amended.
	One respondent asked if the encryption referred to in paragraphs 39(c) and 39(f) refers to sensitive data only, or if all data had to be encrypted.	It has been clarified that the encryption of network traffic and data should be '**in accordance with the data classification**'.	The guidelines have been amended.
Paragraph 39(d)	One respondent asked for this to be explicitly risk based, with the suggested wording: 'protection of endpoints …should be implemented, **according to risk-based principles**'. One respondent asked if the evaluation of whether an endpoint meets security standards before being granted access to a corporate network includes servers. They asked how this would work in the cloud: will servers lose connectivity, if they are non-compliant?	The EBA considers that no change is needed, as the guidelines follow a principle-based approach. The EBA considers that financial institutions are responsible for all their endpoints, including their outsourcing to the cloud, i.e. to ensure that these also meet the security standards of the institution. Nevertheless, institutions have flexibility, which comes from the 'risk-based' approach that the EBA expects institutions to formulate for themselves.	No change. No change.
Paragraph 39(e)	One respondent proposed an amendment that aims to define the scope of this provision, which in their view could be burdensome and could also have a strong impact on costs: 'to verify the integrity of **critical** software, firmware, and information'. One respondent asked what integrity checking for information would be. Another respondent asked that the requirements should be risk based, as integrity checking is not possible in every ICT system (e.g. appliances): 'financial institutions should ensure that integrity checking	These guidelines should be applied in a manner that is proportionate to the nature, scope and complexity of the financial institution's business and the corresponding ICT and security risks. In line with the suggestion, reference to 'integrity-checking mechanisms' is removed and they are not specified, in order to ensure that these guidelines are	No change. The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	mechanisms are in place to verify the integrity of software, firmware, and information, **where applicable**;'	principle based. Moreover, 'information' was replaced by 'data'.	
Paragraph 39(f)	One respondent proposed additional wording regarding a risk-based approach, as it is not possible to encrypt all 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**.'	The EBA agrees with the arguments expressed. The guidelines have been amended to clarify this: 'encryption of data at rest and in transit ***(in accordance with the data classification)***.'	The guidelines have been amended.
	Others asked for details on which level of encryption will be necessary. In transit, is every file, or only the channel (i.e.(TLS) necessary? At rest, is every file necessary?	These guidelines have been amended to clarify this: 'encryption of data at rest and in transit ***(in accordance with the data classification)***.'	The guidelines have been amended.
	Another respondent suggested clarifying that the requirement should only be on critical or sensitive data, as not all the data needs to be encrypted, i.e. 'encryption of **critical or sensitive** data at rest and in transit.' (i.e. either use critical or sensitive). One respondent highlighted the importance of applying non-obsolete encryption methods and sufficient key length. New wording suggested: *'**only non-obsolete** encryption **methods and sufficient key length should be used for encrypting** data at rest and in transit.'*	These guidelines have been amended to clarify this: 'encryption of data at rest and in transit ***(in accordance with the data classification)***.'	The guidelines have been amended.
		The EBA considers that implementing these suggestions would be unduly burdensome and not be principle based.	No change.
Paragraph 40	A comment was received that this paragraph seems very generic and that this should be clarified. In the respondent's view 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).	The EBA considers that there is no need to further explain 'changes', as it refers to both.	No change.
Paragraph 40	One respondent suggested adding cross-references here to Section 4.6.2 'ICT acquisition and development' and Section 4.6.3 'Change management'.	The EBA considers that cross-references between sections are not deemed necessary to ensure that these guidelines remain concise.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
4.4.6. Security monitoring Paragraph 41	Further specification was requested from one respondent on the connection between business/administrative functions (paragraph 41(a)) and relevant 'internal and external factors' (paragraph 41(c))	Further specification is requested on Section 5.2 of the Guidelines on security measures for operational and security risks (EBA/GL/2017/17).	No change.
Paragraph 42	One respondent recommended that the requirement to 'constantly monitor security threats' should be rephrased to state that 'financial institutions establish a threat intelligence gathering and assessment process to identify, triage and counter targeted threats, and that this is embedded into its log correlation and orchestration processes'. Firms should know what they are monitoring for. This was reiterated by a comment on the intention of the wording 'actively monitoring technological developments' and how this should be understood. Another respondent suggested deleting the following wording '.. their ability to provide services. ~~Financial institutions should actively monitor technological developments to ensure that they are aware of security risks~~.', as it was deemed unclear how an institution can do this. Another respondent commented that there seems to be no consideration of proactive measures in this paragraph, e.g. threat hunting.	The EBA considers that there is no need for rephrasing, referring to the principle-based wording.	No change.
		The EBA considers that a financial institution should have the necessary capabilities to actively monitor technological developments and should be aware of the associated security risks.	No change.
	One respondent suggested wording to clarify that proportionality aspects should be taken into account: 'Financial institutions should implement detective measures, **for instance** to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities of software and hardware, and to check for corresponding new security updates.'	The EBA agrees with the comment and suggestion made. The guidelines have been reworded as follows: *'Financial institutions should implement detective, **for instance** to identify possible information leakages […].'*	The guidelines have been amended.
Paragraph 43	One respondent commented that it is not clear how the security monitoring process will help a financial institution identify an operational incident that will be a security incident.	The intention of this requirement is for the security monitoring process to assist a financial institution to have a better understanding of its own systems and risks.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
4.4.7. Information security reviews, assessment and testing	A general comment on Section 4.4.7 was received for the guidelines to consider activities carried out by firms to assess and mitigate operational and ICT risks (e.g. operational risk self-assessment) that could align with the requirements in these guidelines. Another general comment was on the fact that the guidelines do not include minimum KPIs for ISMSs, the Federal Financial Institutions Examination Council (FFIEC) principles for outsourcing and more specific requirements for adequate vulnerability/patch management and network segmentation. As a consequence, institutions do not know what is useful and what the auditor will demand. In contrast to this, the number of penetration tests is deemed too high. If tests for the effectiveness of the security measures are required after major changes, information security incidents and the installation of new internet-facing systems and once per year for critical and every 3 years for other applications, the information security organisation will spend most of its budget on penetration tests and will lose the support of the company in following up. The respondent recommends that it would be better to use the FFIEC wording in the ICT Examination Handbook: 'frequency and scope of a penetration test should be … determined by the risk assessment process.'	The EBA considers that a financial institution itself is responsible for their risk assessment and needs to have an understanding of what is useful for their situation. The guidelines do not consider that penetration tests and red team exercises should be mandatory, as testing should be proportionate, commensurate to the risk exposure of the institution and to the maturity of ICT and security risk management within the organisation. The guidelines are clarified by replacing 'foster' with '**consider good practices such as**'.	No change. The guidelines have been amended.
Paragraph 44	One comment was received that the institution should foster source code reviews, penetration tests and/or red team exercises. Another respondent proposed new wording to ensure that the selection and intensity of the control measures should be made dependent on the needs or threat situation and that proportionality is taken into account: '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	The guidelines are clarified by replacing 'foster' with '**consider good practices such as**'.	The guidelines have been amended. No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	external audits of the information systems, or physical security reviews. **The selection and intensity should be appropriate, depending on the needs or threat situation.** ~~Furthermore, the institution should foster source code reviews, penetration tests, or red team exercises.~~ **Other instruments to consider include source code reviews, penetration testing, and red team exercises.**'	The EBA considers that the suggested wording is part of the proportionality principle: therefore, no change is needed. The guidelines are amended as suggested: '~~or~~' replaced with '**and**'.	The guidelines have been amended.
Paragraph 44	One respondent suggested that some of the terms in this section should be defined in the 'Definitions' section (e.g. red team) and some other related terms should be also used here for the sake of inclusiveness, for example 'vulnerability assessment' and 'blue teaming' (together with 'purple teaming'). Additional wording proposed: *'Furthermore, the institution should foster source code reviews,* ***vulnerability assessments,*** *penetration tests, or* ***blue team -*** *red team* ***(or purple team)*** *exercises.'*	The suggestion is partly accommodated to include 'vulnerability assessment': 'Furthermore, the institution should consider good practices such as source code reviews, **vulnerability assessments**, penetration test and red team exercises.'	The guidelines have been amended.
Paragraph 45	One respondent suggested deleting the word 'new': 'and ensure that this framework considers ~~new~~ threats and vulnerabilities', while another suggested substituting '~~new threats~~' with '**identified threats**'. Another respondent asked for clarification of whether this paragraph introduces a separate framework.	Based on the suggestions, the guidelines have been amended to replace 'new' with '**identified**'.	The guidelines have been amended.
Paragraphs 45 and 46	One respondent asked if a specific security testing environment was required.	The EBA considers that a specific security testing environment is not required.	No change.
Paragraph 46	A request was received to specify 'testing framework', as in the respondent's view it seems that 'testing framework' refers to a concept that goes beyond the simple drafting of a test plan to the merits of how the tests are performed.	The testing framework is more than drafting a test plan; therefore, it is necessary to keep the wording.	No change.
Paragraph 46(a)	With regard to the reference to 'independent testers', some respondents requested that the guidelines consider a firm's ability to perform tests by internal or external providers, as long as those tests are performed by resources having the necessary level of independence	The reference to 'independent testers' includes internal as well as external testers.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	and expertise. This would also highlight that in certain cases, and according to the risk involved, it is more advisable that independent testing is done by internal employees with the necessary separation of duties. Additional wording proposed: '*are carried out by independent **(external or internal)** testers.*'		
Paragraph 47	One comment was received to add the word 'critical' to better reflect the proportionality principle, i.e. that minor or low-risk changes to non-critical or low-risk processes, infrastructure or systems might not need security testing, depending on the type of risks associated with the change (risk-based approach): 'Financial institutions … in the event of changes to **critical** infrastructure, processes ….'	The proportionality principle is already sufficiently included in the wording of 'tests of security measures are conducted'.	No change.
Paragraphs 47 and 49	One respondent suggested that paragraph 49 should be placed before paragraph 47, as the tests conducted on an ongoing basis should be mentioned before the tests conducted in the event of changes to infrastructure, processes or procedures.	The EBA agrees with the proposal. The guidelines have been amended accordingly.	The guidelines have been amended.
Paragraph 48	One respondent proposed changes to allow flexibility in handling weaknesses that are exposed by security tests 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 does the risk of not fixing the weakness. Furthermore, management could be willing to accept the risk of not implementing a security measure …: '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 EBA considers that the obligation to patch cannot be removed in the case of a critical system. There is a timing aspect of 'when do you patch', but if this causes a big delay, the institution should have more robust systems or methods of patch deployment. The EBA considers that risk-based approach is included by the word 'accordingly'.	No change. No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	A comment was received on how to define criticality of systems and for the EBA to clarify that the expectation is for firms to demonstrate having adequate processes for determining criticality and an appropriate process for action on this basis.	See comment on paragraph 18 above	No change.
Paragraph 49	A number of comments were received regarding the testing frequency of 3 years. Some respondents suggested that the timing of 'every 3 years' should be deleted since this paragraph already provides for a risk-based approach, so there is no need to be more prescriptive. Another respondent considered that testing all the critical security measures on an annual basis and all non-critical systems every 3 years can be too much for complex organisations and that these requirements should be adapted to the kind of organisation we are talking about. Other respondents considered that the period of 3 years is a long span of time and that tests for all critical ICT systems should be performed at least on an annual basis, i.e. based on the asset classification process previously mentioned. In 3 years, technology revolutions happen and attack vectors evolve in impressive ways.	The EBA considers that conducting tests on a risk-based approach but at least every 3 years is critical to ensure effective ICT and security risk management. Testing systems less frequently than every 3 years may result in security measures being obsolete.	No change.
	A third view was that new wording should be added to ensure that the timing for testing is risk based and the responsibility of the institution: 'Financial institutions should perform on-going and repeated tests of the security measures, **commensurate with the criticality of the ICT systems.'** ~~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~~.'	The EBA considers that a financial institution has to conduct its own risk assessment and conduct the tests accordingly. However, it is important to ensure that tests are conducted repeatedly, but not less frequently than every 3 years.	No change.
	One respondent also suggested that the scope be deleted (i.e. not to specify 'non-critical systems'). This respondent commented that penetration testing is conducted on all external-facing applications before going live, annually, and when there are material changes to these applications. They test external-facing applications because these	The EBA considers that implementing these suggestions would be unduly burdensome and not be principle based. As suggested in the example provided,	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	are viewed as having a high risk exposure to threat actor operations. Therefore the respondent considered that external-facing applications rather than the criticality of the application would be more reasonable for taking a targeted approach to penetration testing.	an external-facing application should be a critical system.	
Paragraph 50	One respondent suggested that this paragraph should be rephrased to prescribe that only certified payment terminals have access to the network.	The EBA considers the current wording of the guideline to be sufficient, as it is in line with the relevant regulation.	No change.
Paragraph 50	One respondent suggested that it seems that the requirement does not take into account the current trends in payment services technology. Paragraph 50 requires all PSPs to test security measures implemented in payment terminals and devices used to provide payment services, payment terminals and devices used to authenticate the user of payment services and devices and software supplied by the payment service provider to the user of the payment service to enable the user to generate/receive an authentication code. In the case of mobile devices, such as smartphones and tablets, the requirement to test each device model is not unrealistic, but it may be considered excessively burdensome. Therefore, testing could be restricted to a limited range of models, reducing the potential choice of compliant mobile devices. It is suggested that the requirement to test mobile devices (smartphones, tablets, etc.) be limited to the testing of the operating system only (e.g. Android, iOS, Windows Mobile).	The EBA is of the view that, as a rule, PSPs should enter into contracts with their outsourcing providers for the provision of payment services. Any form of contract should be concluded between the PSP and its outsourcer, not with the PSU. The EBA is aware that in some cases PSPs may not have a close relationship with sub-outsourcing providers because the whole process is under the control of the primary outsourcing provider. The EBA is also aware that PSPs might not enter into contracts with suppliers of end user devices, such as tablets or smartphones, or providers of operating systems.	No change.
4.4.8. Information security training and awareness Paragraph 52	A comment was received that training should be required for staff with relevant functions and that heightening the awareness of all staff is addressed in paragraph 54. '… training programme for **relevant** ~~all~~ staff …'	The guidelines have been revised to clarify that training programme includes periodic security awareness programmes. They were also amended to clarify that a training programme should be established for all staff, including the management body and contractors. To ensure that they are well informed, all staff should undergo training (including security awareness	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		programmes), as appropriate, at least annually. Paragraphs 53 and 54 were removed and the guidelines amended accordingly: '*Financial institutions should establish training programme,* ***including periodic security awareness programmes,*** *for all staff* ***and contractors*** *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* ***and trained to address information security-related risks.*** *Financial institutions should ensure that the training programme provides training for* ***all*** *staff members* ***and contractors*** *at least annually*.'	
Paragraph 53	A few comments were received on the training and who it is addressed to. In particular one respondent questioned whether a security awareness programme can be considered a targeted information security training for staff members occupying key roles. Another suggested removing '~~occupying key roles~~', as this should apply to all staff. One respondent made the proposal for the additional wording: *'Financial institutions should ensure that staff members occupying key roles* ***and main ICT risk-handling functions (e.g. ICT operations staff, ICT in-house development staff and ICT security management staff)*** *receive targeted information security training at least annually* ***with mandatory examinations****.'*	The EBA merged a few paragraphs in Section 3.4.8 and redrafted the guidelines to require that institutions should '*establish a training programme,* ***including periodic security awareness programmes****, for all staff* ***and contractors*** *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* ***and trained to address information security-related risks***. This ensures that the guidelines can be applied in a proportionate manner. The EBA considers that a security awareness programme is not considered a targeted information security training and that applying the requirement to all staff would be unduly burdensome and would not be principle based. The EBA considers that examples	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		provided are the examples of roles, but no change is needed to the guidelines in order to keep them principle based. On the last point, the EBA considers that to specify an examination requirement in the guidelines would be too specific.	No change.
Paragraph 54	One respondent proposed the additional wording: *'Financial institutions should establish and implement periodic security awareness programmes to educate their staff, including the management body* ***(together with management assistance personnel),*** *on how to address information security-related risks.'*	The EBA considers 'management assistance personnel' as part of the financial institution's staff; therefore, the suggested clarification is not deemed necessary.	No change.
Paragraph 54	A suggestion was made to replace awareness programmes with 'awareness sessions', as 'sessions' is deemed more flexible.	The word 'programmes' was selected in order to speak about the whole awareness training, which may encompass sessions but also other things such as manuals.	No change
Section 4.5. ICT operations management Paragraph 55	One respondent proposed adding the designation 'appropriate', in order to cater for different internal organisation structures: '[…]based on processes and procedures that are documented, implemented and approved by the **appropriate** management body'. Another requested clarification that only material changes in the overall ICT risk management documentation should be approved by the management body, since not every tiny change and adaption needs management approval, as long as the overall concept is not changed.	The terms 'management body in its management function' and 'management body in its supervisory function' should be interpreted throughout the guidelines in accordance with the applicable law within each Member State. The terms 'management body in its management function' and 'management body in its supervisory function' are used throughout these guidelines without referring to any specific governance structure and should be interpreted throughout the guidelines in accordance with the applicable law within each Member State. This definition is consistent with the EBA Guidelines on internal governance EBA/GL/2017/11. The term 'management body' by	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		definition is an appropriate management body and is already defined in the definitions section of the guidelines. The intention of the guidelines is that the initial development, documentation and implementation of operational processes and procedures should be approved by the management body. The management of changes to ICT and security risk management processes and documentation is defined in Section 3.3.1, paragraph 14.	
Paragraph 55	Two respondents emphasised that the way financial institutions decide to complete the documentation for their ICT operations and maintain their ICT asset inventories may vary and suggested keeping the guidelines principle based with regard to how firms decide to do this to avoid this activity increasing resource requirements and becoming compliance driven.	The guidelines require institutions to develop processes and procedures that should consider the maintenance of their ICT assets inventories; however, they do not specify how these should be achieved, which provides institutions with sufficient flexibility.	No change.
Paragraph 55	Two respondents suggested that the documentation of processes and procedures need not be performed and approved by the members of the management body but by executive/senior management structures. Management body approval of the main features of the operations and a corresponding mandate to a responsible member of staff are sufficient. Certain management body responsibilities outlined in the guidelines should be amended to permit delegation where deemed adequate. The proposed wording is *'Financial institutions should manage their ICT operations based on* ***documented*** *processes and procedures~~.~~'* Another commented that it is not possible that the management body would 'implement' any policy that it would approve, as this extends beyond its strategic role in the governance of the organisation. The proposed wording is *'Financial institutions should manage their ICT operations based on processes and procedures that are documented,*	The management body should approve the processes and procedures; however, the EBA anticipates the delegation of the documentation and implementation. The guidelines have been amended to reflect this: '*Financial institutions should manage their ICT operations based on documented and implemented processes and procedures (****which, for PSPs, include the security policy document in accordance with Article 5(1)(j) of PSD2****) that are ~~documented, implemented and~~ approved by the management body.*	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	implemented and approved by the ~~***management body***~~ ***individual or forum with delegated responsibility for ICT risks.****'*		
Paragraph 56 Automation	A few respondents commented on the use of automation in ICT operations. Some said that the guidelines should remain principle based and suggested removing any reference to the automation of ICT operations, as firms may achieve operational efficiency through means other than automation. These respondents recognised the benefits of automation but also highlighted a number of potential risks, so in certain processes it still makes sense to include expertise in decisions. A change in wording was proposed: *'*~~***To increase the efficiency of financial institutions' ICT operations, f***~~***F****inancial institutions are encouraged to automise* ~~***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.***~~*'* Another respondent suggested removing the requirement for automation and to add '***consider where automation of ICT operations may provide material benefit in the minimisation of potential errors arising from the execution of manual tasks****.'*	The guidelines intend to show that manual tasks may cause errors. However, it is also clear that automation may indeed be one of a number of ways of increasing effectiveness; therefore, the wording is amended to reflect this: '*Financial institutions should maintain and improve, when possible, the efficiency of their ICT operations, including but not limited to the need to consider how to minimise potential errors arising from the execution of manual tasks*'. ~~*'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.'*~~	The guidelines have been amended.
Paragraph 56	One respondent commented that, given the relevance of security, this should be taken into account by ICT operations when performing their duties, at least with the same attention as is given to the other requirements that ICT operations are subject to. Addition of 'and security' is proposed: '[…] is aligned with the business **and security** requirements'.	ICT security is given sufficient attention in other parts of the guidelines, specifically in Section 3.4. To avoid duplication of messages, no further changes are required in paragraph 53.	No change.
Paragraph 56	One respondent requested clarification on how the requirement 'as far as possible' can be measured by competent authorities for compliance.	The paragraph has been revised in line with comments received, and the reference to 'as far as possible' has been removed. The EBA considers that, for the assessment of principle-based requirements,	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		competent authorities are expected to use an approach that takes into account each institution on a case-by-case basis.	
Paragraphs 56 and 57	One respondent recommended that the guidelines remain principle based on how firms decide to increase ICT operational efficiencies and suggested removing the prescriptive requirements on how firms achieve this outcome. The respondent recognised the benefits of ICT operations capacity monitoring and performance management; however, the implementation of such programmes for financial service firms operating globally is often costly, complex and may not deliver immediately the benefits expected. For example, the logging and monitoring of procedures for critical ICT operations may not increase operational efficiency if not implemented appropriately.	The comment has been accommodated in revised paragraph 53 (see comment above), and examples have been removed. With regard to paragraph 57 (revised paragraph 54), the EBA considers that logging and monitoring requirements are important and need to be in place. However, the manner and extent to which they are implemented is decided upon by institutions proportionately.	The guidelines have been amended. No change.
Paragraph 58	One respondent suggested that this requirement should also depend on protection needs and the business criticality of the process and/or asset — only for the critical assets of the bank and only for the key components. The additional wording suggested is *'Financial institutions should maintain an updated inventory of their* **critical** *ICT assets (including the* **core** *ICT systems, network devices, databases).* Another respondent suggested identifying assets that are '**critical'** in providing service capability.	The inventory should contain all assets, which then need to be classified for criticality. Maintaining an inventory of only critical assets risks omitting assets that were not correctly classified.	No change.
Paragraph 58	One respondent requested clarification of the objective behind a requirement to have a single system to carry this information, as the goal of enabling a proper configuration and change management process can be achieved in other ways, including by using a suite of tools. The respondent acknowledged and agreed that financial institutions should maintain up-to-date inventories of ICT assets. However, it considered that the requirement in this section should specify desired outcomes rather than specific features of an asset management system. Financial institutions that maintain very large systems may choose to keep asset, configuration, change and	Paragraph 58 (revised paragraph 53) does not require a financial institution to keep the inventory in a single system. The way the inventory is maintained is up to the institution; these guidelines specify only what should be maintained.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	dependency information in systems specifically optimised for each use, rather than in single monolithic asset inventory systems.		
Paragraph 58	One respondent suggested substituting '~~**document the configuration**~~' with '**contain the configuration**'.	The comment has been accommodated by replacing '~~document~~' with '**store'.**	The guidelines have been amended.
Paragraphs 58 and 59	One respondent suggested that clarification was needed on the extent to which financial institutions have to document interdependencies between the different ICT assets. One respondent suggested specifying the desired outcomes in asset, configuration or change management, to which ICT professionals can adhere using verifiable and commercially reasonable means. The respondent argued that, while it is reasonable to require ICT professionals to understand the components and/or systems on which an application or system depends, this is not true in the opposite direction. For example, while the operating system version on which a particular application relies is an important dependency to understand, it would not be practical for an operating system vendor to know all of the software packages that may at some point run on that operating system.	The EBA considers that providing more detailed recommendations on the level of details or specific solutions would make the guidelines less practical and more burdensome. The intention is to remain principle based, to allow their proportionate implementation.	No change.
Paragraph 59	One respondent suggested identifying the '**legal, regulatory or contractual requirements'** that need to be addressed when managing the asset.	The EBA considers that these **legal, regulatory or contractual requirements** do not need to be captured in the inventory of assets on such a granular level.	No change.
Paragraph 60	One respondent suggested replacing **'~~ICT assets~~**' with '**software assets**' because this provision is limited to software assets, as hardware can be managed in a different way, following a specific hardware technology life cycle. Moreover, the respondent proposed adding '**or other external ICT experts**' to reflect that it is also possible to have support from third parties (e.g. for open source solutions) that are not the vendor of the software. The revised wording proposed was: *'Financial institutions should monitor and manage life cycle of ~~**ICT**~~ **software** assets to ensure that they*	The focus of the paragraph is to ensure that relevant ICT assets continue to meet and support business and risk management requirements. The EBA does not intend to limit the scope to software only, as hardware also needs to be taken into consideration. The comment on external experts has been accommodated: *'ICT assets are supported by their*	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	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.'*	***external or internal*** *vendors and~~ or in-house~~ developers'*	The guidelines have been amended.
Paragraph 62	One respondent suggested substituting '~~**restoration**~~' with '**recovery**'.	The process is a restoration, as backups are performed for the recovery of a system's functionality. The EBA considers that the paragraph's text is logical and sequential.	No change.
Paragraphs 62 and 63	Two respondents recommended that the guidelines remain principle based in how firms decide to implement data and ICT systems backups and restoration procedures and to remove prescriptive requirements on how firms achieve this outcome. One respondent suggested that backup requirements should be aligned to the business recovery requirements. System criticality is more aligned to the BIA for technology in business continuity management. Another respondent recognised the benefits of ICT systems and data backups and restoration. However, it suggested that further considerations may be required (e.g. impact tolerance levels, firms risk appetite).	These guidelines requires financial institutions to define their backup and recovery processes requirements, in line with business recovery requirements and the criticality of the data and the ICT systems. However, the EBA does not specify how this should be achieved. Hence, the EBA has defined principles rather than specific requirements. The EBA specifically mentioned that backup requirements are defined in line with business recovery requirements and the criticality of the data and the ICT systems.	No change.
Paragraph 63	Some respondents requested further specification of supervisory expectations for what is meant by 'sufficiently remote', in order to avoid discrepancies in implementation. One respondent asked for clarification on whether it is acceptable that the remote location or locations are in the same city as the primary site but far away in distance.	The comment has been accommodated in order to remain more principle based regarding the location of backups. With regard to the remote location, it should be in such a location that it is not exposed to the same risks as the primary site. The guidelines have been amended as follows: *'Financial institutions should ensure that data and ICT system backups are stored*	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		securely ~~in one or more locations out of the primary site, which are secure~~ *and are sufficiently remote from the primary site so* ***they are not*** ~~so as to avoid being~~ *exposed to the same risks.'*	
	Another respondent asked what was the desired outcome, an RPO or an RTO?	The desired outcome is to recover systems to meet business recovery requirements. As part of setting these requirements, firms can consider defining RPOs and RTOs that are relevant to specific processes, systems and data.	No change.
4.5.1. ICT incident and problem management	One respondent commented that the implementation of requirements in paragraphs 64 and 65 seems to align with the requirements detailed in the BIS BCBS's 'Principles for the sound management of operational risk' [9] regarding 'loss data collection' (page 11), and recommend considering adding a reference to this document, as it would help clarify and trace requirements to their potential source.	The EBA considers that the objectives of loss data collection and incident and problem management are different.	No change.
Paragraph 64	One respondent commented that this description was primarily focused on the aim of incident management. Since Section 4.5.1 was meant for incident and problem management, the respondent suggested providing additional wording: *'**The primary objectives of problem management are to prevent incidents** […] **(proactive problem management).**'*	The EBA considers that the primary objective is to enable financial institutions to continue or resume critical business functions and processes when disruptions occur. Problem management processes are one of the means to achieve this. The EBA describes problem management processes in paragraph 60(c).	No change.
Paragraph 64	Several respondents noted that the word 'financial **institutions**' was missing.	Drafting change accepted.	The guidelines have been amended.

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

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 64	One respondent suggested the additional wording '**timely** resume', to emphasise the time criticality issue.	Suggestion accepted and the guidelines amended as follows: '[..] *continue or resume, **in a timely manner***[..]'.	The guidelines have been amended.
Paragraph 64	One respondent asked for the guidelines to specify and provide examples of which incidents are considered security incidents and which are considered another type of ICT incident.	The guidelines focus on operational and security incidents that are described in the definitions section of these guidelines.	No change.
	One respondent expected financial institutions to have criteria in place for (1) operational incidents, (2) security incidents, and (3) early warning indicators.	Early warning indicators are part of the problem identification process and the way in which the problem identification process is implemented may vary between institutions; therefore, any further details would be disproportionate and burdensome.	No change.
Paragraph 65	One respondent welcomed the principle-based guidance on resumption of service in the event of a disruption but recommended considering separating out the list of activities that firms should consider in their incident and problem management as examples of how the requirements could apply or be interpreted.	As the guidelines follow a principle-based approach, providing more specific requirements would not be practical and proportionate.	No change.
Paragraph 65(a)	One respondent suggested that, for internal products/services, there is sometimes no SLA available, so this cannot be used as a benchmark. The criticality rating is present in every case. The change in wording suggested is *'business criticality ~~and~~ **or** service agreements'*	The comment has been accommodated. Service level agreements are not the driver to decide the priority of an incident, as this priority should be based on business criticality assessments. Reference to 'service agreements' is removed.	The guidelines have been amended.
Paragraph 65(c)	Two respondents commented that security incidents outside the organisation are not part of an institution's own incident management. A financial institution is unlikely to be able to act to 'identify, consider and resolve' problems external to its organisation. The present wording could be misunderstood to mean that incidents within other organisations would also have to be considered.	The EBA considers that it is important to take account of incidents affecting a financial institution that have occurred outside, for example at a service provider. The ways in which to avoid recurrence of incidents, however, are in the control of an institution. The text of the guidelines has been revised to provide more clarity: '*should analyse operational or security incidents **likely***	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	The suggested changes in wording are *'within* ~~***and/or outside***~~ *the organisation'* and *'financial institutions should analyse operational or security incidents* ~~***that have been identified or have occurred within and/or outside the organisation***~~*.'*	*to* ***affect the financial institution*** *that have been identified or have occurred within and/or outside the organisation[…]'*.	
Paragraph 65(f)	One respondent suggested further considering the impact on firms operating across multiple jurisdictions of having to comply with multiple requirements or reporting obligations. There is an increasing risk of the proliferation of incident reporting requirements for firms, which may increase the reporting burden on firms, as well as divert resources from actual risk mitigation. The respondent suggested that the EBA should consider how to support efficient reporting mechanisms, such as 'provide once, satisfy many', or how reporting information could be aggregated by authorities and shared with industry to support preparedness and response. The respondent was supportive of an effective and coordinated incident response plan that would support the industry in the event of a large-scale disruption, which may require input and testing with the public sector's response (e.g. an EU blueprint).	The EBA is aware of the need for multiple submissions across jurisdictions; however, such a proposal is outside the scope of the guidelines. Moreover, the EBA has flagged this issue to the European Commission in its Joint ESA advice on the need for legislative improvements on ICT risk management requirements (JC 2019 26).	No change.
Paragraph 65(f)	One respondent proposed adding the words 'and internal'. The suggested wording is *'specific external* ***and internal*** *communication plans'*.	The suggested change would overlap with paragraph 60(d), which covers internal communication plans.	No change.
Paragraph 65(f) (ii)	One respondent proposed the addition of '(*e.g. customers, other market participants, the supervisory authority,* ***any existing sectoral CERT/CSIRT),*** *as appropriate*' to ensure maximum involvement of sector structures dedicated to cybersecurity in order to facilitate crisis management coordination and sectoral response in case of systemic events.	As the guidelines follow a principle-based approach and the list of examples cannot be exhaustive, the EBA considers that providing more specific examples would not be practical or proportionate.	No change.
	Another respondent suggested that there may be clashes with other legal provisions here, as potentially confidential (e.g. personal) data that may be protected by law and for which the guidelines are unlikely to be	As the guidelines follow a principle-based approach and the list of examples cannot be exhaustive, the EBA	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	an adequate basis for encroachment in every case can be affected. The suggested additional wording is *'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* ***and legislation (e.g. GDPR)****.'*	considers that providing specific examples would not be practical or proportionate.	
4.6. ICT project and change management Agile principle	Many respondents suggested that Section 4.6, 'ICT project and change management', should be redesigned to allow modern project management practices to be used for system/application development (e.g. Agile, Tribes). It was suggested to focus more on what is to be achieved (control principles) and less on how this should be achieved. Draft requirements could be perceived to dictate that project management and system development methodologies should follow the waterfall model, i.e. a linear sequential design approach for software development. Most financial institutions have already or are in the process of adopting agile software development. This is another example of these guidelines limiting the options available for financial institutions, in this case not only related to risk management but also to business development. One respondent proposed amending this section in such a way that it facilitates agile working in ICT development projects. Financial institutions have increasingly adopted agile ways of working in the development of software. This means that the requirements described in paragraph 73, which envisage that the process of the development of ICT systems should include a), b), c) and d), cannot be met by the financial institutions that use agile methods. In competitive environments, the need for flexibility, especially with the limited separation of duties and new ways of organising projects, is seen as mandatory. The iterative approach of 'agile' methods supports a product rather than a project mindset. This provides greater flexibility throughout the	The EBA has updated all of Section 3.6 to make it more principle based and technology neutral. The EBA defined the desired outcomes of these guidelines and the principles that institutions can apply to achieve these outcomes. The guidelines do not seek to define specific ways in which the outcomes can be achieved, and it is up to institutions to decide how best to apply these principles. The EBA applied the principle of proportionality throughout the text and focused on creating technology agnostic and future proof guidance. Hence, the EBA does not specify what software development methodology is to be used nor what specific standards or technology are to be applied. The executive summary has been amended to include the following sentence: ***'These guidelines intend to be technology and methodology agnostic.'*** Based on the suggestion, the paragraph has been revised and prescriptive elements removed. Instead, the guidelines now require that '*This process should* ***be designed using a risk-based approach.*** ~~*Include:*~~ ~~*a) setting objectives during the development phase;*~~ ~~*b) technical implementation (including secure coding/programming guidelines);*~~ ~~*c) quality assurance standards; and*~~	The guidelines have been amended. The guidelines have been amended. The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	development process, whereas in 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.	~~*d) testing, approval and release, irrespective of whether the development is done in-house or externally by a third party*~~*'*	
	One respondent suggested that the guidelines should rather focus on providing clarification of supervisory expectations regarding adequate governance and control related to (material) changes. The respondent considered that some requirements of the draft guidelines are expendable and not fit for purpose. In particular, where the guidelines outline the implementation of ICT-related changes primarily through a project setup, there is a lack of insight on state-of-the-art ICT challenges. The respondent considered that the draft guidelines focused too strongly on project setup, which did not fit the actual practice in, among other things, software development. Software is increasingly being developed continuously or in agile project setups (e.g. Scrum) rather than in so-called 'waterfall' project setups (as particularly indicated in paragraph 68 of the draft guidelines).	References to the phases of each project have been removed in order to ensure that these guidelines are software development methodology agnostic: *'[…]ICT project management policy that* ~~*defines the phases of each project and*~~ *includes as a minimum'.*	The guidelines have been amended.
	Another respondent advised adding a provision in Section 4.6 on the use of control mechanisms, regardless of the methodology employed.	Logical access controls have to be implemented, including the elements stated in paragraph 31(a) to (g).	No change.
	One respondent suggested the possibility of including the draft guidelines on ICT project management (i.e. Section 4.6.1) as general requirements for, for example, project and change management, into the Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2017/11). It argued that the draft Guidelines on ICT project management, as specified under Section 4.6.1 of the draft guidelines, do not contain any ICT-related specifications but constitute general requirements on project management that are applicable to a multitude	The revised Section 3.6 defines principles relevant to project and change management processes that financial institutions can apply to ensure that changes to production systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner, with the aim of ensuring that ICT projects have appropriate governance and oversight and that the development of applications is carefully monitored from the test phase to the production phase.	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	of fields and should therefore be incorporated (including agile project setups) in guidelines that focus on institutions' organisational duties.	The executive summary has been amended to explain that these guidelines are technology agnostic. Furthermore, the EBA considers that changing the Guidelines on internal governance would be counterproductive.	No change.
General 4.6	One respondent acknowledged the importance of ICT project management and promoting adequate standards to ensure the safe and secure implementation or change of ICT systems, but recommended that the guidelines remain principle based regarding how firms implement adequate standards for ICT project and change management, and rather focus on firms being able to demonstrate adequate capabilities and outcomes.	The executive summary has been amended to explain that these guidelines are technology and methodology agnostic and hence the EBA does not specify what standards or methodology should be used to achieve the requirements of the guidelines.	No change.
General 4.6	One respondent suggested including provisions associated with risk management, since it must be an inherent part of changes, acquisitions, new developments, projects, etc., to enable the 'security by design and by default' paradigm.	In these guidelines, Section 3.4.4 on ICT operations security requires institutions on an ongoing basis to determine whether changes in the existing operational environment influence the existing security measures or require the adoption of additional measures to mitigate related risks appropriately. These changes should be part of the financial institutions' formal change management processes, which should ensure that changes are properly planned, tested, documented, authorised and deployed. A combination of requirements in Section 3.4.4 and Section 3.6 will ensure that information security requirements are considered.	No change.
4.6. ICT project and change management	One respondent suggested that the implementation of this requirement seemed to indicate that it would be expected of firms to complete this blanket control across all activities regardless of criticality; it	Financial institutions should ensure that changes to production systems are recorded, tested, assessed, approved, implemented and verified in a controlled	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraphs 66 to 82	recommended clarification of the scope and of what would be expected of firms and that it would be performed using a risk-based approach to ensure that it is realistically completed, in line with best practices.	manner. An institution should decide how requirements in Section 3.6 apply, considering the scale and complexity of the project or change, the nature of the change or project and related activities, the types of services affected and the corresponding ICT and security risks related to the financial institution's processes and services affected by the change or project.	
4.6.1. ICT project management	One respondent suggested that Section 4.6.1 on ICT project management should be removed, as it is too high level and, to a large extent, is a repetition of more specific and concrete requirements covered elsewhere. The guidelines already required institutions to assess risks in major ICT changes (Section 4.6.3: ICT change management; Section 4.3.1, item 15: identify and assess ICT risks resulting from major change; Section 4.3.3, item 21: ICT risk assessment to be performed annually or on any major changes).	Section 3.6.1 defines important principles related to project management. Although there are some references to this process in other sections of the guidelines, it is important to keep this section to ensure that a holistic set of principles is defined.	No change.
	One respondent suggested that as these guidelines contained ICT and security risk management provisions, procurement management is not within the scope of these guidelines.	The reference to procurement management has been removed to ensure better consistency with a principle-based approach. Furthermore, procurement management-related principles are sufficiently defined in the EBA Guidelines on outsourcing arrangements.	The guidelines have been amended.
Paragraph 66	One respondent commented that the guidelines particularly emphasised the implementation of the ICT strategy through ICT projects but that the objectives of the ICT strategy could be implemented by various equivalent means. The respondent commented that the implementation of an institution's strategy should be effectively supported through adequate governance processes and therefore considered the requirements in the guidelines misleading, as they might be interpreted by institutions as supervisory expectation to	To accommodate the comment, the EBA has amended paragraph 6 in Section 3.2.2 on ICT strategy: *'Financial institutions should establish sets of action plans* ***that contain measures to be taken to achieve the objective of*** ~~*to support*~~ *the ICT strategy. These should be communicated to all relevant staff (including*	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	implement ICT-related strategic objectives exclusively through projects. The respondent suggested that instead of focusing on project setups, clarification of supervisory expectations should focus on an adequate control or change management framework (see Chapter 4.6.3.).	***contractors and*** *third party providers where applicable and relevant).'* Section 3.6. paragraph 61 has also been revised: *'A financial institution should implement a programme and/or* ***project*** *governance process* ***that defines roles, responsibilities and accountabilities*** ~~*e adequate project implementation leadership*~~ *to effectively support the implementation of the ICT strategy* ~~*through ICT projects.*~~*'* Paragraph 71 has also been deleted.	
Paragraph 66	Three respondents requested a clear definition or clarification of 'an adequate project implementation leadership'.	The EBA defined key principles of the project governance process to include roles, responsibilities and accountabilities. However, how this project governance is implemented is up to each institution.	The guidelines have been amended.
Paragraph 67	One respondent suggested that financial institutions should also monitor and mitigate risks regarding the involvement of external solution providers during the project (e.g. transfer of confidential data during development or development environments in the cloud).	The EBA considers that the requirements related to relationships with third party providers are sufficiently covered in Section 3.2.2 ––Strategy, Section 3.2.3 — Use of third parties and Section 3.6.2 — ICT systems acquisition and development.	No change.
Paragraph 68	One respondent suggested that the requirements of this paragraph are too prescriptive, as they do not allow strategy implementation through non-project activities, e.g. agile/lean methods. The respondent suggested deleting ~~***and includes at a minimum: and the points (a) (g).***~~'. Another respondent suggested making them examples and not minimum requirements. Furthermore, in order to allow agile project development methods, additional wording at the end of paragraph 68 was proposed: *'****For agile development, corresponding methods can be used.****'*	The EBA has removed 'phases of each project' to depart from the waterfall approach, but the EBA considers that the underlying principles still remain even if using agile methodology: *'ICT project management policy that* ~~*defines the phases of each project and*~~ *includes as a minimum'.*	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 69	One respondent suggested that the requirements of this paragraph are too prescriptive, as they do not allow strategy implementation through non-project activities, e.g. agile/lean methods. The following changes were suggested: *'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.~~**'.*	The guidelines have been amended in line with the suggestion.	The guidelines have been amended.
Paragraph 69	Two respondents asked which function that was independent from development had enough authority to analyse and approve the security requirements. One respondent asked for clarification of the desired outcome, and pointed out that in a DevOps development scenario, this method may slow down the delivery of security fixes, which seems contradictory to the requirement to push security patches as fast as possible.	Paragraph 61 defines project governance process, which will be relevant for defining the independent function responsible for ensuring that information security requirements are considered.	The guidelines have been amended.
Paragraph 70	Some respondents requested a clear definition of 'adequate knowledge' and in particular whether it means that the project team's member should have knowledge about business, if the scope requires it (e.g. a payment expert), or it means that work stream leads should have project management knowledge, or both.	The aim of the guidelines is to ensure that project participants have knowledge that is both sufficient and relevant to the project and the related business processes and systems being developed.	No change.
Paragraphs 71 and 72	One respondent suggested that the requirements of this paragraph are too prescriptive, as they do not allow strategy implementation through non-project activities, e.g. agile/lean methods. The following change was suggested: '*The responsibilities of the project team members should be defined and documented in the project plan**. ~~and approved by the project implementation leader.~~*** '	See comments on paragraph 66 above. Based on the amended text in paragraph 66, paragraph 71 has been removed.	The guidelines have been amended.
	It also suggests the following change in the ensuing paragraph: '*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,*	Risks stemming from projects need to be considered in institutions' wider risk management frameworks.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	*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	One respondent suggested adding a reference to ISO 27001 A.14 on system/software development life cycle, as ISO 27001 can be considered an appropriate software solution. Another respondent asked that the principles of secure software development life cycles should be discussed in more detail.	The guidelines are technology agnostic; therefore, they do not refer to specific standards or technologies. Although having a secure software development life cycle is good practice, the EBA is not mandating it, but rather specifies principles to achieve similar outcomes.	No change.
Paragraph 73	One respondent suggested deleting the minimum requirements for the acquisition, development and maintenance of ICT systems to allow agile software development. Another respondent commented that the development/maintenance process requirements apply to all ICT systems. As these may be highly complex, high-risk systems or simple, low-risk systems, a risk-based process design should be possible. The respondent proposed using a risk-based approach and specifying that the points listed should be included in principle.	The guidelines aim to provide the facility for a risk-based approach; therefore, the comments have been accommodated by removing the specific requirements set out in items (a) to (d).	The guidelines have been amended.
Paragraph 73(d)	One respondent commented that not specifying applications for testing, approval and release would make the rollout of critical security patches for, for example, operating systems, unduly formal and therefore risky. The respondent proposed clarifying that *'**for financial applications, additionally** testing, approval and release….'*	The guidelines do not intend to be prescriptive. The intention of this requirement was for the security monitoring process to assist a financial institution to have a better understanding of its own systems and risks. As indicated in the previous comment, items (a) to (d) have now been removed.	The guidelines have been amended.
Paragraph 74	Two respondents suggested revising the wording to allow agile software development. They specifically suggested that the second sentence should be removed. One respondent commented that the proposed methodology suggests following a one-solution model; however, the respondent expressed a view that in DevOps product development scenarios, other methods should be considered. The risk can be mitigated by breaking the changes into classes of risk and automating testing batteries for defined risk levels. For example, lower risk issue testing can then be automated, thereby focusing development	The guidelines have been amended to ensure that financial institutions clearly define requirements for ICT systems, and that the guidelines are technology agnostic and would apply to agile software development.	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	resources on critical issues. This method serves to focus attention on the critical levels and meets the requirement of patching security fixes as fast as possible. One respondent suggested the additional wording: *'Financial institutions should ensure that before any acquisition or development of ICT systems takes place* ***(e.g. at the request for information phase),*** *[…].'*	Financial institutions should consider the results of their risk assessments when deciding what methodologies best suit them. These guidelines are technology agnostic and do not specify what specific standards or technology should be used to comply with the guidelines. The EBA amended the executive summary to explain that these guidelines are technology agnostic and hence the EBA does not specify what software development methodology and standards should be used.	No change.
Paragraph 75	Two respondents suggested a change in wording to allow more flexibility: '*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.*' Another respondent commented that only precautions can be taken, as 'prevention' cannot be fully ensured; therefore, a change of wording was suggested: '*Financial institutions should* ***take precautions ~~ensure that measures are in place~~*** *to prevent unintentional alteration ….'* Another respondent commented that the word 'development' creates confusion and sought clarification on what these measures should be.	The comment has been accommodated. The EBA has updated the text to focus the outcome on mitigating the risk. The EBA has amended the text to refer to 'development and implementation in the production environment'.	The guidelines have been amended. The guidelines have been amended. The guidelines have been amended.
Paragraph 76	One respondent proposed adding a reference to business criticality: '*Financial institutions should have a …. their first use.* ***This methodology should take into account the criticality of business processes and assets.***' Another respondent suggested an amendment to allow agile software development: ***~~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~~***	The EBA amended the text to make it more proportional and principle based: '*Financial institutions should have methodology in place for testing and approval of ICT systems prior to their first use.* ***This methodology should consider the criticality of business processes and assets. The testing should ensure that new ICT systems perform as intended.*** *~~When applicable, regression testing should be performed to ensure that new ICT systems perform in~~*	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	~~that the behaviour of the ICT systems in the production environment can be predicted and sufficiently tested.~~'	*~~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~~.'* These amendments also ensure that the guidelines are technology agnostic and do not specify what software development methodology and standards should be used.	
Paragraph 76	One respondent suggested mentioning other equally important test types apart from regression testing (i.e. unit testing, integration testing, user acceptance testing). They also suggested using 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. It proposed additional wording in paragraph 76: *'a) they should 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,* *b) they should use various testing methods, like integration testing, user acceptance testing and performance testing, align risk-based approach to ensure that ICT system has the acceptable characteristics, and* *c) if applicable, regression testing should be performed to ensure that new ICT systems perform in the same way as the previously developed and tested system(s) of the same function or the original system version.'*	These guidelines are technology agnostic and do not specify what specific types of tests should be used to comply with the guidelines. Financial institutions should decide what test types are best to ensure that new ICT systems perform as intended, depending on the criticality of business processes and assets that are affected by a change. They should also use test environments that adequately reflect the production environment. The reference to regression testing is removed.	No change.
Paragraph 77	One respondent requested a definition of 'errant coding practices.'	The text of the guidelines has been revised to provide more clarity on expected processes: '*Financial institutions should test ICT systems, ICT services and information security measures to identify* ***potential***	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		~~*errant coding practices and systems vulnerabilities that could lead to*~~ *security weaknesses, violations and incidents*'.	
Paragraph 77	One respondent suggested using the term 'penetration testing' in this section, similar to paragraph 76, which uses 'regression testing'. The suggested additional wording is *'**When applicable, penetration testing should be performed to identify system vulnerabilities**….'* In addition, the respondent suggested mentioning 'technical testing' and 'functional testing', instead of 'testing'.	The guidelines are sufficiently clear and principle based to require testing without specifying exactly what type is required.	No change.
Paragraph 78	Some respondents suggested replacing '~~unverified'~~ with '**unauthorised or unaccepted**'.	The word 'unverified' encompasses both unauthorised and unaccepted.	No change.
Paragraph 78	Some respondents highlighted a wide practice across the industry of copying production data to testing systems, and to ensure adequate segregation proposed the additional wording *'[…] 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 EBA amended the text to highlight the objective of protecting the confidentiality and integrity of production data in non-production environments. But the guidelines remain technology and methodology agnostic: *'**A financial institution should ensure the integrity and confidentiality of production data in non-production environments. Access to production data is restricted to authorised users.**'*	The guidelines have been amended.
Paragraph 79	One respondent suggested replacing '~~in a comprehensive manner~~' with '**according to best practices**', as reference to best practices avoids the lack of clarity in the term 'comprehensive manner' and caters for future developments in the protection of source code.	The EBA considers that use of the words 'best practices' would create more ambiguity, while 'in a comprehensive manner' is in line with the principle-based and proportionate approach of the guidelines.	No change.
	Another respondent commented that user documentation does not make sense for all systems, e.g. infrastructure systems, and proposed the following addition: *'should contain **(where applicable)** at least user documentation...'*	The comment has been accommodated.	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 79	One respondent requested clarity surrounding the desired outcome of this requirement — i.e. to assist in knowledge transfer from departing employees or to give existing employees an easier path to information discovery. The respondent agreed and acknowledged that source code integrity was critical to the success of any ICT system, but noted that many of the system components require specialised knowledge and may be intellectual property.	The EBA considers that the main purpose of this paragraph is to ensure the transfer of knowledge from departing employees.	No change.
Paragraph 79	One respondent expressed a view that this requirement was partially the same as paragraph 75.	The requirements in this paragraph are specific to source code management.	No change.
Paragraph 80	One respondent requested adding the definition of 'business-managed applications' and using standard definitions (e.g. COBIT, ISO, etc.) where possible.	In the context of this paragraph, business managed applications are merely an example of '*ICT systems developed or managed by the business function's end users outside the ICT organisation'*. The EBA considers the current wording of the guidelines to be sufficient, as it is in line with the relevant regulation.	No change.
Paragraph 80	One respondent requested clarity on the desired outcome of this measure. The respondent said that financial institutions' processes for acquisition and development of ICT systems should not necessarily apply to systems developed outside the organisations. For instance, if telephone systems are outsourced to a provider, the ICT function should manage the performance of the outsourced telecommunications service through an SLA and understand the risks and controls surrounding this outsourcing.	The desired outcome of this paragraph is to ensure that ICT systems managed outside the ICT organisation are subject to the same controls as those managed by the ICT organisation. The EBA is of the view that, as a rule, PSPs should enter into a contract with their outsourcing providers for the provision of payment services. Any form of contract should be concluded between the PSP and its outsourcer, not with the PSU. The EBA is aware that in some cases PSPs may not have close a relation with sub-outsourcing providers because the whole process is under the control of the primary outsourcing providers. The EBA is also aware that PSPs might not enter into contracts with suppliers of end user devices,	

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		such as tablets or smartphones, or with providers of operating systems.	
Paragraph 80	One respondent requested clarity on the term 'risk-based manner'.	The term risk-based manner is the same as risk-based approach, which has been used in other places throughout the text. This means that it is up to an institution to define the process applicable for the management of the business-managed applications based on the risk and criticality of these systems. The wording has been amended to be consistent with other parts of the guidelines.	The guidelines have been amended.
4.6.3. ICT change management	One respondent suggested adding a comment regarding the 'post-implementation review', which should give assurance that the change implementation has been done successfully without unexpected impacts. Based on a risk assessment, a 'post-implementation review' may be required for new implementations as well as for changes to implementations. The suggestion was also made for this section to mention proper change documentation, control and approval.	The EBA has updated the text in this paragraph to be more principle based, removing specific requirements of certain elements of the change management process to ensure that financial institutions focus on outcomes of the change management process and have sufficient flexibility to achieves these outcomes. Furthermore, the incident and problem management process will provide additional assurance if the implementation is not successful.	The guidelines have been amended.
Paragraph 81	One respondent requested clarification or confirmation that this paragraph covers a risk-based approach. The respondent agreed that an ICT change management process should be in place, but suggested that not all ICT systems are equally qualified/sensitive.	The EBA confirms that paragraph 75 considers a risk-based approach and that financial institutions should consider the impact of the proposed changes and the potential implementation risks.	No change.
Paragraph 81	Two respondents suggested that the requirements in this paragraph were too prescriptive. One respondent proposed the following changes: '*Financial institutions should establish and implement an ICT change management process to ensure that all changes to ICT systems are*	The EBA has updated the text in this paragraph to be more principle based, removing specific requirements of certain elements of the change management process to ensure that financial institutions focus on outcomes	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	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.***~~ ' Another respondent requested outcome-based requirements that allow organisations to demonstrably meet the goals set in the guidelines without necessarily imposing a specific deployment process. They provided an example that some recurring changes deemed to be low-risk changes may be undertaken by automated systems. Under such a model, a risk assessment is performed for the class of changes, and automated procedures are developed and tested, but each individual change is not independently authorised or formally accepted (although	of the change management process and have sufficient flexibility to achieves these outcomes by removing the prescriptive items (a) to (f).	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	each change would be independently logged for traceability). Such a mechanism allows a repetitive activity to be undertaken over time in a consistent and scalable manner.		
General comment	One respondent commented that the implementation of the requirement in paragraph 81(c) seems to align with the requirements detailed in the BIS BCBS's 'Principles for the sound management of operational risk' regarding 'Principle 7: Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.' The respondent recommended considering referring to this document, as it would help clarify and trace requirements to their potential source.	The EBA agrees that ICT and security risk management is a subset of operational risk; however, there is no benefit to adding a reference to it in the guidelines.	No change.
Paragraph 81(c)	One respondent commented that not all changes can be tested absolutely (e.g. keys), and proposed the following addition: *'testing and independent validation processes of ICT systems' changes for possible compatibility and security implications prior to deployment to production environment, **if technically possible**'*.	The EBA has updated the text in this paragraph to be more principle based, removing specific requirements of certain elements of the change management process to ensure that financial institutions focus on outcomes of the change management process and have sufficient flexibility to achieves these outcomes, by removing the prescriptive items (a) to (f), including item (c) on testing.	The guidelines have been amended.
Paragraph 81(d)	One respondent proposed additional wording: *'an authorisation process, only after which ICT changes **are permitted t**o move to production.'*	As per comment above, item (d) has been removed.	The guidelines have been amended.
Paragraph 81(e)	Two respondents requested the clarification of the term 'asset owners'. In paragraph 19 there is reference to 'asset owners' who are accountable for the classification of the information assets. In paragraph 81(e), the reference to the 'asset owner' seems to be different, and it is unclear whether it refers to the business owner or the ICT person responsible for the application.	As per comment above, item (e) has been removed.	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 81(e)	One respondent requested a definition of 'urgent or emergency ICT changes', using standard definitions (e.g. COBIT, ISO, etc.) where possible.	The EBA has updated the text to provide more clarity on how these changes need to be managed: *'**Financial institutions should handle the changes during emergencies (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards**.'*	The guidelines have been amended.
Paragraph 82	One respondent suggested that the requirements in this paragraph were too prescriptive and proposed the following changes: '*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* ***in accordance with the financial institutions formal change management process****.* ~~***part of financial institutions' formal change management process, which should ensure that changes are properly planned, tested, documented and authorised.***~~	The comment has been accommodated.	The guidelines have been amended.
4.7. Business continuity management	One respondent suggested that the guidelines should remain focused on minimum standards for ICT and security risk management and that the requirements in the guidelines that relate to areas that are not directly related to technology resilience, such as references to business continuity management, are identified and removed. This would ensure that the guidelines are focused on ICT risks and would avoid inconsistent or duplicative requirements.	The EBA considers that ICT is an essential part of business continuity management and that it would be counterproductive not to include business continuity management in the context of the overall objectives of these guidelines. Furthermore, this is necessary for institutions within the scope of PSD2 that are not within the scope of the EBA Guidelines on internal governance (EBA/GL/2017/11).	The guidelines have been amended.
General comment	One respondent welcomed a risk-based approach for business continuity management of ICT systems and services and encouraged the alignment, where relevant, with key concepts developed by the UK authorities in their proposed approach to operational resilience.	ICT and security risk management is a part of operational resilience. The UK approach is not yet finalised and any alignment efforts at this stage would not be useful due to the different stages of progress.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
General comment	One respondent made a general comment that most of the guidelines regarding business continuity are acceptable. In some cases, however, the complexity of a financial institution is taken into account and at other times the requirements for the content of plans (BCP and recovery plans) are much too detailed. This will lead to plans that are unmanageable, unmaintainable and practically not usable.	The EBA considers that the level of detail in the guidelines is sufficiently practical to achieve the desired outcomes while providing institutions with the flexibility to do so.	No change.
General clarification	One respondent suggested that the implementation of requirements in paragraphs 83 to 97 seems to align with the requirements detailed in BIS BCBS's 'Principles for the sound management of operational risk' regarding 'business resiliency and continuity: Principle 10', and recommended referring to this document, as it would help clarify and trace requirements to their potential source.	The EBA agrees that ICT and security risk management is a subset of operational risk; however, adding reference to it in the guidelines would create confusion.	No change.
BCM is treated as a subset of ICT	Two respondents stated that it was unclear why BCM is treated as a subset of ICT risk. One respondent commented that this may lead to a new layer of requirements as opposed to business continuity planning for business as a whole, and risks confusion, mixed control standards and the potential duplication of effort with no material benefit. The approach in the guidelines diverges from the emerging approaches and supervisory focus on end-to-end service availability and accountability at the service level. Another respondent recommended reconsidering the inclusion of the BCM elements outlined in this section to avoid introducing unnecessary complexity to institutions and a potentially siloed approach to BCM. By setting specific requirements for one function (i.e. ICT), at the expense of all other functions, the guidelines would undermine this emerging approach. They would create a discrete and additional layer of BCM requirements specifically for ICT, as opposed to the business as a whole.	BCM is not a subset of ICT and security risk. However, in the context of these guidelines, BCM is an important concept for the mitigation of ICT and security risks. On completely separating BCP from business, the EBA's view is that it would be counterproductive to separate ICT from the rest of the business process; thus, these are considered where relevant (see comment on Section 3.7). The EBA updated the executive summary with the following clarification with regard to Section 3.7: *'Section 3.7 specifies expectations with regard to business continuity management and developing response and recovery plans, including testing, and their consequent updating based on the testing results. Financial institutions should ensure that they have effective crisis communication measures in place so*	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	It argued that this section of the guidelines varies from providing very specific guidance for ICT functions to providing more strategic requirements for an institution's overall BCM. The respondent said that the guidance applies a narrow lens to BCM, which may deflect focus from other, equally important, impact types and that effective assurance for large global banks relies on an approach that can be consistently applied across all business divisions and jurisdictions.	*that all relevant internal and external stakeholders can be informed in a timely manner. '**The ICT business continuity management processes are an integral part of the overall institution's business continuity management process and should not be separated**.'*	
Paragraph 83	One respondent suggested that this could refer to the preparation phase of BCM when high-availability solutions (e.g. redundancy, data mirroring) can minimise the probability of an ICT system and/or service outage. This 'going concern' approach should be given at least as much emphasis in the BCM process as is given to those preparations that activate after the ICT disaster happens ('gone concern'), where truly the main concerns are limiting losses, disaster containment and making the systems operable again.	The EBA considers that this paragraph is relevant to BCM, whereas the processes defined in the other parts of the guidelines (e.g. risk management, change management, information security and vendor management) ultimately support a financial institution's operational resilience, including ICT.	No change.
4.7. (including paragraphs 93 to 95)	One respondent proposed that, although financial market infrastructures (FMIs) are a subset of the bank's interdependencies, Section 4.7 (including paragraphs 93 to 95) should caveat the guidelines with an appropriate qualifying statement to exempt banks from the responsibility of FMIs' business continuity planning and ongoing BCM governance. The respondent explained that financial institutions are reliant on third party service providers, including FMIs as payment, clearing and settlement operators, to ensure continuity of services to the customer. FMIs are subject to regulatory requirements for their resilience framework (such as the ECB's cyber resilience oversight guidance for FMIs or the principles for FMIs issued by the BIS and IOSCO). However, it is not always within the control of an individual bank or financial institution to mandate or ensure compliance of an	The EBA considers that it is the financial institution's responsibility to assess risks to its business processes, including risks from FMIs and to design measures to recover affected business processes. Institutions should consider alternative processes if there is a failure of an FMI.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	FMI's business continuity planning or to test its response and recovery capabilities.		
4.7.1. Business impact analysis	One respondent noted that the principle of proportionality applies to all requirements included in the draft guidelines. A system for business continuity management is built on a BIA, which enables the identification of critical processes, for which appropriate mechanisms should be in place to ensure business continuity. Depending on the scale of operations and the size of the enterprise, in accordance with the principle of proportionality, the analysis should provide information on the requirements for business continuity management.	The EBA confirms that the principle of proportionality applies throughout these guidelines.	No change.
Paragraph 84	One respondent requested clarification on whether paragraph 84 resembles paragraph 17.	Paragraph 17 covers the identification of functions, processes and assets, whereas paragraph 78 defines BIAs. However, the outcomes of the analysis performed in paragraph 17 can be used for the BIA in paragraph 78.	No change.
Paragraph 84	One respondent suggested amending paragraph 84 in such a way that a scenario analysis is not expected to be a mandatory part of a BIA. They commented that, as part of sound business continuity management, financial institutions should conduct a BIA by means of, among other things, scenario analysis. They pointed out that, according to their understanding, the scope of the BIA is to analyse a financial institution's exposure to severe business disruptions. The impact derived from such disruptions does not change depending on the underlying scenario (the root cause triggering the disruption). Consequently, scenario analyses do not provide added value within this context. In contrast to this, scenario analyses can add value in other areas of business continuity management, such as business continuity planning, response planning and testing.	The EBA considers that scenario planning is an effective way to assess the impact of severe business disruptions. However, the guidelines do not limit the BIA to scenario testing only, as its main aim is to assess exposure to severe business disruptions and their potential impact.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 84	Two respondents requested clarification of which criticality dimension paragraph 84 refers to, as the guidelines consider criticality in an extended sense, assessing the dimensions of confidentiality, integrity and availability as well as continuity.	The criticality assessment is defined in Section 3.3.2 as referred to in this paragraph; also integrity and in particular availability as described in paragraph 78 are roughly equal to the term 'continuity').	No change.
Paragraph 84	Two respondents requested clarification of what 'external data' refers to.	This has been clarified by adding that external data can include third party provider data relevant to a business process or publicly available data that can be relevant to the BIA.	The guidelines have been amended.
Paragraph 84	One respondent requested clarification of whether BCP requirements need to be included in the BIA.	The outcomes of the BIA are used in designing the BCP as explained in paragraph 80.	No change.
Paragraph 85	One respondent suggested that this section could discuss in more detail other high-availability solutions relevant to different disaster scenarios (e.g. disaster recovery as a service (DRaaS), cloud solutions, active-active geo-redundant data centres, asymmetrical data mirroring methods against software errors replicating real-time online, etc.).	The EBA does not refer to specific technologies, to ensure that the guidelines are technology agnostic and future proof.	No change.
4.7.2. Business continuity planning	One respondent suggested that the reference to disruption of business services in paragraphs 86 to 88 (e.g. 'severe business disruption that') appears highly aligned with the overall approach currently taken by the UK authorities, and potentially the Basel Committee, on operational resilience, and recommended considering a reference to operational resilience, to avoid potential inconsistencies or divergent approaches being developed.	As noted in earlier comments, adding references to other documents within the guidelines would create confusion.	No change.
	One respondent suggested that, due to financial institutions outsourcing ICT functions, BCM provisions must be included in the respective SLAs. It recommended that such a requirement is included in Section 4.7.2. They noted that paragraph 92 discussed only the outsourcing parties' responsibilities in the recovery plans.	These provisions are sufficiently covered in the EBA Guidelines on outsourcing and should not be replicated here.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraphs 86 and 96	Some respondents suggested removing any reference to prescriptive activities expected from the management body, such as the documentation and approval of business continuity plans (paragraph 86) or the requirement that identified deficiencies resulting from tests should be analysed, addressed and reported to the management body (paragraph 96). The respondent also suggested reconsidering the need for the management body to approve specific risk-type policies. Another respondent commented that the management body should approve the strategy but not the specific BCPs of all functions; therefore, approval of BCPs should be done by the executive management. One respondent proposed adding the designation '*documented and approved by* ***appropriate*** *management body* or **responsible management**', in order to cater for different internal organisation structures. Also the term 'management body' refers to board level and BCPs are usually described at a much more technical level than the board is used to.	The EBA considers that the approval of the business continuity plans and the review of the results of tests are consistent with the management body's management and supervisory functions as defined in the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2017/11). The management body in its supervisory function oversees and challenges the management function and provides appropriate advice. The management body should monitor, periodically review, and address any weaknesses identified regarding the implementation of processes, strategies and policies.	No change.
Paragraph 86	Two respondents proposed adding the wording *'**Besides other risks**, the plans should support […]',* as BCPs cover all risks, not only ICT risks.	The risks are considered in the previous sentence, so there is no need to repeat them.	No change.
Paragraph 86	Two respondents proposed deleting *'**~~the confidentiality, integrity and availability of~~**'*. One respondent argued that 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 cause problems of continuity but not necessarily).	Incidents and disruptions can affect confidentiality, integrity and availability, so this should be addressed by the BCPs. Continuity is covered by availability.	No change.
Paragraph 86	One respondent commented that disaster recovery (the ICT service continuity) should/can be treated separately in accordance with ISO standards.	The EBA considers BCPs and disaster recovery processes as separate but complimenting each other. The BCP is aimed at ensuring that an institution can continue operating, while the disaster recovery process is aimed at recovery activities. The EBA does not specify which standards should be used.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 86	One respondent suggested that financial institutions need to assess their dependencies from third parties and, where necessary, analyse whether the business continuity and disaster recovery measures put in place by third parties satisfies/aligns with the requirements of the financial institutions. One respondent requested that Section 4.7.2 should reflect more the BCP process and its connection with third party vendors — BCPs must cover this area — than the continuity related to services provided by external parties.	Section 3.7.1 refers to the necessary considerations for the BIA, which should consider third parties as per Section 3.3.2. Furthermore, more guidance on BCM related to third party providers relationships is provided in the EBA Guidelines on outsourcing. For clarification, paragraph 78 has been revised to include a reference to 'third parties': *'[…]The BIAs should also consider the criticality of the identified and classified business functions, supporting processes**, third parties** and information assets, and their interdependencies, in accordance with Section 3.3.3.'*	The guidelines have been amended.
Paragraph 87	One respondent commented that the RTO is an objective. If a maximum time was required, it suggested using the term maximum tolerable outage (MTO).	RTO is an objective, since meeting the envisaged time is never guaranteed. In addition, the term MTO is much less known, and, in practice, RTO covers MTO. The EBA has updated the text of paragraph 81 to make it clearer that the objective of the BCPs is to recover processes within RTO: *'Financial institutions should put BCPs in place to ensure that they can react appropriately to potential failure scenarios and that they are able to **recover** ~~and maintain~~ the operations 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 it is acceptable for data to be lost in the event of an incident).'*	The guidelines have been amended.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 87	One respondent viewed imposing a sector critical standard that required entities to establish a specific RTO for their sector critical systems as impractical, technically infeasible and potentially a risk to financial stability and a contagion risk. A more practical and feasible approach is one that focuses more broadly on resumption of service, measured by the entity's best efforts to ensure the ability to safely meet contractual and regulatory service obligations.	The guidelines do not set a specific RTO value, but the guidelines do require that one is established by the institution in order to have a proportionate and applicable objective for recovery that would involve planning for the necessary efforts for meeting contractual and regulatory service obligations.	No change.
Paragraph 87 RTO and RPO definition	One respondent suggested that application would be facilitated and confusion avoided by re-using established and well-known definitions from international standards when available, e.g. the ISO 22301 standard definitions for RTO and RPO. It proposed to (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.**'; and (2) align the definition of the RPO with ISO 22301: '**The point to which information used by an activity must be restored to enable the activity to operate on resumption**.'	These guidelines are technology agnostic and do not specify what specific standards or technology should be used to comply with the guidelines. RTO and RPO were sufficiently defined in the Guidelines on ICT risk assessment under SREP. As there were no changes introduced, the EBA does not see it necessary to repeat definitions provided there.	No change.
Paragraph 87	One respondent suggested to add '**timely** maintain **or restore**' and '**minimum** operation **requirements**', in order to add a critical characteristic of what BCM should ensure, which is ensuring the minimum operation requirements for time-critical business functions if there is a major disruption/crisis. The suggested revised wording is *'and that they are able to **timely** maintain **or restore** the **minimum** operation **requirements** of their critical business activities after a disruption within a recovery time objective'.*	The guidelines are sufficiently proportionate to allow institutions to decide the best way to comply with these requirements without setting minimum requirements and allowing institutions to set those timely operational requirements through their RTOs and RPOs.	No change.
Paragraph 87	One respondent requested more explanation and examples of how *'financial institutions should prioritise business continuity actions using a risk-based approach'.* It asked if a previous risk assessment is needed to decide which BCP to choose if several BCPs exist depending on the scenario, and if a business disruption implies the use several of them.	The prioritisation requirements will define how the recovery of business processes or systems should be prioritised depending on their criticality, for example by giving restoration priority to the most critical and time-sensitive processes. If separate BCPs are created for	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		scenarios, the term BCP in this document points to the collection of these plans.	
Paragraph 87	One respondent commented that this mix of disaster recovery and ICT security incidents is not the best practice in the industry, given the fact that these are two different processes that have different characteristics.	Paragraph 81 refers to failure and disruption, with the objective of ensuring business continuity and disaster recovery, irrespective of the source of failure or disruption.	No change.
Paragraph 88	One respondent requested clarification of this paragraph, as it implies that ICT is responsible for certain fraud scenarios, e.g. phishing. The responsibility for fraud scenarios lies with fraud operations.	Paragraph 82 refers to extreme but plausible scenarios, including cyber-attacks. Institutions need to consider scenarios that affect their ability to provide services. Phishing and fraud may result in disruption (e.g. phishing can spread ransomware). Institutions need to consider how they would recover from the results of these activities.	No change.
4.7.3. Response and recovery plans	One respondent suggested that regarding the BCM measures, it should be sufficient from a host competent authority perspective that BCM measures could also be implemented by the parent entity of a cross-border group if the parent entity is situated in an EU Member State. Furthermore, guidance is needed with regard to BCM measures provided by parent entities in third countries. The respondent suggested aligning this with the supervisory equivalence decisions, which allow countries recognised as equivalent to be treated in a similar way to Member States.	Each institution should consider how BCM is implemented in their particular entity. If support and services are provided from another legal entity, this needs to be considered as part of the requirements in Sections 3.3.2, 3.7.1 and 3.7.2.	No change.
Paragraph 89	There were two comments to review the cross-references, e.g. paragraph 87 should be paragraph 88.	The guidelines have been updated.	The guidelines have been amended.
Paragraph 90	Two respondents requested that the meaning of 'short-term' and 'long-term' are clarified.	The EBA considers that providing a more detailed description will not be proportionate, as it is up to the	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		institution to define the length of short- and long-term periods, based on a relevant BIA. However, as a general practice, short term refers to hours or days, whereas long term refers to days and months.	
Paragraph 91	One respondent suggested that paragraph 91 should be deleted, as it was unnecessary. It argued that to require a second plan with alternative options undermines the requirement to have solid response and recovery plans in the first place. Paragraph 90 already requires short- and long-term recovery options, which covers alternative options.	The objective is to address the fact that sometimes recovery is not possible, for example if a main system and backups are deleted. Thus, alternative workaround considerations are required.	No change.
Paragraph 91	Two respondents suggested deleting the reference to '~~**unforeseen circumstances**~~', as it makes the perimeter of the BCP extremely broad. The suggested wording is *'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 proposal would be limiting and the guidelines intend to capture a broad range of circumstances that may lead to the need for alternative options.	No change.
4.7.4. Testing of plans	One respondent recommended considering how mutual recognition of tests could be achieved in order to satisfy cross-jurisdictional requirements where firms operate across jurisdictions.	Each legal entity should consider how BCM is implemented in their particular entity. If support and services are provided from another legal entity, this needs to be considered as part of Sections 3.3.2, 3.7.1 and 3.7.2	No change.
	One respondent suggested that testing activities could be broken down into two categories: 'table top exercises' and 'simulation scenarios'. Although the latter provides a clear view of a plan's effectiveness, table top exercises assist in optimising the plans (prior to the simulation tests) without any disruption to business operations.	The EBA considers that it is appropriate to avoid referring to table top exercises, in order to maintain a principle-based approach.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 93	One respondent generally agreed that testing of operations was an important aspect of risk management in general, and of BCPs in particular, and was of the opinion that testing of services provided by third parties should be limited to 'where applicable'. This follows widely applicable standards on outsourcing and is in line with paragraph 95(a), according to which financial institutions' testing of BCPs should include 'testing of services provided by third parties, where applicable'. An additional wording was proposed: *'Financial institutions should test their BCPs, and ensure that the operation of their business functions, supporting processes, information assets and their interdependencies (including those provided by third parties**, where applicable**) are tested at least annually.[…].'*	The comment has been accommodated.	The guidelines have been amended.
Paragraph 93	One respondent suggested considering reviewing the expectation of annual testing of critical business functions. It suggested that testing could be required when relevant changes occur or at least every 3 years, rather than on an annual basis. Another respondent suggested that a general requirement to test BCPs annually is unreasonable, as testing should be geared to risk/protection needs. A change of wording was proposed: '*are **~~tested at least annually~~** **regularly***.'	The guidelines aim to harmonise requirements for critical business functions and to test plans periodically. The guidelines do not require everything to be tested annually, only the critical aspects.	The guidelines have been amended.
Paragraph 94	One respondent suggested considering reviewing the expectation of annual updates of BCPs. It suggested that updates could be required when relevant changes occur or at least every 3 years, rather than on an annual basis. Another respondent suggested that a general requirement to update BCPs annually is unreasonable, as updating should be geared to	See comment above.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	risk/protection needs. Change in wording proposed: '*BCPs should be updated* ***~~at least annually~~*** ***on given occasions****, based on testing results.*'		
Paragraph 94	One respondent commented on *'BCPs should be updated at least annually, based on testing results, current threat intelligence and lessons learned from previous events'* and suggested that in business continuity this should be called horizon scanning.	No changes are required, as paragraph 88 defines what needs to be considered to update the BCP, and introducing a new term may create more confusion.	No change.
Paragraph 95	One respondent suggested aligning the terms and concepts related to operational resilience (e.g. 'adequate set of severe but plausible testing scenarios', 'demonstrate ability to sustain the viability of the business until critical operations are re-established') with terminology proposed by the UK authorities in their approach to operational resilience.	Please refer to previous general comment on Section 3.7.	No change.
Paragraph 95(a)	One respondent requested a clarification in the case of including '*an adequate set of severe but plausible testing scenarios*'. It raised a question of whether if the critical functions are tested independently, that is first a critical function is recovered and then another, and so on, it can it be considered to be a severe testing scenario.	An institution's BCP planning and testing should be based on a BIA and the respective criticality assessment of business processes. The recovery order should be defined in the plan and subsequently tested to ensure that assumptions made during planning can be implemented in practice.	No change.
Paragraph 95(a)	One respondent suggested that there should be flexibility in the execution of the disaster recovery tests and suggested replacing 'should' with 'could'. The proposed change in wording is '*This* ***~~should~~*** ***could*** *include the switch-over of critical business functions […]'.* Another respondent suggested removing the second sentence, as the switch-over called for under paragraph 95(a) is impracticable and harbours additional risks — no backup system is available for the duration of testing. ***~~'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.~~***'	The guidelines need to set out requirements and could not provide the necessary requirement for such a test. The EBA considers that testing the switch-over of critical business functions is necessary for all institutions, but the requirement provides sufficient flexibility, as it guides institutions to perform tests in a certain way, but also allows them to use different methods to achieve the same outcome.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 95(a)	One respondent commented that this paragraph suggests that use of redundant infrastructure (e.g. servers, data centres) must be implemented, but the requirement to have such infrastructure at those levels should be a result of a BIA, risk assessment analysis and the RTO parameters defined and the ability of the financial institution to recover services within the RTO time. If the RTO time does not exceed the maximum time and the financial institution is able to recover its services to normal operations in their primary location, then an extra recovery environment may not be required.	The guidelines allow that individual systems redundancy is a mechanism to ensure ongoing resilience, whereas paragraph 89(a) refers to testing disaster recovery. Also, please note that paragraph 89 mentions 'until critical operations are re-established'. This highlights that this is not a blanket requirement for everything. The EBA considers that financial institutions should test existing infrastructure and not create additional structures.	No change.
Paragraph 96	One respondent suggested that reporting to the management body should be confined to key aspects. The change in wording proposed is *'Test results should be documented and ~~any~~ identified **main findings or** deficiencies…..'.*	The comment limits the assessment, remediation and reporting of identified issues to the main ones that may lead to an institution's inability to recover if less serious issues are not addressed but in combination can contribute to a wider failure.	No change.
4.8. Payment service user relationship management	There was a suggestion to add an acronym: '*4.8. Payment service user **(PSU)** relationship management*'	The acronym if already defined.	No change.
4.8. Payment service user relationship management	One respondent commented that while the term 'PSP' is used throughout the guidelines, certain requirements in this section seem to be only applicable to either a credit institution or a TPP. The guidelines should therefore specify when a requirement applies to all types of PSPs and when they are directed specifically at an account servicing payment service provider (ASPSP), a payment initiation service provider (PISP) and/or an account information service provider (AISP). Specific reference was made to paragraphs 101 to 103, that in their view should only apply to ASPSPs. Establishing or disabling specific payment functionalities should be initiated and processed only by these entities,	The EBA considers that all guidelines should apply to all PSPs so as not to favour specific business models and to ensure technological neutrality. Therefore, the guidelines require all security measures to be complied with by each addressee in relation to the payment services they provide, regardless of the size of the PSP and the business model followed. However, the guidelines are subject to the principle of proportionality, set out in Section 3.1, which means	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	as this is the level at which the decision is made, i.e. Directive 2015/2366/EU (PSD2) does not allow for establishing or disabling specific payment functionalities through a TPP.	that the steps that PSPs are required to take to be compliant may differ between PSPs, depending on their size and the nature, scope, complexity and riskiness of the particular service(s) they provide or intend to provide.	
Relationship between the TPPs and the ASPSPs	One respondent suggested that to make the relationship between the TPPs and the ASPSPs transparent for PSUs, the PSU should always be made aware by TPPs that they are not acting on behalf of the ASPSP. This will help ensure stronger consumer protection, as it will allow PSUs to make more informed decisions and maintain consumers' trust in the developing payments system. In order to prevent the trust that the PSUs have in the ASPSPs from being misused, the respondent suggested that Section 4.8 require the TPPs to clearly articulate to the PSUs whether or not it is acting on behalf of the ASPSP. To make such a statement obvious to the PSU, it could be provided in a disclaimer when an instruction is initiated or added to the TPP's documentation or guidance for the PSU.	The EBA agrees with the comment that the PSU should always be aware of which PSP is responsible for the service in question. This concern has been reflected in the executive summary section of the guidelines: '*The EBA stresses the importance of ensuring transparency, such that PSUs are always aware of which PSP is responsible for providing them with the payment service.'*	The guidelines have been amended.
Section 4.8 — General comment	One respondent suggested that Section 4.8 covers responsibilities that are outside the scope of ICT; these are covered by operations. This lies outside the mandate of the chief information officer.	These guidelines focus on ICT and security risks as well as on security risks, which can be of an operational nature. Proper communication with the PSU is to be seen as an important element of an integrated risk management approach in this context.	No change.
Paragraph 98 — Consent of a PSU	One respondent questioned whether the consent of a PSU was required to send such awareness information (campaigns, bulletins, etc.).	The EBA assumes that such consent is already included in the general contractual agreements related to the corresponding payment service. It is not in the scope of these guidelines to define any contractual requirements in this context.	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 100	One respondent commented that the wording 'where product functionality permits' creates an ambiguity about whether this is optional or not. Another respondent suggested that this requirement appeared to be onerous from a merchant's point of view and requested a clarification of the desired outcome for this approach. For example, in many payment instances a PSP was integrated into the merchant application via an API call (white label service), to facilitate a simple integration into the business. The respondent noted that requirements in paragraph 100 will require many businesses to rewrite applications.	As it is a requirement under these guidelines, it is not to be seen as optional. However, it should only be provided if product functionality permits such an approach. A possible use could be disabling the ability to make foreign payments if the user wishes to. In this context the proportionality principle set out in Section 3.1 should also be considered.	No change.
Paragraph 102	One respondent recommended informing the PSU about other security-related events as well, for example master data changes (e.g. customer's phone numbers, passwords) and other non-transaction-based events that could help prevent fraudulent activities.	The EBA agrees in principle with the respondent. However, the focus of these guidelines should be on transactions. This does not exclude the fact that PSPs might offer additional functionalities if considered useful.	No change.
Paragraphs 103 and 104	One respondent commented that there is no differentiation made between PSUs that are consumers and PSUs that are corporate clients. With regard to corporate clients, PSPs could expect a more elaborate knowledge and understanding of risks and threats related to payment services than PSUs that are consumers. It should be appropriate to amend a risk-based approach to these provisions to enable differential treatment of PSUs with regard to the scope of information needed.	The EBA agrees in principle with the respondent but would like to point out that, even if there is no explicit differentiation in the wording of these guidelines, this does not exclude a differentiation being made in practice. In this context the proportionality principle set out in Section 3.1 should also be considered.	No change.
Paragraph 103	One respondent acknowledged the role of PSPs in keeping PSUs informed of security updates but suggested that there is a potential risk to the level playing field and to financial stability if further consideration of a horizontal data sharing framework is not developed under PSD2.	These guidelines derive from the mandate to issue guidelines in Article 95 of Directive (EU) 2015/2366 (PSD2). That means that they are developed under PSD2 and fulfil the requirements of PSD2 to establish a level playing field.	No change.
5.1. Draft cost-benefit	One respondent recommended in Section 5.1A adding a new point iii. The suggested wording is *'ii. the increasing reliance on third parties for ICT services and products, often in the form of diverse packaged*	The EBA considers that this is covered by reliance on third parties (item ii).	No change.

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
analysis: impact assessment	*solutions resulting in manifold dependencies and potential constraints and concentration risks.* ***iii. increased dependencies between the actors of the financial sector and the ICT infrastructures supporting the sector**.'*		

Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu