EBA/GL/2017/17

12/12/2017

Final Report

Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)

Abbreviations

AIS	account information service
AISP	account information service provider
ASPSP	account servicing payment services provider
BCBS	Basel Committee on Banking Supervision
BCP	business continuity plan
CA	competent authority
CP	Consultation Paper
CRR	Capital Requirements Regulation
CSC	common and secure communication
EBA	European Banking Authority
ECB	European Central Bank
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
GL	Guidelines
ICT	information and communication technology
ISO	International Organization for Standardization
ISMS	information security management system
NIS	(Directive (EU) 2016/1148 on security of) network and information systems
NIST	National Institute of Standards and Technology
PIS	payment initiation service
PISP	payment initiation services provider
PSC	personalised security credentials
PSD2	Payment Services Directive (EU) 2015/2366
PSP	payment service provider
PSU	payment service user
SCA	strong customer authentication
SREP	Supervisory Review and Evaluation process
TPP	third-party provider

Contents

1. Executive summary

Directive (EU) 2015/2366 on payment services in the internal market (PSD2) entered into force in the European Union on 12 January 2016 and will apply as of 13 January 2018. One of the 12 mandates conferred on the European Baking Authority (EBA), as specified in Article 95 of PSD2, requires the EBA to develop, in close cooperation with the European Central Bank (ECB), Guidelines (GL) on the security measures for operational and security risks of payment services.

More specifically, PSD2 provides that payment service providers (PSPs) shall establish a framework with appropriate mitigation measures and control mechanisms to manage operational and security risks relating to the payment services they provide.

In fulfilment of this mandate, the EBA has taken into account the existing EBA Guidelines on the Security of Internet Payments under PSD1 (EBA/GL/2014/12), and has also used as a basis existing standards and frameworks in other areas related to operational and security risks and has adapted them where appropriate to the specificities of payment services. The EBA and the ECB have also carried out a risk analysis to determine the main threats and vulnerabilities to which PSPs are exposed.

These resultant Guidelines set out the requirements that PSPs should implement in order to mitigate operational and security risks derived from the provision of payment services. GL 1 defines a general principle on proportionality. This is then followed by GL 2 to GL 9, which cover governance, including the operational and security risk management framework, the risk management and control models, and outsourcing; risk assessment, including the identification and classification of functions, processes and assets; and the protection of the integrity and confidentiality of data and systems, physical security and access control.

Furthermore, the Guidelines cover the monitoring, detection and reporting of operational or security incidents; business continuity management, scenario-based continuity plans including their testing and crisis communication; the testing of security measures; situational awareness and continuous learning; and the management of the relationship with payment service users (PSUs).

To seek the views of the market, the EBA published on 5 May 2017 a Consultation Paper (CP) on the draft Guidelines on the security measures for operational and security risks of payment services. The consultation ran for three months, and 43 responses were received. Following analysis of the comments received from the market, the EBA has made some amendments to the Guidelines. These include, in particular, some clarifications requested by respondents concerning the scope of the Guidelines; the addition of some definitions; some clarifications of particular terms used in the Guidelines; changes to the level of detail (or lack thereof) of the Guidelines; the articulation of the proportionality principle; and clarifications as to the certification process.

2. Background and rationale

2.1 Background

1. Directive (EU) 2015/2366 on payment services in the internal market (PSD2) entered into force in the European Union on 12 January 2016 and will apply as of 13 January 2018. PSD2 has conferred 12 mandates on the EBA, one of which requires the EBA to develop, in close cooperation with the ECB, Guidelines on the security measures for operational and security risks of payment services (Article 95 of PSD2).

2. In accordance with Article 95(1) of PSD2, 'payment service providers (PSPs) shall establish a framework with appropriate mitigation measures and control mechanisms to manage operational and security risks (hereafter "risk management framework"), relating to the payment services they provide. As part of that framework, PSPs shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents'.

3. Furthermore, in accordance with Article 95(2) of PSD2, PSPs shall provide 'to the competent authority (CA) on an annual basis, or at shorter intervals as determined by the CA, an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures implemented in response to those risks'.

4. In support of these provisions, Article 95(3) requires the EBA, in close coordination with the ECB, and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, to issue Guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 with regard to the establishment, implementation and monitoring of the security measures, including certification processes where relevant.

5. Moreover, the EBA shall promote cooperation, including the sharing of information, in the area of operational and security risks associated with payment services among the CAs, and between the CAs and the ECB and, where relevant, the European Union Agency for Network and Information Security (ENISA).

6. These Guidelines are one of the three security-related mandates conferred on the EBA in PSD2, and which the EBA has developed in close cooperation with the ECB. They complement the Regulatory Technical Standards (RTS) on strong customer authentication and common and secure communication under PSD2 (EBA/RTS/2017/02), which were submitted to the European

Commission for adoption on 23 February 2017,[1] and the Guidelines on major incidents reporting under PSD2 (EBA-GL-2017-10), which were published on 27 July 2017.[2]

7. On 5 May 2017, the EBA launched a consultation on the draft Guidelines, which ended on 7 August 2017. The EBA received 43 responses to the CP, 33 of which were published, with permission, on the EBA website. This Final Report, and specifically the 'Rationale' section below, summarises the main comments received and the changes the EBA has made as a result. Further detail on all of the responses and the EBA's feedback to them is provided in the feedback table at the end of this report.

2.2 Rationale

8. The 'Rationale' section summarises the key concerns and questions that have been raised by respondents to the CP, and explains what, if any, changes the EBA has made to the Guidelines as a result. The concerns cover the following topics:

a) the scope and technology neutrality;

b) the inclusion of definitions of certain terms;

c) the principle of proportionality;

d) the level of detail; and

e) specific concerns/issues raised by the respondents on each of the Guidelines.

Scope of application

9. A number of comments, primarily from account information service providers (AISPs) and payment initiation service providers (PISPs), suggested that some of the requirements in the Guidelines should not be addressed to all PSPs, and that the Guidelines should specify when a requirement is applicable to all PSPs and when it is applicable only to account servicing payment services provider (ASPSPs), PISPs and/or AISPs. In addition, some respondents suggested that the scope of the requirements needs to be extended beyond the payment process so as also to cover, for example, enrolment, identity verification and regulatory risks, while others suggested that the scope needs to be limited to payment services only.

10. The EBA would like to point out that the scope of EBA Guidelines is defined not by the EBA but by the legislators, as expressed in the Directive, and that the Directive explicitly states that the Guidelines apply to all PSPs. Therefore, all PSPs have to comply with all provisions of the Guidelines in respect of the payment services they provide, regardless of the category of PSP in which they happen to fall. However, the Guidelines are subject to the principle of proportionality, which means that the detailed steps that PSPs are required to take to be compliant may differ between

[1] See http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

[2] See http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

PSPs depending on their size, and the nature, scope complexity and riskiness of the particular service(s) they provide or intend to provide.

11. A number of respondents pointed out that some of the requirements set out in these Guidelines are also included in other regulations or standards setting requirements for some categories of PSPs, in particular banks. By way of response, the EBA would like to point out that the scope of these Guidelines is limited to the 'provision of payment services' and, therefore, other processes or activities undertaken by certain PSPs (e.g. banks) are out of the scope of these Guidelines but may plausibly be subject to other regulatory requirements. In addition, for reasons of simplification, the EBA decided to remove reference to 'the provision of payment services' from the actual Guidelines and include it only in this section, with a view to clarifying that all requirements are strictly limited to the risks, functions, processes and assets related to the provision of payment services. Some references were, however, kept elsewhere, to retain the necessary level of clarity of particular requirements.

Definitions

12. Many respondents asked the EBA to include in the 'Definitions' section of the Guidelines the definitions of additional terms that are used in the Guidelines, or to provide the necessary explanatory text in the requirements where such terms are used. In particular, respondents asked the EBA to define and/or clarify terms such as 'event', 'operational or security incident', 'risk appetite' and 'early warning indicators'.

13. Having considered the merits or otherwise of the above requests, the EBA concluded that, for some terms, there is merit in including the requested definition in the Guidelines, while for some other commonly used and self-explanatory terms further clarifications or definitions are unnecessary. The EBA also arrived at the view that any ambiguous terms should be removed from the Guidelines. Regarding the definition of 'operational or security incident', for consistency reasons the EBA added the definition of this term previously adopted for the purposes of the EBA Guidelines on major incidents reporting under PSD2 (EBA/GL/2017/10).

14. In addition to the above requests, some respondents also asked the EBA to include definitions of the terms 'critical assets', 'continuous monitoring', 'internal and external factors', 'service providers' and 'detective measures to identify possible information leakages'. The EBA considered that, in line with the overarching intention to draft high-level requirements, it would not be appropriate to define those terms and that they should instead be interpreted according to their generic meaning. This will also allow PSPs to adapt those requirements to the range of payment services they offer and related threats, and provide them with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines.

Principle of proportionality

15. Several respondents suggested that, in order to be able adequately to address the great variety of business models and risks implied by payment services provided by very differently structured and regulated PSPs, the principle of proportionality should be applied in a broader sense than

proposed by the EBA and include the size and complexity of the applicant, as well as the risk profile of a given PSP or the role it plays in the payment chain.

16. Having reconsidered the importance of the proportionality principle, the EBA has concluded that it is appropriate to redraft the principle to include the size of the PSP and the nature, scope, complexity and riskiness of the particular services offered by the PSP. The EBA is of the view that all the elements currently included in the principle should be taken into account when determining the precise steps a given PSP needs to take in order to comply with the Guidelines. For the same reason, the principle has been moved from its current location to the new GL 1, on general principles.

Certification process and reference to industry standards

17. A few respondents requested that the Guidelines also specify requirements in relation to certification processes, referred to in Article 5(3) of PSD2, and also, as far as possible, to industry standards such as ISO 27001/22301.

18. Given that (i) no national authority requires such certification processes at present, (ii) the EBA is not mandated to make certification processes compulsory and (iii) the alternative of market-driven certification processes is voluntary, the EBA has concluded that there is little subject matter that could conceivably be harmonised throug EBA Guidelines. The Guidelines therefore stay silent on this particular topic for now, which may change at some point in the future, should the market or regulatory practices change such that the Guidelines need to be amended during the regular reviews that the EBA will carry out.

Level of detail of the requirements

19. Many respondents found the level of detail of the requirements set out in these Guidelines appropriate. However, several other respondents were of the opinion that the Guidelines are too general, which, in their view, increases the risk of divergent interpretation and application by the CAs, which could potentially affect the level playing field that PSPs enjoy at present. Some of those respondents suggested providing the same level of detailed requirements as in the EBA Guidelines on the security of internet payments (EBA/GL/2014/12) or providing a more detailed document for compliance assessment, such as an ‘assessment guide’.

20. Other respondents were of the opposite view, that the Guidelines are too prescriptive and too detailed, which, in their opinion, could result in PSPs putting their focus on ‘tick-box’ compliance with the requirements rather than keeping an open mind about how most efficiently to prevent the most critical risks. Those respondents also remarked that prescriptive requirements may not be compatible with a risk-based approach and they therefore suggested defining the security requirements at a higher level to afford PSPs appropriate operational flexibility in addressing the relevant risks. In response to the above comments, the EBA carefully considered the level of detail of the particular Guidelines.

21. Having assessed these responses, the EBA reviewed and redrafted several Guidelines, particularly with a view to removing overly prescriptive or ambiguous requirements, such as the reference to ‘advanced threat activities’, which was removed from GL 4.2. However, as regards the remaining

Guidelines that the EBA decided to keep unchanged, it was concluded that setting even highter level requirements throughout the Guidelines could, in the EBA's view, make them less clear in terms of the concrete steps required for complying with the requirements.

22. On a general note, however, the EBA has decided to keep the original objective of these Guidelines, which is to set out the requirements at a high level, as explained in Sections C and D of the impact assessment, to enable PSPs (i) to ensure that the established security system under those requirements would fulfil the need to mitigate and manage operational and security risks faced in the near future; (ii) to adapt those requirements to the developments in their ecosystem; and (iii) to establish measures not only to address current risks, but also to anticipate and counteract unknown exposures. Furthermore, the EBA strives to ensure technological neutrality and enable PSPs to adapt their security measures to technology changes. With the above arguments in mind, the EBA found it inappropriate to define more detailed conditions for compliance either directly in the Guidelines or in an accompanying document. This includes the 'assessment guide' suggested by some respondents, which is not a document that the EBA would publish alongside its regulatory products.

General comments

23. Prior to developing the Guidelines, the EBA performed a comprehensive risk analysis in order to understand and identify the threats and vulnerabilities to which PSPs are exposed. The risk analysis identified a wide range of threats and vulnerabilities and concluded that the type and nature of the threats are evolving rapidly, and that the Guidelines should therefore remain flexible, so as to allow PSPs to apply the Guidelines in a way that adapts to the changing risk landscape and currently unknown threats and vulnerabilities.

24. Some respondents requested the inclusion of the EBA's risk assessment as an annex to these Guidelines. The EBA, however, concluded that it would not be appropriate to publish the risk assessment upon which these Guidelines were drafted because of the risk of such analysis being exploited by potential fraudsters, which would contravene the objectives of the Guidelines.

Transitional provisions

25. Several respondents raised concerns about the implementation date of the Guidelines, pointing out that a period of six months between the date originally foreseen in PSD2 for the issuance of these Guidelines (13 July 2017) and the stated date of their applicability (13 January 2018) seems to be too short for proper implementation. One respondent suggested that the Guidelines should allow a period of at least six months from the publication date of the final Guidelines to their application date.

26. However, according to Article 5(1) of PSD2, the subset of legal entities that seek authorisation as payment or electronic money institutions are required to take these Guidelines into account when applying for authorisation as of 13 January 2018, which is why the application date of the Guidelines cannot be delayed beyond that date. That said, the EBA acknowledges that PSPs will require time to implement the Guidelines and are therefore not expected to comply with the Guidelines until the

EBA has published the translations of the Guidelines in all official EU languages, issued the compliance table, and the CAs have implemented the Guidelines into their national regulatory or supervisory frameworks.

Miscellaneous responses to specific requirements proposed in the CP

27. With regard to GL 2, on governance, the EBA amended some of the requirements in order to clarify that PSPs are required to include in their risk management framework a comprehensive security policy, a description of their risk appetite and their security objectives and measures.

28. Some respondents requested that the EBA clarify the nature and meaning of the term 'auditor' in GL 2.6. The EBA emphasised the importance of an audit being independent and conducted by auditors with the appropriate expertise. In line with the clarification of this term already provided by the EBA in the context of the RTS on strong customer authentication (SCA) and common and secure communication (CSC),[3] the EBA has amended GL 2.6 such that the audit is to be performed by an auditor with expertise in IT security and payments and operationally independent within or from the PSP.

29. Several respondents also requested that the EBA provide clarification on the provisions included in the requirement related to the outsourcing of payment services. The EBA assessed these comments but concluded that the requirement should remain unchanged. In response to some of the comments received on outsourcing, the EBA points out that the general requirements regarding the outsourcing relation between the PSP and its service providers, including the relevant liability aspects, are covered in Articles 19 and 20 of PSD2. The requirements in GL 2.7 and 2.8 were included only to take due consideration of the specificities of an outsourcing relation and its potential impact on the risk management function of PSPs and their level of detail is, in the EBA's opinion, appropriate to enable their flexible application by different PSPs.

30. Several respondents also raised concerns with regards to some of the requirements included in GL 3, on risk assessment. In particular, respondents argued that the classification included in GL 3 in terms of criticality of data is too narrow and that it should be broadened to include the sensitivity of data. Some other respondents proposed to move one particular requirement, concerning the management of access rights on information assets, from GL 3 to GL 2. In both cases, the EBA assessed the comments received, agreed with the arguments presented, and amended the requirements accordingly. Concerning the latter comment, the EBA concluded that it is more appropriate to move the specific requirement not to GL 2 but to GL 4, on protection.

31. Several respondents also requested clarification on the frequency of the periodic reviews of the risk assessment. The EBA amended the relevant requirement to clarify that such reviews should be performed on an annual basis, as laid down in Article 95(2) of PSD2.

[3] https://www.eba.europa.eu/documents/10180/1894900/EBA+Opinion+on+the+amended+text+of+the+RTS+on+SCA+and+CSC+%28EBA-Op-2017-09%29.pdf

32. Concerning GL 4, on protection, some respondents suggested dividing one of the requirements concerning the 'protection of sensitive payment data' and 'integrity checking' into two distinct requirements. The EBA agrees with this suggestion.

33. In addition, many respondents suggested that there is a need for clarification of the terms 'data minimisation' and 'sensitive data', particularly in the context of the General Data Protection Regulation (GDPR) ((EU) 2016/679). By way of response, the EBA points out that the term 'sensitive payment data' has the same meaning as in PSD2 and should be understood in that way. As for the term 'data minimisation', the EBA also clarifies that it should be understood in the context of the GDPR. However, to avoid the potential for confusion, as pointed out by respondents, instead of referring to the term 'data minimisation' the EBA decided to include the objectives of data minimisation (in line with the wording of the definition in the GDPR) in GL 4.6.

34. Several respondents requested that the EBA clarify certain terms that are used in GL 5, on detection, such as 'continuous monitoring and detection processes', 'internal and external factors', 'misuse of access' and 'services providers'. The EBA considered these requests and concluded that, since a general understanding exists in the market about these terms, they should not be defined in the Guidelines. Nevertheless, the EBA redrafted a few of the requirements with the aim of reducing potential ambiguities. With regard to 'early warning indicators', the EBA has decided not to provide a definition, as PSPs should be sufficiently flexible to define these indicators themselves as appropriate to their specific business models and risk profiles. However, the corresponding Guideline has been amended to specify the purpose of the indicators.

35. Concerning GL 6, on business continuity, several respondents requested clarification on the requirement that, to the extent possible, the payment services must continue to be provided in the event of severe business disruption. The EBA has amended the respective requirement in the GL clarifying that PSPs should strive for the continuous provision of the payment services.

36. With regard to business continuity plans (BCPs), several respondents commented that BCPs should be required regardless of size, business model and complexity of activities. The EBA agrees with this suggestion and amended the relevant requirement in the Guidelines accordingly. With regards to the frequency of testing the BCP, some respondents commented that annual testing of is too prescriptive. However, the EBA upheld its view that the requirement to test the BCP annually is necessary in order to ensure that the plans will work properly if the scenarios contained therein materialise.

37. Some respondents indicated that they disagree with the inclusion of testing in these Guidelines since they consider the specific requirements to go beyond the mandate set out in Article 95 of PSD2. In this respect, EBA upheld its original view that testing is part of the scope of the mandate given by Article 95 of PSD2, given that it states that a PSP should have appropriate mitigation measures and control mechanisms to manage operational and security risks. In the EBA's view, testing is an important tool to ensure that the mitigation measures defined by a PSP are appropriate and testing should be included in the Guidelines.

38. Some respondents were concerned that the scope of GL 8, on situational awareness and continuous learning', goes beyond the mandate of Article 95. The EBA does not agree with these respondents as it considers security training and awareness, and monitoring of emerging risks, to be reasonable and plausible security measures designed to mitigate security and operational risks.

39. Based on several comments received requesting clarifications with regard to sharing of the information on security and operational risks and reservations raised by the respondents over the issues of confidentiality and competition, the EBA has decided to remove the requirement on information sharing as the implementation from the PSPs' side could be difficult in practice, and the it would be challenging for CAs to consistently supervise this requirement. The EBA considered that such a requirement would not be proportional to the purpose of achieving broader awareness of payment fraud and security issues related to the provision of payment services. The EBA would nevertheless encourage all PSPs to participate in any platforms enabling the exchange of information on operational and security risks and threat intelligence with other PSPs and relevant third parties such as operators of payment systems, industry associations, etc., as long as these initiatives comply with applicable EU law, such as Directive (EU) 2015/2366 and Regulation (EU) 2016/679 or, if applicable, Regulation (EC) 45/2001, and that the initiatives neither favour nor disadvantage any particular type of provider over others.

40. Concerning GL 9, on PSU relationship management, several respondents commented that there is a need to make the relationship between the AISPs/PISPs and the ASPSPs transparent for PSUs. In this context, the EBA stresses the importance of ensuring transparency, such that PSUs are always aware as to which PSP is responsible for providing them with the payment service.

41. Several respondents commented that the PSP should provide the payer with the option to 'adjust' limits, not only reduce them. The EBA agreed with the rationale of this comment and hence has amended GL 9.5 accordingly. In addition, several respondents remarked that informing the PSU of the potential security breaches and attacks is excessive and should be required on a best effort basis only. The EBA considers that this mitigating measure is sound to reduce security and operational risk in payment services. Additionally, no conflict was detected with other cited regulations, which have a different scope of application. The relevant Guideline, GL 9.7, has been redrafted by providing reference to the relevant articles of PSD2 clarifying that the intention of GL 9.7 is to provide more concrete requirements for PSPs in terms of their compliance with the referred articles.

42. Some respondents commented that it makes sense to inform customers about general changes to security procedures that affect them directly, but that some changes to internal security procedures should be communicated to PSUs only on specific request. In recognition of the comment, the EBA amended the appropriate Guideline to clarify that the PSUs need to be provided only with information that is relevant to them. In addition, several respondents commented that the term 'secured channel' should be specified. The EBA agrees with the merits of clarifying the necessary features and purpose of such a communication channel, which is needed to ensure the integrity and, if required, confidentiality of the information that is being sent/received via this channel, and has consequently redrafted the relevant Guideline.

3. Guidelines

EBA/GL/2017/17

12/12/2017

Guidelines

on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains Guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010.[4] In accordance with Article 16(3) of Regulation (EU) No 1093/2010, CAs 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 Union law should be applied in a particular area. CAs as defined in Article 4(2) of Regulation (EU) No 1093/2010 to which 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. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, CAs must notify the EBA that they comply or intend to comply with these Guidelines, or otherwise give reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, CAs will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/201x/xx'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their CAs. 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).

[4] 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).

2. Subject matter, scope and definitions

Subject matter and scope

5. These Guidelines derive from the mandate given to the EBA in Article 95(3) of Directive (EU) 2015/2366[5] (PSD2).

6. These Guidelines specify requirements for the establishment, implementation and monitoring of the security measures that PSPs must take, in accordance with Article 95(1) of Directive (EU) 2015/2366, to manage the operational and security risks relating to the payment services they provide.

Addressees

7. These Guidelines are addressed to PSPs as defined in Article 4(11) of Directive (EU) 2015/2366 and as referred to in the definition of 'financial institutions' in Article 4(1) of Regulation (EU) 1093/2010 and to CAs as defined in point (i) of Article 4(2) of that Regulation by reference to the repealed Directive 2007/64/EC[6] (currently Directive (EU) 2015/2366[7]).

Definitions

8. Unless otherwise specified, terms used and defined in Directive (EU) 2015/2366 have the same meaning in these Guidelines. In addition, for the purposes of these Guidelines, the following definitions apply:

Management body	– For PSPs that are credit institutions, this term has the same meaning of the definition in point (7) of Article 3(1) of Directive 2013/36/EU[8]; – For PSPs that are payment institutions or electronic money institutions, this term means directors or persons responsible for the management of the PSP and, where relevant, persons responsible for the management of the payment services activities of the PSP; – 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.

[5] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

[6] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ L 319, 5.12.2007, p. 1).

[7] In accordance with the second subparagraph of Article 114 of Directive (EU) 2015/2366, any reference to the repealed Directive 2007/64/EC shall be construed as a reference to Directive (EU) 2015/2366 and shall be read in accordance with the correlation table in Annex II to Directive (EU) 2015/2366.

[8] Directive 2013/36/EU of the European Parliament and of the Council on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

Operational or security incident	A singular event or a series of linked events unplanned by the PSP which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.
Senior management	(a) For PSPs that are credit institutions, this term has the same meaning of the definition in point (9) of Article 3(1) of Directive 2013/36/EU; (b) For PSPs that are 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 PSP; (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.
Security risk	The risk resulting from inadequate or failed internal processes or external events that have or may have an adverse impact on the availability, integrity, confidentiality of information and communication technology (ICT) systems and/or information used for the provision of payment services. This includes risk from cyber-attacks or inadequate physical security.
Risk appetite	The aggregate level and types of risk an institution is willing to assume within its risk capacity, in line with its business model, to achieve its strategic objectives.

3. Implementation

Date of application

9. These Guidelines apply from 13 January 2018.

4. Guidelines

Guideline 1: General principle

1.1 All PSPs should comply with all the provisions set out in these Guidelines. The level of detail should be proportionate to the PSP's size and to the nature, scope, complexity and riskiness of the particular services that the PSP provides or intends to provide.

Guideline 2: Governance

Operational and security risk management framework

2.1 PSPs should establish an effective operational and security risk management framework (hereafter 'risk management framework'), which should be approved and reviewed, at least once a year, by the management body and, where relevant, by the senior management. This framework should focus on security measures to mitigate operational and security risks and should be fully integrated into the PSP's overall risk management processes.

2.2 The risk management framework should:

a) include a comprehensive security policy document as referred to in Article 5(1)(j) of Directive (EU) 2015/2366;

b) be consistent with the risk appetite of the PSP;

c) define and assign key roles and responsibilities as well as the relevant reporting lines required to enforce the security measures and to manage security and operational risks;

d) establish the necessary procedures and systems to identify, measure, monitor and manage the range of risks stemming from the payment-related activities of the PSP and to which the PSP is exposed, including business continuity arrangements.

2.3 PSPs should ensure that the risk management framework is properly documented, and updated with documented 'lessons learned' during its implementation and monitoring.

2.4 PSPs should ensure that before a major change of infrastructure, processes or procedures and after each major operational or security incident affecting the security of the payment services they provide, they review whether or not changes or improvements to the risk management framework are needed without undue delay.

Risk management and control models

2.5 PSPs should establish three effective lines of defence, or an equivalent internal risk management and control model, to identify and manage operational and security risks. PSPs should ensure that the aforementioned internal control model has sufficient authority, independence, resources and direct reporting lines to the management body and, where relevant, to the senior management.

2.6 The security measures set out in these Guidelines should be audited by auditors with expertise in IT security and payments and operationally independent within or from the PSP. The frequency and focus of such audits should take the corresponding security risks into consideration.

Outsourcing

2.7 PSPs should ensure the effectiveness of the security measures set out in these Guidelines when operational functions of payment services, including IT systems, are outsourced.

2.8 PSPs should ensure that appropriate and proportionate security objectives, measures and performance targets are built into contracts and service-level agreements with the providers to whom they have outsourced such functions. PSPs should monitor and seek assurance on the level of compliance of these providers with the security objectives, measures and performance targets.

Guideline 3: Risk assessment

Identification of functions, processes and assets

3.1 PSPs should identify, establish and regularly update an inventory of their business functions, key roles and supporting processes in order to map the importance of each function, role and supporting processes, and their interdependencies related to operational and security risks.

3.2 PSPs should identify, establish and regularly update an inventory of the information assets, such as ICT systems, their configurations, other infrastructures and also the interconnections with other internal and external systems in order to be able to manage the assets that support their critical business functions and processes.

Classification of functions, processes and assets

3.3 PSPs should classify the identified business functions, supporting processes and information assets in terms of criticality.

Risk assessments of functions, processes and assets

3.4 PSPs should ensure that they continuously monitor threats and vulnerabilities and regularly review the risk scenarios impacting their business functions, critical processes and information assets. As part of the obligation to conduct and provide CAs with an updated and comprehensive risk assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigating measures and control mechanisms implemented in response to those risks, as laid down in Article 95(2) of Directive (EU) 2015/2366, PSPs should carry out and document risk assessments, at least annually or at shorter intervals as determined by the CA, of the functions, processes and information assets they have identified and classified in order to identify and assess key operational and security risks. Such risk assessments should also be done before any major change of infrastructure, process or procedures affecting the security of payment services occurs.

3.5 On the basis of the risk assessments, PSPs should determine whether and to what extent changes are necessary to the existing security measures, the technologies used and the procedures or payment services offered. PSPs should take into account the time required to implement the changes and the time to take appropriate interim security measures to minimise operational or security incidents, fraud and potential disruptive effects in the provision of payment services.

Guideline 4: Protection

4.1 PSPs should establish and implement preventive security measures against identified operational and security risks. These measures should ensure an adequate level of security in accordance with the risks identified.

4.2 PSPs should establish and implement a 'defence-in-depth' approach by instituting multi-layered controls covering people, processes and technology, with each layer serving as a safety net for preceding layers. Defence-in-depth should be understood as having defined more than one control covering the same risk, such as the four-eyes principle, two-factor authentication, network segmentation and multiple firewalls.

4.3 PSPs should ensure the confidentiality, integrity and availability of their critical logical and physical assets, resources and sensitive payment data of their PSUs whether at rest, in transit or in use. If the data include personal data, such measures should be implemented in compliance with Regulation (EU) 2016/679[9] or, if applicable, Regulation (EC) 45/2001.[10]

4.4 On an on-going basis, PSPs should determine whether changes in the existing operational environment influence the existing security measures or require the adoption of further measures to mitigate the risk involved. These changes should be part of the PSP's formal change management process, which should ensure that changes are properly planned, tested, documented and authorised. On the basis of the security threats observed and the changes made, testing should be performed to incorporate scenarios of relevant and known potential attacks.

4.5 In designing, developing and providing payment services, PSPs should ensure that segregation of duties and 'least privilege' principles are applied. PSPs should pay special attention to the segregation of IT environments, in particular to the development, testing and production environments.

Data and systems integrity and confidentiality

4.6 In designing, developing and providing payment services, PSPs should ensure that the collection, routing, processing, storing and/or archiving and visualisation of sensitive payment data of the PSU is adequate, relevant and limited to what is necessary for the provision of its payment services.

4.7 PSPs should regularly check that the software used for the provision of payment services, including the users' payment-related software, is up to date and that critical security patches are deployed. PSPs should ensure that integrity-checking mechanisms are in place in order to verify the integrity of software, firmware and information on their payment services.

[9] Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[10] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

Physical security

4.8 PSPs should have appropriate physical security measures in place, in particular to protect the sensitive payment data of the PSUs as well as the ICT systems used to provide payment services.

Access control

4.9 Physical and logical access to ICT systems should be permitted only for authorised individuals. Authorisation should be assigned in accordance with the staff's tasks and responsibilities, limited to individuals who are appropriately trained and monitored. PSPs should institute controls that reliably restrict such access to ICT systems to those with a legitimate business requirement. Electronic access by applications to data and systems should be limited to the minimum that is required to provide the relevant service.

4.10 PSPs should institute strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements. Controls such as roles-based access, logging and reviewing of the systems activities of privileged users, strong authentication and monitoring for anomalies should be implemented. PSPs should manage access rights to information assets and their supporting systems on a 'need-to-know' basis. Access rights should be periodically reviewed.

4.11 Access logs should be retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with GL 3.1 and GL 3.2, without prejudice to the retention requirements set out in EU and national law. PSPs should use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of payment services.

4.12 In order to ensure secure communication and reduce risk, remote administrative access to critical ICT components should be granted only on a need-to-know basis and when strong authentication solutions are used.

4.13 The operation of products, tools and procedures related to access control processes should protect the access control processes from being compromised or circumvented. This includes enrolment, delivery, revocation and withdrawal of corresponding products, tools and procedures.

Guideline 5: Detection

Continuous monitoring and detection

5.1 PSPs should establish and implement processes and capabilities to continuously monitor business functions, supporting processes and information assets in order to detect anomalous activities in the provision of payment services. As part of this continuous monitoring, PSPs should have in place appropriate and effective capabilities for detecting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets used in the provision of payment services.

5.2 The continuous monitoring and detection processes should cover:

a) relevant internal and external factors, including business and ICT administrative functions;

b) transactions in order to detect misuse of access by service providers or other entities; and

c) potential internal and external threats.

5.3 PSPs should implement detective measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities for software and hardware, and check for corresponding new security updates.

Monitoring and reporting of operational or security incidents

5.4 PSPs should determine appropriate criteria and thresholds for classifying an event as an operational or security incident, as set out in the 'Definitions' section of these Guidelines, as well as early warning indicators that should serve as an alert for the PSP to enable early detection of operational or security incidents.

5.5 PSPs should establish appropriate processes and organisational structures to ensure the consistent and integrated monitoring, handling and follow-up of operational or security incidents.

5.6 PSPs should establish a procedure for reporting such operational or security incidents as well as security-related customer complaints to its senior management.

Guideline 6: Business continuity

6.1 PSPs should establish sound business continuity management to maximise their ability to provide payment services on an on-going basis and to limit losses in the event of severe business disruption.

6.2 In order to establish sound business continuity management, PSPs should carefully analyse their exposure to severe business disruptions and assess, quantitatively and qualitatively, their potential impact, using internal and/or external data and scenario analysis. On the basis of the identified and classified critical functions, processes, systems, transactions and interdependencies in accordance with GL 3.1 to GL 3.3, PSPs should prioritise business continuity actions using a risk-based approach, which can be based on the risk assessments carried out under GL 3. Depending on the business model of the PSP, this may, for example, facilitate the further processing of critical transactions while remediation efforts continue.

6.3 On the basis of the analysis carried out under GL 6.2, a PSP should put in place:

a) BCPs to ensure that it can react appropriately to emergencies and is able to maintain its critical business activities; and

b) mitigation measures to be adopted in the event of termination of its payment services and termination of existing contracts, to avoid adverse effects on payment systems and on PSUs and to ensure execution of pending payment transactions.

Scenario-based business continuity planning

6.4 The PSP should consider a range of different scenarios, including extreme but plausible ones, to which it might be exposed, and assess the potential impact such scenarios might have.

6.5 Based on the analysis carried out under GL 6.2 and plausible scenarios identified under GL 6.4, the PSP should develop response and recovery plans, which should:

a) focus on the impact on the operation of critical functions, processes, systems, transactions and interdependencies;

b) be documented and made available to the business and support units and readily accessible in case of emergency; and

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

Testing of business continuity plans

6.6 PSPs should test their BCPs, and ensure that the operation of their critical functions, processes, systems, transactions and interdependencies are tested at least annually. The plans should support objectives to protect and, if necessary, re-establish the integrity and availability of their operations, and the confidentiality of their information assets.

6.7 Plans should be updated at least annually, based on testing results, current threat intelligence, information-sharing and lessons learned from previous events, and changing recovery objectives, as well as analysis of operationally and technically plausible scenarios that have not yet occurred, and, if relevant, after changes in systems and processes. PSPs should consult and coordinate with relevant internal and external stakeholders during the establishment of their BCPs.

6.8 PSPs' testing of their BCPs should:

a) include an adequate set of scenarios, as referred to in GL 6.4;

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 processes to respond adequately to the scenarios above.

6.9 PSPs should periodically monitor the effectiveness of their BCPs, and document and analyse any challenges or failures resulting from the tests.

Crisis communication

6.10 In the event of a disruption or emergency, and during the implementation of the BCPs, PSPs should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including external service providers, are informed in a timely and appropriate manner.

Guideline 7: Testing of security measures

7.1 PSPs should establish and implement a testing framework that validates the robustness and effectiveness of the security measures and ensure that the testing framework is adapted to consider new threats and vulnerabilities, identified through risk-monitoring activities.

7.2 PSPs should ensure that tests are conducted in the event of changes to infrastructure, processes or procedures and if changes are made as a consequence of major operational or security incidents.

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

7.4 The testing framework should ensure that tests:

a) are performed as part of the PSP's formal change management process to ensure their robustness and effectiveness;

b) are carried out by independent testers who have sufficient knowledge, skills and expertise in testing security measures of payment services and are not involved in the development of the security measures for the corresponding payment services or systems that are to be tested, at least for final tests before putting security measures into operation; and

c) include vulnerability scans and penetration tests adequate to the level of risk identified with the payment services.

7.5 PSPs should perform on-going and repeated tests of the security measures for their payment services. For systems that are critical for the provision of their payment services (as described in GL 3.2), 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.

7.6 PSPs should monitor and evaluate the results of the tests conducted, and update their security measures accordingly and without undue delay in the case of critical systems.

Guideline 8: Situational awareness and continuous learning

Threat landscape and situational awareness

8.1 PSPs should establish and implement processes and organisational structures to identify and constantly monitor security and operational threats that could materially affect their ability to provide payment services.

8.2 PSPs should analyse operational or security incidents that have been identified or have occurred within and/or outside the organisation. PSPs should consider key lessons learned from these analyses and update the security measures accordingly.

8.3 PSPs should actively monitor technological developments to ensure that they are aware of security risks.

Training and security awareness programmes

8.4 PSPs should establish a training programme for all staff to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures in order to reduce human error, theft, fraud, misuse or loss. PSPs should ensure that the training programme provides for training staff members at least annually, and more frequently if required.

8.5 PSPs should ensure that staff members occupying key roles identified under GL 3.1 receive targeted information security training on an annual basis, or more frequently if required.

8.6 PSPs should establish and implement periodic security awareness programmes in order to educate their personnel and to address information security related risks. These programmes should require PSP personnel to report any unusual activity and incidents.

Guideline 9: Payment service user relationship management

Payment service user awareness on security risks and risk-mitigating actions

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

9.2 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.

9.3 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.

9.4 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.

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

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

9.7 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 Cost-benefit analysis/impact assessment

Article 95(3) of Directive (EU) 2015/2366, of 25 November 2015, on payment services in the internal market (PSD2) requires the EBA, in coordination with the ECB, to issue Guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 with regard to the establishment, implementation and monitoring of security measures for operational and security risks of payment services by PSPs as demanded under Article 95 of PSD2.

Article 16(2) of the EBA Regulation provides that the EBA should carry out an analysis of 'the potential related costs and benefits' of any Guidelines it develops. This analysis should provide an overview of the findings regarding the problem to be dealt with, the solutions proposed and the potential impact of these options.

This section contains the impact assessment on PSPs, PSUs and other stakeholders arising from adopting the requirements for establishing, implementing and monitoring security measures to prevent operational and security risks of payments.

A. Problem identification and baseline scenario

Efficient payment systems reduce the cost of exchanging goods and services, and are indispensable to the functioning of the interbank, money and capital markets. Weak payment systems can result in an inefficient use of financial resources, inequitable risk-sharing among market participants, actual losses and a reduction in confidence in the payment system and in the very use of money.

The retail payment system shows a continuous trend in innovations with new providers and payment solutions. These continual changes give rise to concerns about the current trend of rising frauds, especially in, but not limited to, the field of internet payments.[11]

The risk analysis exercise conducted by the EBA and the ECB has identified various threats and vulnerabilities to which PSPs are currently exposed when providing their payment services. The most common risks are:

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

In addition to the current risks PSPs are facing, the rapid developments in their ecosystem give rise to new threats which cannot be anticipated and/or counteracted with the current security systems in place.

[11] EBA (2016): EBA Consumer Trends – Report 2016 (http://www.eba.europa.eu/documents/10180/1360107/Consumer+Trends+Report+2016.pdf).

Users of payment services are increasingly concerned about security at all stages of the payment process. The level of consumer awareness about potential (cyber) risks and about consumer protection measures available in the payment sector is low.[12] Lower user confidence affects the payment systems because the perception of failing payment security affects the way in which consumers make payment choices. If consumer confidence in specific payment instruments is undermined, users may switch to alternative but less efficient forms of payments, compromising the smooth operation of payment systems, decreasing efficiency throughout the economy and undermining firms' efforts to realise cost efficiencies. Unsophisticated users with low financial literacy further facilitate the work of fraudsters and can be an additional risk to PSPs.

Further, the different level and detail of security requirements between EU Member States leads to an uneven level playing field whereby providers in some countries are subject to more stringent requirements than those in other countries.

To address these issues, these Guidelines describe requirements for PSPs to establish, implement and monitor security measures which mitigate the outlined risks and will help to ensure common application of the requirements on security measures among Member States.

B. Policy objectives

This paper introduces nine Guidelines with regard to the establishment, implementation and monitoring of security measures which PSPs need to have in place under Article 95 of PSD2, as well as to promote cooperation among relevant stakeholders in the area of operational and security risks associated with payment services.

In general, these Guidelines aim to foster the establishment of a harmonised EU-wide minimum level of security in payment services. The establishment of harmonised European recommendations for the security of payment services is expected to contribute to fighting payment fraud, making payments safer and more secure and thus enhancing consumer trust in retail payments in the EU.

These Guidelines further contribute to the EBA objectives of enhancing regulatory and supervisory convergence and protecting users of payment services in the EU[13] by ensuring that PSPs' security measures are established, implemented and monitored consistently, efficiently and effectively across the EU.

More specifically, these Guidelines aim to help PSPs to ensure the integrity, availability, confidentiality, authenticity and continuity of payment-related services and to avoid incidents during the payment process. They further aim to help PSPs to avoid losses resulting from inadequate or failed internal processes, people and systems or from external events.

Operationally, these Guidelines are drafted considering existing international guidance and frameworks to define minimum requirements for PSPs that allow their risk-controlling management/operational systems to address the most commonly identified threats and vulnerabilities. However, in view of the

[12] European Commission (2015): Special Eurobarometer 423 – Cyber Security Report, February 2015 (http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf).
[13] EBA Work Programme (2017) (https://www.eba.europa.eu/about-us/work-programme/current-work-programme).

speed of technological advances and the introduction of new ways of affecting payments, along with the fact that fraudsters have become more organised and their attacks more sophisticated, these Guidelines consider the necessary adaptability of the security systems to address future/unknown types of incident.

C. Options considered and preferred option

To improve the overall resilience of PSPs against operational and risks, PSPs' security systems shall cover eight elements (GL 2 to GL 9) in line with the two general principles (GL 1). The Guidelines outlined in this CP prescribe the requirements to establish appropriate roles and responsibilities, structures, systems, policies and procedures for a sound security framework. They further ensure that PSPs implement effective processes for monitoring transactions and anticipating changes in the threat landscape in order to ensure that security measures are implemented effectively. Risks from and to PSPs shall be reduced, considering especially the risks from PSUs.

The EBA drafted these Guidelines considering the risks they address. Based on the risk analysis, the applicability of the Guidelines has been considered. In that light, the following options have been considered:

Option 1.1: Strongly prescriptive requirements; and

Option 1.2: High-level requirements on the establishment, implementation and monitoring of the security measures for PSPs.

Option 1.1 would define requirements which can become obsolete very quickly in an ecosystem in which new threats are evolving continuously. PSPs would be unable to ensure that the established security system under those requirements would fulfil the need to mitigate and manage operational and security risks faced in the near future. The retained option (Option 1.2) reflects high-level requirements, which allow PSPs to adapt those requirements to the developments in their ecosystem. These Guidelines reflect PSPs' need to establish systems for current risks but also to anticipate and counteract unknown exposures.

D. Cost-benefit analysis

These Guidelines will affect PSPs, PSUs and other stakeholders. The preferred options describe the requirements on security measure for operational and security risks of payment services in a high-level way.

They will affect the way in which PSPs establish, implement and monitor their security systems as required under PSD2. Under the more stringent security regulation of PSD2, PSPs will be required to establish systems which enforce a stronger identification of their current functions, processes and assets and a continuous assessment of that information. The requirements on PSPs under Article 95 of PSD2 further focus on the adaptability of PSPs' security systems. Accordingly, PSPs will need to establish systems that allow them to monitor and to analyse all of their processes and all incidents that occur and to anticipate possible threats and the environment in which they operate. PSPs are further required to put in place sound responses and recovery arrangements and to implement systems which allow the efficient exchange of information with other PSPs which are or could be exposed to the same risks.

It is expected that PSPs will incur one-off costs as a result of setting up technical, personnel and administrative process when implementing the necessary security and reporting systems. As regards the continuous monitoring exercise, it is expected that PSPs will need further staff who will operate the new security systems and ensures continuous adaptation of the technology.

Prior to the adoption of PSD2, security measures for operational and security risks of payments have been legally based on Directive 2007/64/EC (PSD1). The EBA Guidelines on the security of internet payments, [14] which came into force on 1 August 2015, and the ECB Recommendations for the security of internet payments,[15] set current requirements for PSPs offering internet payment services. PSPs which offer internet payments can partly rely on security systems established under these requirements. However, as PSD2 tightens requirements on PSPs, it is expected that PSPs providing internet payment will need to adapt their systems accordingly.

The requirement outlined in these Guidelines on the security measures for mitigating the operational and security risks of PSPs will benefit PSPs' operations by aiming to ensure that services are not interrupted and meet the guaranteed standards. This avoids costs stemming from loss of services, need for restoring services and loss of reputation.

PSUs will benefit from the requirements as they decrease the probability of incidents during the payment processes, especially fraud and the related losses. The increase in trust in the payment services will, in turn, positively affect the payment system and the overall financial system. However, there is the possibility that increased costs will be passed on to the users.

The adaptation of these Guidelines aims to prevent the occurrence of incidents and will in the long run hamper fraudsters' activities. This will lead to the strengthening of the payment system.

4.2 Feedback on the public consultation

The EBA publicly consulted a draft of these Guidelines by publishing a CP on 5 May 2017. The consultation period lasted for three months and ended on 7 August 2017. Forty-three responses were received, 33 of which were published on the EBA website.

This section presents a summary of the key points and other comments that arose from the consultation, the analysis and discussion triggered by these comments, and the actions taken to address them if deemed necessary.

In some cases, several industry respondents made similar comments or the same respondent repeated its comments in response to more than one question. In such cases, the comments and the EBA's analysis of the comments are included in the table below. Changes to the Guidelines have been incorporated as a result of the responses received during the public consultation, as described in detail below.

[14] EBA (2014): Final guidelines on the security of internet payments, 19 December 2014 (https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29.pdf/f27bf266-580a-4ad0-aaec-59ce52286af0).
[15] ECB (2013): Recommendations for the security of internet payments, 31 December 2013 (http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html).

Summary of key issues and the EBA's feedback

As already stated in Section 2.2, Rationale, above, the EBA has decided to make changes to the Guidelines to reflect some of the concerns raised by respondents. In the feedback table that follows, the EBA has summarised the comments received and explains which responses have and have not led to changes, and the reasons for the decision.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
Feedback on responses to Question 1				
[1]	General responses	One respondent suggested that the Guidelines should be accompanied by an operational document containing greater detail which can be adapted by PSPs, similar to the assessment guide on the recommendations on the security of internet payments issued by the ECB in February 2014.	The legal instruments of the EBA do not foresee any additional guidance on their application, or assessing compliance with them, such as assessment guides. Instead, any requirements that apply to PSPs are set out in the Guidelines themselves. The EBA decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. It also leaves a degree of flexibility for PSPs to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable PSPs to adapt their security measures to technology changes.	None.
[2]	General responses	One respondent suggested making it clear that, in the event of outsourcing to entities other than PSPs, such as network providers, or of using devices/software not supplied by PSPs, there are objective limits to the Guidelines for PSPs because matters would fall outside their control and remit. The respondent refers in particular to Guidelines such as GL 3.5, GL 3.8, GL 3.10 and GL 6.3.	The EBA agrees that it would be difficult to adequately test the security of payment devices and software used for the provision of payment services, the authentication of the PSU or the generation/receipt of authentication codes as most of these devices will be manufactured by other companies and these are 'black boxes' for the PSP. Although such devices might pass independent security certification processes at the vendor, such products should nevertheless be considered as 'standard products' which are purchased. It is important that the PSP has sufficient assurance of the security of the devices and terminals delivered by the manufacturer. It is the responsibility and task of the PSP to test all security measures before implementation and during operations. This includes the determination of the effectiveness of security measures in purchased products which are independently certified, such as devices, terminals, etc. How this should be done is up to the PSP, but the PSP should evidence the implementation of such security measures relevant to the externally sourced devices and software if requested. As stipulated in Article 19, Paragraph 6, of PSD2, 'Outsourcing of important operational functions, including IT systems, shall not be undertaken in such way as to impair materially the quality of the payment institution's internal control and the ability of the CAs to monitor and retrace the payment institution's compliance with all of the obligations laid down in this Directive'. As also stipulated in GL 2 of the EBA Guidelines on outsourcing: 'The ultimate responsibility for the proper management of the risks associated with outsourcing or the outsourced activities lies with an outsourcing institution's senior management' and 'The outsourcing of functions does not relieve an outsourcing institution of its	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			regulatory responsibilities for its authorized activities or the function concerned.'	
[3]	General responses	Several respondents were of the view that the Guidelines are too general and that this therefore increases the risk of divergent interpretation and application by the CAs and can potentially impact the level playing field that applies to PSPs.	As is stated in Sections C and D of Section 4.1, Cost-benefit analysis/impact assessment, the objective of these Guidelines is to set out the requirements at a high level. In particular, Section C explains why the EBA chose the preferred approach. Option 1.1 would define requirements which can become obsolete very quickly in an ecosystem in which new threats are evolving continuously. PSPs would be unable to ensure that the established security system under those requirements would fulfil the need to mitigate and manage operational and security risks faced in the near future. The retained option (Option 1.2) reflects high-level requirements, which allow PSPs to adapt those requirements to the developments in their ecosystem. These Guidelines reflect PSPs' need to establish systems for current risks but also to anticipate and counteract unknown exposures. Another important guiding principle considered by the EBA when drafting these Guidelines was technological neutrality, and in this respect the high-level character of the Guidelines should enable PSPs to adapt their security measures to technology changes.	None.
[4]	General responses	Several respondents requested that more specific requirements be added in the area of security measures. One respondent provided the following example: in the event that the end customer does not have the required software (i.e. as found on a smartphone) to install the necessary applications, then a hardware token, for example, is a must.	The EBA considers the requirement for a hardware token to be overly prescriptive. The EBA decided to draft high-level requirements which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. It also leaves a level of flexibility for PSPs to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable PSPs to adapt their security measures to technology changes. The EBA therefore finds it inappropriate to include very prescriptive requirements such as the one suggested.	None.
[5]	General responses	One respondent suggested adding more detailed requirements, such as in the EBA Guidelines on the security of internet payments.	When drafting these Guidelines, the EBA considered to the extent possible, within the limitations of the mandate, the inclusion of the relevant requirements of the EBA Guidelines on the security of internet payments. In the said review, the EBA considered that some of the requirements were included in PSD2 or in other EBA regulatory products. Another important guiding principle when drafting these Guidelines was technological neutrality, so in some cases the EBA did not find it appropriate to include very prescriptive requirements applicable only to	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			internet payments, which would not be of relevance to other payment services covered by these Guidelines.	
[6]	General responses	Several respondents held the opposite view to the respondents providing responses 3-5, considering that the Guidelines are too prescriptive and detailed, which could lead PSPs to focus mainly on being compliant with the standards rather than efficiently preventing the most critical risks, which in turn could create unnecessary costs. They were also of the view that prescriptive requirements may diverge from the risk-based approach and suggested defining the security requirements at a higher level in order to afford PSPs the appropriate operational flexibility in addressing the relevant risks. One respondent suggested that the level of detail in the Guidelines should be kept high and referred in particular to GL 2.3.	As is stated in Sections C and D of the impact assessment, the objective of these Guidelines is to set out the requirements at a high level. Section C clearly explains why the EBA chose the preferred approach: Option 1.1 would define requirements which can become obsolete very quickly in an ecosystem in which new threats are evolving continuously. PSPs would be unable to ensure that the established security system under those requirements would fulfil the need to mitigate and manage operational and security risks faced in the near future. The retained option (Option 1.2) reflects high-level requirements, which allow PSPs to adapt those requirements to the developments in their ecosystem. These Guidelines reflect PSPs' need to establish systems for current risks but also to anticipate and counteract unknown exposures. Another important guiding principle considered by the EBA when drafting these Guidelines was technological neutrality, and in this respect the high-level character of the Guidelines should enable PSPs to adapt their security measures to technology changes. Setting even higher level requirements throughout the Guidelines could, in the EBA's view, make the requirements less clear in terms of the concrete steps that need to be taken to comply with the requirements. Nevertheless, in recognition of this and other, more detailed, comments related to particular Guidelines, the EBA reviewed and generalised several Guidelines, particularly with a view to removing overly prescriptive or ambiguous requirements. For example, an ambiguous reference to 'advanced threat activities' was removed from GL 4.2.	The second sentence up to the end of the paragraph of GL 2.3 (now GL 3.3) has been deleted and the deleted section, with amended wording, moved to GL 3.11 (now GL 4.10), where it was deemed to be more appropriate. Therefore, GL 2.3 (now GL 3.3) now reads: 'PSPs should classify the identified business functions, supporting processes and information assets in terms of criticality. ~~PSPs should manage access rights to information assets and their supporting systems on a 'need-to-know' basis. Access rights should be periodically reviewed. PSPs should maintain access logs and use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of payment services.'~~ Additionally, GL 4.2 (now GL 5.2) has been amended and now reads:

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				'The continuous monitoring and detection processes should cover: a) relevant internal and external factors, including business ~~line~~ and ~~IT~~ ICT administrative functions; b) ~~and~~ transactions, in order to detect misuse of access by service providers or other entities~~;~~ and c) potential ~~insider~~ internal and external threats ~~and other advanced threat activities~~'
[7]	General responses	Several respondents suggested that the Guidelines should refer to generic standards as much as possible, such as ISO 27001/22301. One respondent proposed that the ISO/IEC 27000 information security management system (ISMS) family should be the mandatory method to be used in these Guidelines for the framework to be comparable between PSPs. The respondent undertook a matching of the requirements within the Guidelines against the ISO/IEC 27000 ISMS family and claims that there is a high level of consistency.	The EBA acknowledges that (i) no national authority requires such certification processes at present, (ii) the EBA is not mandated to make certification processes compulsory and (iii) that the alternative of market-driven certification processes is voluntary. As a result, the EBA has concluded that there is little subject matter that could conceivably be harmonised throughout EBA Guidelines. The Guidelines therefore stay silent on this particular topic for now, which may change at some point in the future, should market or regulatory practices have changed such that the Guidelines need to be amended during the regular reviews that the EBA will carry out.	None.
[8]	General responses	Several respondents requested the addition of a glossary, and, in particular, definitions of the following: a. 'critical assets' in GL 2.2, GL 3.3 and GL 6.5; b. 'continuous monitoring' ; c. 'internal and external factors'; d. 'service providers'; e. 'detective measures to identify possible information leakages';	With regard to the term 'critical assets', the EBA would like to point out that each PSP is required, as stipulated in GL 2.3 (now GL 3.3), to define the criticality of its business functions, supporting processes and information assets on its own judgement, taking into consideration the importance of these aspects to the general business model, risk profile, etc. With regard to other terms requested to be defined, the EBA would like to emphasise that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. It also leaves PSPs with a level of flexibility to adapt their legal and institutional solutions to comply with	With regard to comment f, GL 4.2 (now GL 5.2) was redrafted and now reads: 'potential ~~insider~~ internal and external threats ~~and other advanced threat activities~~.'

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		f. 'advanced threat activities'; g. 'major change' (GL 1.4).	the requirements set out in these Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable PSPs to adapt their security measures to technology changes. The EBA therefore finds it inappropriate to define the following terms, which should also be interpreted in accordance with their generic meaning, restated below: b. 'continuous monitoring', meaning monitoring that is performed at all times; c. 'internal and external factors', meaning factors which relate, respectively, to the PSP itself, its functions, processes and assets, and factors that are not inherent to the PSP, but can influence it from the outside; d. 'service providers', meaning any entities that may provide services of any kind to the PSP; e. 'detective measures to identify possible information leakages', for which the purpose is indicated in the term itself. Regarding the request for a definition of 'advanced threat activities', the EBA agreed with the comments that this is an ambiguous term and therefore removed it from the Guidelines. Lastly, regarding the request for a definition of a 'major change', the EBA is of the view that all PSPs should assess whether any changes in infrastructure, processes or procedures may have a material or immaterial impact on the security, integrity or continuity of their payment-related systems and/or the security of sensitive payment data or funds. Every major change should be taken into account when reviewing the risk management framework.	
Feedback on responses to Question 2				
[9]	GL 1	One respondent was of the view that GL 1 should make explicit reference to the measures of business continuity, as provided for by GL 5. Moreover one respondent considered that GL 1 is formulated in too general a manner.	The EBA agrees with the view that GL 1 (now GL 2) should refer to the measures of business continuity, as provided by GL 5 and, therefore, the relevant Guideline has been amended accordingly to reflect this. However, the EBA disagrees with the opinion that GL 1 is formulated in too general a manner. The EBA points out that technological and business neutrality was an important guiding principle and, therefore, the high-level character of the Guidelines should enable PSPs to adapt their security measures, and hence their governance arrangements, especially taking into consideration the regular changes in this area.	GL 1.2 (c) became GL 2.2 (d). It has also been amended and now reads: 'establish the necessary procedures and systems to identify, measure, monitor and manage the range of risks stemming from the payment-

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				related ~~provision of payment services~~ activities of the PSP and to which the PSP is exposed, including business continuity arrangements.'
[10]	GL 1.1	A few respondents proposed to extend the term 'senior management' by adding 'and/or the shareholders'.	The EBA is of the view that there is no need to extend the term 'senior management' by adding 'and/or the shareholders', mainly because the rights and obligations of shareholders do not refer to what the 'senior management' is responsible for within the organisation. Therefore, the EBA deems that the definition of 'senior management' included in the Guidelines is sufficient.	None.
[11]	GL 1.1	One respondent indicated that it is unclear whether or not an overarching operational risk framework, supported by a number of other underlying sub-risk frameworks, meets the Guideline requirement, or if the guidelines require a standalone operational and security risk framework for payment services. One respondent also mentioned that the risk framework is a policy document, which usually focuses on principles and policies rather than detailed 'measures'; hence, the proper approach would be to ensure a minimum level of harmonisation of the requirements across the EU. One respondent added that it would be helpful for the Guideline to cover other operational risk aspects as well as security measures.	The EBA is of the view that it is possible to have in place an overarching operational risk framework that refers to payment services as well as to other services, for example credit, deposit and capital-raising services. Competent authorities should ensure the appropriate application of the Guidelines by PSPs, but it is impossible to indicate a minimum level of harmonisation of the requirements across the EU. All addressees shall make every effort to comply with the Guidelines. In addition, CAs may require PSPs to report their compliance with the Guidelines. The EBA points out that the Guidelines will be applicable to all PSPs within the EU and its scope is sufficient. Regarding the final point, for GL 1.1 to be in compliance with PSD2 provisions, the risk management framework should focus on security measures to mitigate operational and security risks of payment services – what is mandated by PSD2. In recognition of the comment, the EBA has reviewed the Guidelines and added reference to operational risk in addition to security risk wherever applicable.	Several Guidelines have been amended to reflect also the 'operational risk'; for instance, GL 2.5 (now GL 3.5) now reads: 'On the basis of the ~~identification,classification and~~ risk assessments, PSPs should determine whether and to what extent changes are necessary to the existing security measures, the technologies used and the procedures or payment services offered. PSPs should take into account the time required to implement the changes and the time to take appropriate interim measures to minimise operational or security incidents, fraud and potential disruptive effects in the provision of payment services.' ~~and to~~

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				~~their payment service users.~~
[12]	GL 1.1	Moreover, one respondent pointed out that in GL 1.1 and GL 1.2 the EBA should clarify the terms 'risk management framework' and 'security policy' and how they relate to each other.	The EBA points out that GL 1.2 (now GL 2.2) refers to 'risk management framework' and, as also stated in the Background and Rationale sections of the Guidelines, this is a framework that PSPs shall establish with appropriate mitigation measures and control mechanisms to manage operational and security risks relating to the payment services they provide. On the other hand, with regard to the 'security policy', as also stipulated in Article 5, Paragraph 1 (j), of PSD2, such policy includes a detailed risk assessment in relation to the payment services, a description of security control, etc. As for the relation between the two, it is reflected by the indication in GL 2.2 (a) that the security policy should be included in the risk management framework.	None.
[13]	GL 1.2	One respondent proposed adding: 'The risk management framework should be in line with the information security strategy and should set the risk appetite of the PSP.	The EBA points out that, as a rule, the security policy should be in line with the information security strategy. The EBA further clarifies that GL 1.2 (now GL 2.2) refers to 'risk management framework' and 'security policy' as well as to the 'risk appetite', which should be set within the risk management framework.	GL 1.2 (now GL 2.2) has been amended and now reads: 'The risk management framework should: a) include a comprehensive security policy document as referred to in Article 5(1)(j) of Directive (EU) 2015/2366; ~~which sets the risk appetite of the PSP, its security objectives and measures;~~ b) be consistent with the risk appetite of the PSP;

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				~~b~~c) define and assign key roles and responsibilities as well as the relevant reporting lines required to enforce the security measures and to manage security and operational risks ~~related to the provision of payment services~~; d) establish the necessary procedures and systems to identify, measure, monitor and manage the range of risks stemming from the ~~provision of payment services~~ payment-related activities of the PSP and to which the PSP is exposed, including business continuity arrangements.'
[14]	GL 1.2	One respondent indicated that the risk management framework could be read as having ownership of the IT risk, which would not be appropriate, as the business owner always carries the risk. Ownership of IT security risk should remain with IT, just as compliance and legal risks remain, respectively, with compliance and legal.	The EBA points out that the Guidelines, according to PSD2, refer to operational and security risks derived from the provision of payment services. It should be noted that these risks may have some relations to IT risk. As GL 1.2 (b) (now GL 2.2 (c)) indicates, the risk management framework should define and assign the key roles and responsibilities as well as the relevant reporting lines required to enforce the security measures and to manage security and operational risks. Therefore, a PSP may assign IT risk to a particular part of its organisation as long as it assures to fulfil the provisions included in Guidelines.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[15]	Gl 1.2	Some of the respondents suggested assessing the risk appetite of a PSP by comparing the security policy with market best practices, which would involve the PSP's risk management function, senior management and occasionally the management body. They further elaborated that the risk appetite should be set in an overarching risk policy and expanded accordingly in a security policy. In their opinion it would be helpful for the security policy to be separate from the risk framework.	The EBA points out that the risk appetite should be specified in the risk management framework, as should the security policy. Therefore, the EBA agrees with the view of the respondents and has amended the Guideline accordingly.	GL 1.2 (now GL 2.2) has been amended and now reads: 'The risk management framework should: a) include a comprehensive security policy document as referred to in Article 5(1)(j) of Directive (EU) 2015/2366; ~~which sets the risk appetite of the PSP, its security objectives and measures;~~ b) be consistent with the risk appetite of the PSP; ~~b~~c) define and assign key roles and responsibilities as well as the relevant reporting lines required to enforce the security measures and to manage security and operational risks ~~related to the provision of payment services~~; d) establish the necessary procedures and systems to identify, measure, monitor and manage the

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				range of risks stemming from the ~~provision of payment services~~ payment-related activities of the PSP and to which the PSP is exposed, including business continuity arrangements.'
[16]	GL 1.2	One respondent requested clarification of the term 'risks stemming from the provision of payment services and to which the PSP is exposed' in relation to the business risk (financial risk) and the security risk (operational/non-financial risk).	The EBA would like to clarify that 'risks stemming from the provision of payment services and to which the PSP is exposed' are different depending on the nature of PSP's activity. These risks should be identified by the PSP and may refer to business risk/financial risk as well as to security risk/operational risk/non-financial risk.	None.
[17]	GL 1.2	A few respondents indicated the need to link the 'comprehensive security policy' with the certain provision of payment services to avoid overlaps with other business fields which are often covered by other security policies.	The EBA is of the view that the Guideline should be flexible and it is not necessary to link 'the comprehensive security policy' with the certain provision of payment services. The EBA further clarifies, as also stipulated in Article 5, Paragraph 1 (j), of PSD2, that such a policy should include a detailed risk assessment in relation to the payment services, a description of security control and mitigation measures taken to adequately protect PSUs against the risks identified, including fraud and illegal use of sensitive and personal data.	None.
[18]	GL 1.3	Several respondents indicated that 'lessons learned' should be documented and taken into account for the future. This should include documentation of losses incurred to allow the tracking of the mistakes that resulted in those losses to enable the PSPs to improve their processes.	The EBA agrees with the proposal and has therefore amended the Guideline accordingly.	GL 1.3 (now GL 2.3) has been amended and now reads: 'PSPs should ensure that the risk management framework is properly documented ~~and reviewed on an on-going basis, by the management body and where relevant, by the senior management,~~ and updated with documented 'lessons learned' during its

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				implementation and monitoring~~. In this context, Article 95 PSD2 requires PSPs to conduct an updated and comprehensive assessment of operational and security risks and the adequacy of the mitigation measures at least on a yearly basis.~~'
[19]	GL 1.4	Several respondents expressed the need to clarify what is meant by a 'major change of infrastructure, processes or procedures', as well as 'risk management framework'. One respondent expressed the view that major changes should not trigger the review of the risk management framework because: 1) the risk management framework for payment systems is part of the overall risk management framework for bank infrastructure, which should be consistent over a period of time (e.g. one to several years); 2) it may be that significant infrastructure changes and incidents take place, each of which would trigger a review/potential change of the risk management framework. Moreover, review of the risk management framework should take place at regular intervals (e.g. annually).	'Risk management framework' as stated in the 'Background' section of the Guidelines, is a framework that the PSPs shall establish with appropriate mitigation measures and control mechanisms to manage operational and security risks relating to the payment services they provide. As for the 'major change of infrastructure, processes or procedures' such infrastructure, processes, procedures differ depending on PSP's business model, size and complexity of the activities. Therefore, given the business and technological neutrality embodied in the Guidelines the EBA cannot provide a single definition for this term. The EBA is of a view that each PSP should assess whether any changes in infrastructure, processes or procedures may have a material or immaterial impact on the security, integrity or continuity of the PSP's payment-related systems and/or the security of sensitive payment data or funds. Every critical change should be taken into account when reviewing the risk management framework. In addition to reviewing the risk management framework at least once a year, which is indicated in GL 2.1, this Guideline should refer to the PSP's reaction to any given incident.	GL 1.4 (now GL 2.4) has been amended and now reads: 'PSPs should ensure that before a major change of infrastructure, processes or procedures and after each major operational or security incident affecting the security of the ~~provision of~~ payment services they provide, they review whether or not changes or improvements to the risk management framework are needed without undue delay.'
[20]	GL 1.4	One respondent recommended that the currently misleading wording of GL 1.4 be amended in accordance with the intention of paragraph 12 of the background and rationale section.	The EBA agrees with the respondent that the Guidelines should be developed in such a way that they require PSPs to embed a dynamic and agile risk management framework, with appropriate mitigation measures and control mechanisms to address current and future threats and vulnerabilities. The EBA further clarifies that the dynamic and agile concepts were some of the guiding principles when drafting GL 1.1 (now GL 2.1)–GL 1.4 (now GL 2.4).	Please see amendment ref. no. [19]

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[21]	GL 1.5	Several respondents considered it necessary to define what is meant by 'three lines of defence'. They indicated that the Guidelines should further determine more specific processes and/or objectives regarding the 'three lines of defence' or risk measures. One of them mentioned that referring to the principle of three lines of defence in accordance with the option of implementing either internal or external auditors seems inadequate and contradictory. One respondent also stated that this concept was not required in the EBA Guidelines on Information and Communication Technology (ICT) risk assessment under the Supervisory Review and Evaluation process (SREP) (EBA/GL/2017/05, 11 May 2017) and in its commentary section the EBA differentiated between general internal governance arrangements of banks on the one hand and ICT risk assessments and mitigation measures on the other hand.	The EBA is of the opinion that the existence of different business models makes it impossible to define the term 'three lines of defence'. PSPs should implement security measures in line with their security policies in order to mitigate identified risks which are currently being considered in this Guideline with an 'equivalent internal risk management and control model'. In addition, the EBA points out that it decided to draft high-level requirements that PSPs can adapt to the development of the payment services they offer and the related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable PSPs to adapt their security measures to technology changes. The measures described above should be adapted as appropriate to the PSP in question, as well as its specific risk assessment and needs. The EBA would also like to remind respondents that the proportionality principle set out in GL 1.1 should also be applied.	None.
[22]	GL 1.5	One respondent stated that PSPs should take appropriate measures to identify and manage operational and security risks and that a clear reference to the risks arising from the provision of payment services is missing.	The EBA would like to clarify that the scope of the Guidelines is limited to the provision of payment services, as indicated in the 'Scope of application' section. Therefore, this provision applies to all Guidelines, including GL 2, on governance.	None.
[23]	GL 1.6	A few respondents suggested adding that, if a PSP has not been operating for a minimum period of time, for instance three years, its CA may request that the PSP perform an external, independent audit of the security measures, or that the audit be performed by a certified auditor.	The EBA is of the view that this proposal is not needed because CAs always have the option of requiring specific supervisory measures, including requiring that an external audit be carried out.	None.
[24]	GL 1.6	A few respondents pointed out that GL 1.6 includes references to both 'auditors' and 'experts'. The term 'auditors' should be used throughout this section to make it clear what is meant. Moreover, it should be made clear that the auditor must have expertise in IT risk management.	The EBA agrees with the proposal that the term 'auditors' should be used instead of 'experts', and therefore additional clarification was added to GL 1.6 (now GL 2.6). In agreement with the comment, the EBA would like to emphasise the importance of an audit being independent and conducted by auditors with the appropriate expertise. To that end, and in line with the clarification of this term already provided by the EBA in the context of the RTS on SCA and CSC (see also https://www.eba.europa.eu/documents/10180/1894900/EBA+Opinion+on+the+amended+text+of+the+RTS+on+SCA+and+CSC+%28EBA-Op-2017-09%29.pdf), the EBA has amended GL 2.6 to say that the 'audit is to be performed by an auditor with expertise in IT security and	GL 1.6 (now GL 2.6) has been amended and now reads: 'The security measures set out in ~~the~~ these Guidelines should be audited by ~~internal or external~~ ~~independent and qualified~~ auditors with

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			payments and operationally independent within or from the payment service provider'.	expertise in IT security and payments and operationally independent within or from the PSP. ~~in accordance with the applicable audit framework of the PSPs.~~ The frequency and focus of such audits should take the corresponding security risks into consideration. ~~and neither the internal nor external independent and qualified auditors experts should be involved in any way in the development, implementation or operational management of the payment services provided~~.'
[25]	GL 1.6	One respondent indicated that this requirement may be difficult to apply, for example, to banking groups composed of autonomous entities where internal audit controls are entrusted to central structures. Further clarifications are required in the case of banking associations composed of several autonomous PSPs.	The EBA does not see any difficulties with the application of this requirement in the case where internal audit controls are entrusted to central structures. Nevertheless, the Guideline has been amended to provide more clarity. In agreement with the comment, the EBA would like to emphasise the importance of an audit being independent and conducted by auditors with the appropriate expertise. To that end, and in line with the clarification of this term already provided by the EBA in the context of the RTS on SCA and CSC (see also https://www.eba.europa.eu/documents/10180/1894900/EBA+Opinion+on+the+amended+text+of+the+RTS+on+SCA+and+CSC+%28EBA-Op-2017-09%29.pdf), the EBA has amended GL 2.6 such that the 'audit is to be performed by an auditor with expertise in IT security and payments and operationally independent within or from the payment service provider'.	Please refer to amendment ref. no. [24].
[26]	GL 1.6	One respondent expressed the view that GL 1.6, in addition to specifying that the security measures should be audited by internal or external independent and qualified auditors, should	The EBA is of the view that it is not possible to require certification for the auditing of security measures especially under PSD2. The EBA disagrees with the view that audit should not be necessary if the PSP or the third -	Please refer to amendment ref. no. [24].

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		include a statement regarding the certification required for the auditing of security measures under PSD2. Either the audit should be performed by a certified auditor or the PSP should obtain the relevant external qualification. Another respondent also proposed that an audit should not be necessary where the PSP or the third-party provider (TPP) has obtained a certification by a renowned, independent and qualified institution.	arty service provider has obtained been certified by a renowned, independent and qualified institution. Nevertheless, the Guideline has been amended to emphasise the importance of an audit being independent and conducted by auditors with the appropriate expertise. To that end, and in line with the clarification of this term already provided by the EBA in the context of the RTS on SCA and CSC (see also https://www.eba.europa.eu/documents/10180/1894900/EBA+Opinion+on+the+amended+text+of+the+RTS+on+SCA+and+CSC+%28EBA-Op-2017-09%29.pdf), the EBA has amended GL 2.6 to say that the 'audit is to be performed by an auditor with expertise in IT security and payments and operationally independent within or from the payment service provider'.	
[27]	GL 1.6	One respondent requested clarification on the technical depth the mentioned audit should have – that is, whether a paper-based exercise is sufficient or an in-depth technical assessment, such as a penetration test, is needed.	In recognition of the comment, the EBA would like to emphasise the importance of an audit being independent and conducted by auditors with the appropriate expertise. To that end, and in line with the clarification of this term already provided by the EBA in the context of the RTS on SCA and CSC (see also https://www.eba.europa.eu/documents/10180/1894900/EBA+Opinion+on+the+amended+text+of+the+RTS+on+SCA+and+CSC+%28EBA-Op-2017-09%29.pdf), the EBA has amended GL 2.6 to say that the 'audit is to be performed by an auditor with expertise in IT security and payments and operationally independent within or from the payment service provider'.	Please refer to amendment ref. no. [24].
[28]	GL 1.7	On the point of avoiding unnecessary paperwork, one respondent proposed minimum EU-wide mandatory questions for outsourcing service providers, which includes a fixed set of expected deliverables, i.e. an audit report which could also act as an inspection catalogue for auditors, related to these Guidelines. The respondent also proposed to have a list of outsourcing providers which passed an audit according to such a questionnaire.	The EBA is of the view that creating minimum EU-wide mandatory questions for outsourcing service providers is not possible. The EBA points out that each supplier should be assessed individually.	None.
[29]	GL 1.7	One respondent stated that the term 'outsourcing' should be defined. The definition should limit regulatory outsourcing to third-party providers of services which are typical for the PSP itself and which would otherwise be performed by the PSP.	The EBA points out that references to outsourcing are already included in the primary legislation having mandated the adoption of these Guidelines (PSD2, in particular Article 19). The EBA considers that outsourcing is a commonly used term that does not need to be further defined in these Guidelines.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[30]	GL 1.7	Several respondents considered that GL 1.7 is formulated in too general a manner.	In consideration of the comment, the EBA has redrafted GL 1.7 (now GL 2.7) to limit its scope to the outsourcing of operational functions of payment services, including IT systems, in line with Article 19(6) of PSD2.	GL 1.7 (now GL 2.7) has been amended and now reads: 'PSPs should ensure the effectiveness of the security measures set out in these Guidelines when operational functions of payment services, including IT systems, are outsourced.'
[31]	GL 1.7	One respondent suggested that a definition of 'effectiveness' would be useful as these terms occur in multiple parts of the Guidelines, not just in relation to outsourcing. In addition, the term 'adequacy' should be incorporated in relation to testing the design of a control and 'effectiveness' in relation to testing how well the control is operating.	The EBA clarifies that it does not see the need to include definitions of 'effectiveness' or 'adequacy' as each PSP should implement its own specific measures to ensure the mitigation of risks. Such measures depend on the PSP's size and on the nature, scope, complexity and riskiness of the particular services that the PSP provides or intends to provide.	None.
[32]	GL 1.8	Several respondents suggested that, for payment services, it is not always either possible or necessary to stipulate a contract with external providers which calls for the security measures required of the PSP to be complied with. For instance, in the case of tablet/mobile payment applications which entail fingerprint-authentication processes, the security mechanism is contained within the device purchased by the PSU, with whom the PSP cannot draw up any form of contract. The same goes for the application and the operating environment in which it is run. The PSP has no choice but to accept the contractual terms of the supplier of the operating system. Therefore, it is suggested that GL 1.8 be amended accordingly.	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 such as tablets or smartphones or providers of operating systems.	None.
[33]	GL 1.8	One respondent indicated that GL 1.8 should call out any fines or penalties for outsourced area in the event when providers do not meet performance targets.	The EBA clarifies that the specific terms of agreement between PSPs and outsourcing providers are out of scope of these Guidelines. It should be noted that the PSP is responsible for the assessment of the outsourcing provider and drawing up an appropriate contract.	None.
[34]	GL 1.8	One respondent claimed that the term 'seek assurance' needs to be clarified.	In the EBA's view the term 'seek assurance' is commonly understood, and such assurance should be checked in conjunction with the service-level agreement that each PSP has with its outsourcing provider.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[35]	GL 1.8	One respondent suggested that outsourced activities under GL 1.8, risk, should be covered in GL 2.	The EBA points out that issues connected with outsourcing have been deliberately placed in GL 1 (now GL 2) as they are linked to the governance arrangements that the PSP should have in place in relation to the provision of payment services.	None.
[36]	GL 1.8	Moreover, several respondents considered that GL 1.8 is formulated in too general a manner.	The EBA disagrees with the opinion that GL 1.8 (now GL 2.8) is formulated in too general a manner. The EBA points out that technological and business neutrality was an important guiding principle when drafting the Guidelines. The security objectives, measures and performance targets referred to in GL 1.8 (now GL 2.8) depend on the PSP's size and on the nature, scope, complexity and riskiness of the particular services that the PSP provides or intends to provide. They also depend on the relevant service-level agreement that the PSP has in place with the outsourcing provider.	None.
Feedback on responses to Question 3				
[37]	GL 2	Some respondents argued that GL 2 should reflect more clearly the fact that it is the PSP itself that is responsible for performing a reasonable assessment of its risks and reviewing that assessment.	The EBA is of the opinion that the framework provided by PSD2, and these Guidelines in particular, sufficiently stress the fact that PSPs themselves are responsible for the assessment and review of their risk landscape. More specifically, the executive summary highlights that the Guidelines set out the requirements that PSPs should implement in order to mitigate operational and security risks derived from the provision of payment services, in line with the scope of application according to which PSPs are the addressees of these Guidelines. Therefore the EBA is of the opinion that it is not necessary to introduce additional clarification with regard to the addressees.	None.
[38]	GL 2.1	Several respondents asked for more clarity on the definition of 'critical' as mentioned in GL 2.1. Another respondent argued that the classification in terms of criticality of data is too narrow and that it should be broadened to include the sensitivity of data.	The EBA agrees that the use of the term 'critical' in relation to human resources requires more clarification. The intention of the Guideline should be that any key roles in the organisation are identified. Therefore, the EBA decided to replace the term 'critical human resources' with 'key roles'.	GL 2.1 (now GL 3.1) has been amended and now reads: 'PSPs should identify, establish and regularly update an inventory of their business functions, ~~critical human resources~~ key roles ~~(especially those with privileged system access or performing sensitive business functions),~~ and

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				supporting processes in order to map the importance of each function, role and supporting processes, and their interdependencies related to operational and security risks. ~~in the provision of payment services~~.'
[39]	GL 2.1	A respondent asked for the Guideline to focus only on the necessary processes and assets for conducting the risk assessment activities, instead of describing the content of the risk assessment.	The EBA believes that the scope of these Guidelines should not be limited to the processes and assets necessary for conducting a risk assessment but that they should also provide high-level guidance on the content of the risk assessment in order to ensure a common approach in the market. Furthermore, the EBA points out that the mandate is to issue Guidelines with regard to the establishment, implementation and monitoring of the security measures and therefore all security measures prescribed therein are in line with the mandate conferred to the EBA by PSD2.	None.
[40]	GL 2.1	Another respondent asked that 'human resources' be changed to 'technical groups' in order to prevent a conflict with German law.	As highlighted under ref. no. [38], the EBA agrees to replace the term 'critical human resources' with 'key roles'.	See amendment ref. no. [38].
[41]	GL 2.2	A respondent asked for more clarity on the definition of inventory, as mentioned in GL 2.2.	The EBA would like to point out that in its opinion it is not necessary to further define the term 'inventory' within the context of GL 2.2 (now GL 3.2) as the contents of this inventory are already stated in this Guideline. Examples of items to be included in the inventory are already listed: '[…] such as ICT systems, their configurations, other infrastructures'. To further increase clarity of the requirements stated therein, the EBA redrafted the Guideline to include the purpose of keeping such inventory.	GL 2.2 (now GL 3.2) has been amended and now reads: 'PSPs should identify, establish and regularly update an inventory of the information assets ~~used for the provision of payment services,~~ such as ICT systems, their configurations, other infrastructures and also the interconnections with other internal and external systems, in order to ~~know~~ be able to manage the ~~critical~~ assets that support their critical

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				business functions and processes ~~for the provision of payment services~~
[42]	GL 2.3	Another respondent proposed that sentences 2 to 4 of GL 2.3 – 'PSPs should manage access rights to information assets and their supporting systems on a 'need-to-know' basis. Access rights should be periodically reviewed. PSPs should maintain access logs and use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of payment services' – should be moved to GL 5.3, on risk mitigation measures.	The EBA agrees with the comment. However, following its review, the EBA considers that it is more appropriate to include this text in GL 3.11 (now GL 4.10), which is on protection.	The second sentence up to the end of the paragraph of GL 2.3 (now GL 3.3) has been deleted and the deleted section moved, with amended wording, to GL 3.11 (now GL 4.10). Additionally, a new Guideline, GL 4.11, has been introduced. Therefore, GL 2.3 (now GL 3.3) now reads: 'PSPs should classify the identified business functions, supporting processes and information assets in terms of criticality. ~~PSPs should manage access rights to information assets and their supporting systems on a 'need-to-know' basis. Access rights should be periodically reviewed. PSPs should maintain access logs and use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of payment services.'~~

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				GL 3.11 (now GL 4.10) has been amended and now reads: '[…] PSPs should manage access rights to information assets and their supporting systems on a 'need-to-know' basis. Access rights should be periodically reviewed.' In addition, a new Guideline, GL 4.11, has been introduced, which reads: 'Access logs should be retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with GL 3.1 and GL 3.2, without prejudice to the retention requirements set out in EU and national law. PSPs should use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of payment services.'
[43]	GL 2.3	One respondent suggested that the Guidelines should refer to IT risk management frameworks, as defined in other regulations.	The EBA points out that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. It also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. Therefore, the EBA is of the opinion that no particular risk management framework should be imposed, as the PSPs themselves are better suited to find a risk framework proportionate to their operation. Moreover, the EBA is of the view that, if the particular Guideline were to refer to risk management frameworks defined in other regulations, a maintenance issue would be introduced inasmuch as the Guideline might have to be updated when the frameworks or other regulation are altered.	
[44]	GL 2.3	Several respondents proposed that the second last sentence be moved to GL 3, on access control. Another respondent proposed that the last sentence be moved to GL 4, on detection.	As stated under amendment ref. no. [42] , the EBA agrees to move these sentences. The text in GL 2.3 describes mitigating measures and does not fit with GL 2 (now GL 3), which is about risk analysis. Therefore, the relevant Guidelines on protection have been amended to reflect this change.	The second sentence up to the end of the paragraph of GL 2.3 (now GL 3.3) has been deleted and the deleted section, with amended wording, moved to GL 3.11 (now GL 4.10). Additionally, a new Guideline, GL 4.11, has been introduced. Therefore, GL 2.3 (now GL 3.3) now reads: 'PSPs should classify the identified business functions, supporting processes and information assets in terms of criticality. ~~PSPs should manage access rights to information assets and their supporting systems on a 'need-to-know' basis. Access rights should be periodically reviewed. PSPs should maintain access logs and use this information to facilitate identification and investigation of anomalous activities that~~

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				~~have been detected in the provision of payment services.~~' GL 3.11 (now GL 4 10) has been amended and now reads: '[…] PSPs should manage access rights to information assets and their supporting systems on a 'need-to-know' basis. Access rights should be periodically reviewed.' In addition, a new Guideline, GL 4.11, has been introduced, which reads: 'Access logs should be retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with GL 3.1 and GL 3.2, without prejudice to the retention requirements set out in EU and national law. PSPs should use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of payment services.'

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[45]	GL 2.3	Multiple respondents asked for a provision on how long the logs are to be kept to be included.	The EBA agrees that guidance should be given on how long the logs are to be kept and redrafted the text to include a requirement to set log retention periods commensurate with the criticality of the business functions, supporting processes and information assets. This requirement is in line with the other Guidelines as it uses the risk assessment as a tool for the operational and security risk framework. However, the EBA found it more appropriate to introduce a new Guideline on protection as this relates to the protection measures.	A new Guideline, GL 4.11, has been introduced, which reads: 'Access logs should be retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with Guidelines 3.1 and 3.2, without prejudice to the retention requirements set out in EU and national law. PSPs should use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of payment services.'
[46]	GL 2.3	One respondent asked the EBA to define the need-to-know principle explicitly in the Guideline.	The EBA is of the opinion that the 'need to know' principle is standard practice in the industry and sufficiently defined.	None.
[47]	GL 2.3	Another respondent asked the EBA to clarify the relationship between the asset classification and access rights.	As stated under amendment ref. no. [42], the EBA agrees to move these sentences as the text in GL 2.3 describes mitigating measures, and does not fit with GL 2 (now GL 3), which is about risk analysis. The EBA is therefore of the opinion that, by moving this sentence, the Guideline no longer inhibits a relationship between these two elements.	The second sentence up to the end of the paragraph of GL 2.3 (now GL 3.3) has been deleted and the deleted section, with amended wording, moved to GL 3.11 (now GL 4.10). Additionally, a new Guideline, GL 4.11, has been introduced. Therefore, GL 2.3 (now GL 3.3) now reads: 'PSPs should classify the identified business

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				functions, supporting processes and information assets in terms of criticality. ~~PSPs should manage access rights to information assets and their supporting systems on a 'need-to-know' basis. Access rights should be periodically reviewed. PSPs should maintain access logs and use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of payment services.'~~ GL 3.11 (now GL 4.10) has been amended and now reads: '[…] PSPs should manage access rights to information assets and their supporting systems on a 'need-to-know' basis. Access rights should be periodically reviewed.' In addition, a new Guideline, GL 4.11, has been introduced, which reads: 'Access logs should be retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				accordance with GL 3.1 and GL 3.2, without prejudice to the retention requirements set out in EU and national law. PSPs should use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of payment services.'
[48]	GL 2.3	One respondent argued that a definition of 'criticality' is missing and it is not clear which factors need to be taken into consideration for assessing of the criticality of business functions, processes and information assets – confidentiality, integrity, availability or others.	The EBA points out that it decided to draft high-level requirements, and to allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. Therefore, the EBA is of the opinion that the sense of criticality may differ from PSP to PSP and it would not be appropriate in line with the high level requirements defined in these Guidelines to define it further. The EBA therefore expects PSPs to carry out a business impact analysis to identify their critical business, processes, etc.	None.
[49]	GL 2.4	Another respondent argued that GL 2.4 should be placed under GL 3.	The EBA is of the opinion that GL2.4 (currently GL3.4) describes actions to be carried out in order to decide on what protection measures (to implement. Furthermore, as GL 2.4 (currently GL3.4) and GL 3 (currently GL4) describe two different phases within the process, the EBA is of the view that GL 2.4 (now GL 3.4) referring to the risk assessment should be kept before GL 3 (currently GL4) as the latter defines security measures for protection.	None.
[50]	GL 2.4	One respondent asked for the Guidelines to refer to IT risk management frameworks defined in other regulations and another respondent asked that the scope of the risk assessment be limited to processes and assets that are defined as high in criticality.	The EBA is of the view that if the Guidelines were to refer to risk management frameworks defined in other regulations, a maintenance issue would be introduced and the Guidelines would possibly have to be updated when the frameworks or other regulation are altered.	GL 2.4 (now GL 3.4) has been amended and now reads: 'PSPs should ensure that they continuously

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		Additionally, the respondent was of the opinion that the last sentence should be deleted.	In addition, the EBA points out that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. Therefore, the EBA is of the opinion that imposing the implementation of a particular risk management framework would not be appropriate in line with the high level requirements defined in these Guidelines, as the PSPs themselves are better suited to find a risk framework proportionate to their operation. The EBA is of the opinion that processes and assets have to be subject to risk assessments in order to decide whether they are critical or not. Prioritisation according to criticality is in the EBA's view an inherent part of any risk assessment. Therefore, it would not be advisable to limit the scope of the risk assessment. However, given that this sentence is already included in GL 2.3 (now GL 3.3), it has been removed from GL 2.4 (now GL 3.4).	monitor threats and vulnerabilities and regularly review the risk scenarios impacting their business functions ~~assets~~, critical processes and ~~business functions~~ information assets. As part of the obligation to conduct and provide CAs with an updated and comprehensive risk assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigating measures and control mechanisms implemented in response to those risks, as laid down in Article 95(2) of Directive (EU) 2015/2366, PSPs should carry out and document risk assessments, at least annually or at shorter intervals as determined by the CA of the functions, processes and information assets they have identified and classified in order to identify and assess key operational and security risks ~~for the provision of payment services~~. Such risk assessments should also be done before any major change of infrastructure, process or procedures affecting the security of payment

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				services occurs. ~~Assets, processes and functions should be prioritised according to their criticality~~.'
[51]	GL 2.4	Several respondents commented that the frequency of the periodic review of the risk assessment needs to be defined.	The EBA is of the opinion that the periodic review of the risk assessment should be done on an annual basis. This would be in line with Article 95, paragraph 2, of PSD2: 'Member States shall ensure that payment service providers provide to the competent authority on an annual basis, or at shorter intervals as determined by the competent authority, an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.'	GL 2.4 (now GL 3.4) has been amended and reads: 'PSPs should ensure that they continuously monitor threats and vulnerabilities and regularly review the risk scenarios impacting their business functions ~~assets~~, critical processes and ~~business functions~~ information assets. As part of the obligation to conduct and provide CAs with an updated and comprehensive risk assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigating measures and control mechanisms implemented in response to those risks, as laid down in Article 95(2) of Directive (EU) 2015/2366, PSPs should carry out and document risk assessments, at least annually or at shorter intervals as determined by the CA of the functions, processes and information assets they have identified and

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				classified in order to identify and assess key operational and security risks ~~for the provision of payment services~~. Such risk assessments should also be done before any major change of infrastructure, process or procedures affecting the security of payment services occurs. ~~Assets, processes and functions should be prioritised according to their criticality~~.'
[52]	GL 2.5	One respondent argued that GL 2.5 should be placed under GL 4.	The EBA is of the opinion that GL 4 (now GL 5) relates to the monitoring of the operation of the payment services. As GL 2 (now GL 3) refers to threats outside the operations of the payment services, the EBA does not agree with the respondent and does not propose to make any changes.	None.
Feedback on responses to Question 4				
[53]	GL 3	One respondent suggested that there is a need to clarify that security measures implemented by ASPSPs must not prevent or restrict the provision of payment services by TPPs.	The EBA is of the opinion that the provision of payment services by TPPs, that is, AISPs and PISPs, is sufficiently covered by PSD2 under Articles 66 and 67. Specifically: ▪ Article 66.4c of PSD2 requires that the ASPSP shall 'treat payment orders transmitted through the services of a payment initiation service provider without any discrimination other than for objective reasons, in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer'. ▪ Article 67.3b of PSD2 requires that the ASPSP shall 'treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons'.	None.
[54]	GL 3	One respondent suggested adding more clarity to the wording of requirements in GL 3 since there is lot of room for interpretation.	The EBA points out that it decided to draft high-level requirements that PSPs can adapt to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. Therefore, the EBA is of the opinion that prescribing more detailed requirements in the commented Guideline would not be appropriate in line with the high level requirements defined in these Guidelines.	
[55]	GL 3	One respondent commented that the storage of PSUs' personalised security credentials (PSC) is already regulated under PSD2. To revoke the authorisation for using the PSU credentials, there must be an explicit agreement between the PSU and the AISP (revocation is regulated in Article 55 of PSD2).	The EBA confirms that GL 3 (now GL 4) refers to the revocation of access of PSPs' personnel and not to the revocation of the consent given by a PSU to an AISP, which would be out of the scope of these Guidelines.	None.
[56]	GL 3.1	Some respondents suggested using only one term, either 'security measures' or 'security controls', as these have the same meaning, in paragraph 25 of the background and rationale of the Final Report and GL 3.1.	The EBA agrees that the same term should be used in both sections, since they were used with the same meaning, and therefore does not refer to 'security controls' in the current version of the rationale, which currently refers to changes made in the Guidelines following the public consultation.	None.
[57]	GL 3.1	One respondent was concerned about the fact that PSPs may not always be able to implement preventive measures, and suggested drawing a distinction between automated and manual controls.	The EBA is of the view that implementing security measures, including preventive measures, is part of the scope of the Guidelines. As such, all PSPs should be able to develop preventive security measures against identified operational and security risks, whether automated or manual, within a level of flexibility introduced by the proportionality principle set out in GL 1.1.	None.
[58]	GL 3.2	Many respondents mentioned the need to clarify the definition of 'defence-in-depth' and 'multi-layered controls'.	The Guideline itself explains that 'defence-in-depth' should be understood as meaning more than one control covering the same risk. The EBA has included in GL 3.2 (now GL 4.2) explicit references to the 'four-eyes principle' and to 'two-factor authentication' as required practices regarding the implementation of the 'defence-in-depth' approach as well as the implementation of network segmentation and the establishment of multiple firewalls. A technical examples of the 'defence-in-depth' approach would be the implementation of prevention mechanisms against, for example, hackers by employing firewalls and IDS/IPS (network layer), by using application firewalls (application layer), by conducting server hardening (operating system) and so on. All these measures together can be regarded as 'multi-layered controls' because they tackle the same risk (hacker intrusion) in deferent layers, whereas a network firewall alone could be bypassed by an experienced attacker.	GL 3.2 (now GL 4.2) has been amended and now reads: 'PSPs should establish and implement a 'defence-in-depth' approach by instituting multi-layered controls covering people, processes and technology ~~related to the provision of payment services~~, with each layer serving as a safety net for preceding layers. Defence-in-depth

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				should be understood as having defined more than one control covering the same risk such as the 'four-eyes principle', two-factor authentication, network segmentation and multiple firewalls.'
[59]	GL 3.2	Some respondents suggested referring to 'three levels of defence' instead of 'defence-in-depth'.	The EBA is of the view that 'defence-in-depth' and 'three lines of defence' (covered under GL 2.5) are different concepts. 'Defence-in-depth' means building security measures into different levels to address the same risks while 'three lines-of-defence' refers to organisational structure. Therefore, the EBA does not agree with the suggestion to replace 'defence-in-depth' by 'three levels of defence'.	None.
[60]	GL 3.2	Some respondents believed that that it should not be mandatory to have more than one control covering the same risk, since this may not be relevant for all operational risks, especially those with rather low impacts and likelihood and also because this would be difficult to implement or even counterproductive, for example having to install two different types of antivirus software on the same computer.	The EBA is of the opinion that 'defence-in-depth' is an effective approach to mitigating risks and also widely considered as a best practice. Defence-in-depth can also be achieved by overarching organisational, technical or physical security measures that tackle several different risks. For this reason, it is up to the PSP to cover all of its processes, in different layers, in accordance with its risk assessment. The 'defence-in-depth' concept does not require the installation of two different types of antivirus software on every computer. Therefore, the EBA does not consider it appropriate to redraft the commented requirements.	None.
[61]	GL 3.2	One respondent was concerned that 'multi-layered controls' could be misinterpreted and could lead, in practice, to the situation whereby, instead of developing smart and robust controls, numerous multi-layered controls are designed at the first line of defence without any higher security but solely to achieve compliance with the regulation. The respondent suggested a reference to the general and therefore more adequate 'three lines of defence' principle instead.	The EBA is of the view that 'defence-in-depth' and 'three lines of defence' (covered under GL 2.5) are different concepts. 'Defence-in-depth' is an approach of building security measures in different levels for the same risks while 'three-lines-of-defence' refers to organizational structure. Therefore the EBA does not agree with the suggestion to replace 'the reference to 'multi-layered controls' by 'three lines of defence'.	None.
[62]	GL 3.2	One respondent raised concerns that the general requirement for multi-layer controls would contravene the principle of proportionality. He suggested rewording the sentence as follows: 'adequate control mechanisms, e.g. multi-layered controls covering people, processes and/or technology […] provided that the respective risk qualifies as relevant for the	The EBA is of the view that 'defence-in-depth' is an approach and as such is also proportional. It is the responsibility of PSPs to ensure the security all of their processes, in different layers, in accordance with their risk assessment, as required in GL 3, on risk assessment.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		proper performance of payment services and calls for a multi-layered control setting.'		
[63]	GL 3.2	One respondent considered that a PSP that is too small to operate an in-house three lines of defence model or technical controls to manage security risks should be required to use third-party services to provide the independent challenge and attestation which an in-house function would normally provide.	The EBA is of the view that all Guidelines should apply to all PSPs so as not to favour specific business models and 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 GL 1.1, which means that the steps that PSPs are required to take to be compliant may differ between PSPs depending on their size and on the nature, scope, complexity and riskiness of the particular service(s) they provide or intend to provide. In particular, for the business model and technological neutrality reasons stated above, the EBA does not agree that a PSP could be prevented from being able to comply with the requirements defined in these Guidelines by the fact of being too small. The EBA is of the opinion that it is up to the PSPs themselves, in line with the principle of proportionality, set out in GL 1.1, to comply with the requirements of these Guidelines by their own means or by relying on/outsourcing it to TPPs.	None.
[64]	GL 3.3	A few respondents suggested, for better clarity, splitting the sentence into two separate parts as follows: 'PSPs should protect the confidentiality, integrity and availability of their critical logical and physical assets, resources related to the provision of payment services. PSPs should protect the sensitive payment data of their payment service users against abuse, attacks and inappropriate access and theft.'	The EBA is of the opinion that the suggested rewording would affect the intended meaning. However, an amendment has been made in order to clarify the sentence. In addition, following the comments on GL 3.5, and having considered necessary revisions to GL 3.5, the EBA decided to merge GL 3.5 with GL 3.3 (now GL 4.3) to avoid overlap.	GL 3.3 (now GL 4.3) has been amended and now reads: 'PSPs should ~~protect~~ ensure the confidentiality, integrity and availability of their critical logical and physical assets, resources ~~related to the provision of payment services~~ and sensitive payment data of their PSUs whether at rest, in transit or in use. If the data include personal

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				data, such measures should be implemented in compliance with Regulation (EU) 2016/67[16] or, if applicable, Regulation (EC) 45/2001[17]. ~~against abuse, attacks and inappropriate access and theft.~~'
[65]	GL 3.3	One respondent was concerned about the robustness and security of screen scraping as a method of access provision for TPPs. He therefore strongly recommended that the EBA includes guidance on the protection requirements expected of TPPs and security issues created by screen scraping.	The EBA points out that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guideline. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. Therefore, the EBA is of the opinion that prescribing a a specific access method in the commented Guideline would not be appropriate in line with the principle of technological and business model neutrality followed in drafting these Guidelines.	None.
[66]	GL 3.5	Many respondents suggested the need to clarify the definition of 'sensitive data', 'user data' and 'critical resources' in accordance with the GDPR.	For better clarity the EBA has removed references to payment data, user data, credentials and certificates and included instead 'sensitive payment data'. It is clarified that the terms 'sensitive payment data' have the same meaning as in PSD2. The EBA also clarifies that the remaining term 'critical resources' corresponds to the resources the PSP classify as critical according to its own risk assessment performed under GL 2.4 (now GL 3.4).	GL 3.5 has been merged with GL 3.3 (now GL 4.3), which now reads: 'PSPs should ~~protect~~ ensure the confidentiality, integrity and availability of their critical logical and physical assets, resources ~~related to the provision~~

[16] Regulation (EU) of the European Parliament and of the Council of 27 April2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).
[17] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			Following the above comments and having considered necessary revisions to GL 3.5, the EBA decided to merge it with GL 3.3 (now GL 4.3) to avoid overlap.	~~of payment services~~ and sensitive payment data of their PSUs whether at rest, in transit or in use. If the data include personal data, such measures should be implemented in compliance with Regulation (EU) 2016/67[18] or, if applicable, Regulation (EC) 45/2001.[19] ~~against abuse, attacks and inappropriate access and theft.~~'
[67]	GL 3.5	One respondent suggested adding 'in use' such that the first sentence reads 'whether at rest, in use or in transit'.	The EBA agrees with the comment and has added 'in use' at the end of the first sentence for completeness. Furthermore, taking into considerations all comments on GL 3.5 and having the necessary revisions to GL 3.5, the EBA decided to merge GL 3.5 with GL 3.3 (now GL 4.3) to avoid overlap.	GL 3.5 has been merged with GL 3.3 (now GL 4.3), which now reads: 'PSPs should ~~protect~~ ensure the confidentiality, integrity and availability of their critical logical and physical assets, resources ~~related to the provision of payment services~~ and sensitive payment data of their PSUs whether at rest, in transit or in use. If the data include personal data, such measures should be implemented in compliance with Regulation

[18] Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[19] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				(EU) 2016/67[20] or, if applicable, Regulation (EC) 45/2001.[21] ~~against abuse, attacks and inappropriate access and theft.~~'
[68]	GL 3.5	Many respondents suggested the need to clarify the scope of the software that is subject to integrity-checking mechanisms and suggested that it be clarified that it concerns only software that is under the control of the PSP, that is, that the operating system and the web browser of the PSU's device are excluded.	The EBA clarifies that PSPs should ensure that integrity-checking mechanisms are in place in order to verify the authenticity and integrity of software, firmware and information on their payment services. This relevant amendment has been added in the Guideline and has been moved to GL 3.8 (now GL 4.7).	GL 3.5 has been merged with GL 3.3 (now GL 4.3), which now reads: 'PSPs should ~~protect~~ ensure the confidentiality, integrity and availability of their critical logical and physical assets, resources ~~related to the provision of payment services~~ and sensitive payment data of their PSUs whether at rest, in transit or in use. If the data include personal data, such measures should be implemented in compliance with Regulation (EU) 2016/67[22] or, if applicable, Regulation (EC) 45/2001[23]. ~~against abuse, attacks and inappropriate access and theft.~~'

[20] Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).
[21] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).
[22] Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).
[23] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				In addition, GL 3.8 (now GL 4.7) has been amended and now reads: '~~Upon access to the payment service,~~ PSPs should regularly check that the software used for the provision of payment services including the users' payment related software, is up to date and critical security patches are deployed. PSPs should ensure that integrity checking mechanisms are in place in order to verify the integrity of software, firmware and information on their payment services.'
[69]	GL 3.5	Several respondents raised concerns on technological neutrality and suggested amending last sentence to read 'Integrity checking or organisational processes …'	The EBA is of the view that integrity checking mechanisms refer by default to technical components and as such an amendment is not considered required.	None.
[70]	GL 3.5	One respondent suggested dividing the Guideline into two parts: 'protection of sensitive data' and 'integrity checking'.	The EBA agrees with this comment. The last sentence regarding integrity checking has been moved to GL 4.7 as stated in response to amendment ref. no.[68].	GL 3.5 has been merged with GL 3.3 (now GL 4.3), which now reads: 'PSPs should ~~protect~~ ensure the confidentiality, integrity and availability of their critical logical and physical assets, resources ~~related to the provision of payment services~~ and sensitive payment data of their PSUs whether at rest, in transit or in use. If the data include personal

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				data, such measures should be implemented in compliance with Regulation (EU) 2016/67[24] or, if applicable, Regulation (EC) 45/2001[25]. ~~against abuse, attacks and inappropriate access and theft.~~' GL 3.8 (now GL 4.7) has been amended and now reads: '~~Upon access to the payment service,~~ PSPs should regularly check that the software used for the provision of payment services including the users' payment related software, is up to date and critical security patches are deployed. PSPs should ensure that integrity checking mechanisms are in place in order to verify the integrity of software, firmware and information on their payment services.'
[71]	GL 3.5	Some respondents asked for the addition of specific security requirements for TPPs on how to access, store and use the PSC of PSUs.	The EBA is of the opinion that security requirements on how to access, store and use the PSC of PSUs are already addressed by the RTS on strong	None.

[24] Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).
[25] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			customer authentication and common and secure communication (RTS on SCA and CSC). Hence, the EBA is of the opinion that this comment is out of scope of these Guidelines.	
[72]	GL 3.6	Some respondents suggested that agile software development should be recognised as a compliant approach to segregation of duties. In addition, another respondent suggested that segregation of environments should also apply to data.	The EBA points out that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable PSPs to adapt their security measures to technology changes. Therefore, the EBA is of the opinion that recognising agile development practices as adequate is out of the scope of the mandate of these Guidelines, as it would not be appropriate in line with the high level requirements defined in these Guidelines. The EBA would further like to point out that segregation of duties and least privilege accesses should in the EBA's opinion always be applied regardless of the development practices used by PSPs. The EBA is of the opinion that segregation of duties is relevant in the context of conflicting interests in relation to certain organisational roles. The EBA is also of the view that IT environments include data by default. Therefore, a further amendment is not appropriate.	None.
[73]	GL 3.7	Many respondents suggested the need to clarify the definition of 'data minimisation' and 'sensitive data', particularly in the context of the GDPR.	The EBA clarifies that the term 'sensitive payment data' has the same meaning as in PSD2 and should be understood within the referred context. As for the term 'data minimisation', the EBA clarifies that it should be understood in the context of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – 'GDPR'). Since the term 'data minimisation has not been used elsewhere in the Guidelines the EBA, for greater clarity, has redrafted the relevant Guideline to be in line with both PSD2 and the GDPR (including the concept of data minimisation in the requirements of this Guideline, instead of defining it).	GL 3.7 (now GL 4.6) has been amended and now reads: 'In designing, developing and <u>providing</u> ~~maintaining~~ payment services, PSPs should ensure that ~~data minimisation is an essential component of the core functionality~~ the <u>collection</u> ~~gathering,~~ routing, processing, storing and/or archiving, and visualisation ~~of~~

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				sensitive payment data of the PSUs is adequate, relevant and limited to what necessary for the provision of its payment services. ~~: of sensitive data should be kept at the absolute minimum level.~~'
[74]	GL 3.7	One respondent considered that the 'data minimisation' principle should only apply to data transferred outside of the PSP's infrastructure.	The EBA is of the view that the data minimisation principle shall also apply to data stored within the PSP's infrastructure. Therefore, the suggested amendment is not appropriate in the EBA's view.	None.
[75]	GL 3.7	One respondent was concerned that the 'data minimisation' requirement could conflict with other legal requirements such as commercial law, tax law and anti-money laundering regulations, and suggested adding a second sentence as follows: 'The aim of a minimum level in relation to storing and/or archiving does not interfere with legal requirements on the storage and/or the archiving of data'.	While drafting these Guidelines, the EBA considered to the extent possible the requirements stemming from other regulations and the requirements in these Guidelines are related only to the management of the operational and security risks. Due to the material differences in the addressees, objectives and scope of different regulatory requirements with regard to cyber risks and operational risks, it is impossible to merge or harmonise them to a greater extent, as these Guidelines relate only to managing operational and security risks in the provision of payment services. With regard to this particular comment, the EBA clarifies that reference to laws and regulations regarding taxes and anti-money laundering regulations would be redundant in these Guidelines and the EBA did not identify any conflicting requirements. The EBA is of the opinion that keeping data at the minimum level does not mean interference with legal requirements. If data have to be kept because of legal requirements, the minimum level would be defined by these legal requirements.	None.
[76]	GL 3.7	One respondent suggested adding that PSUs should give clear, direct consent to all access by TPPs to transactional payment data.	The EBA is of the opinion that security requirements on how to access, store and use the PSC of PSUs are already addressed by the RTS on SCA and CSC. Hence, the EBA is of the opinion that the comment is out of scope of these Guidelines.	None.
[77]	GL 3.8	One respondent found the meaning of this paragraph to be unclear.	In recognition of this comment the EBA redrafted the relevant Guideline to clarify the scope, content and frequency of the control.	GL 3.8 (now GL 4.7) has been amended and now reads: '~~Upon access to the payment service,~~ PSPs

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				should regularly check that the software used for the provision of payment services, including the users' payment related software, is up to date and critical security patches are deployed. PSPs should ensure that integrity checking mechanisms are in place in order to verify the integrity of software, firmware and information on their payment services.'
[78]	GL 3.8	Many respondents suggested the need to clarify the meaning of 'up to date'.	The EBA agrees with this comment and therefore has redrafted the Guideline accordingly, adding a requirement for critical security patches to be deployed.	GL 3.8 (now GL 4.7) has been amended and now reads: '~~Upon access to the payment service,~~ PSPs should regularly check that the software used for the provision of payment services, including the users' payment related software, is up to date and critical security patches are deployed. PSPs should ensure that integrity checking mechanisms are in place in order to verify the integrity of software, firmware and information on their payment services.'

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[79]	GL 3.9	One respondent asked for any reference to physical security measures to be removed since such measures are already addressed by broader regulations.	The EBA is of the opinion that the mandate given by Article 95(3) of PSD2 refers to security measures whether or not they are physical and is of the opinion that such measures apply only to the provision of payment services, as indicated in the scope of these Guidelines. Physical security measures are fully part of operational and security measures.	None.
[80]	GL 3.9	One respondent suggested that physical security should also include people and buildings. Another respondent also suggested that physical security measures must include also all relevant processes that deal with physical security for PSUs, for example enrolment of PSUs and issuing PSUs with credentials.	The EBA agrees. The draft guideline 'PSPs should have appropriate physical security measures in place, in particular to protect the personal and sensitive data of the PSU as well as its information systems used to provide payment services' may be misinterpreted as a need to protect only the PSUs' information systems and not the PSP's own information systems. Therefore, the relevant Guideline has been amended to clarify that all information systems used to provide payment services need to be protected.	GL 3.9 (now GL 4.8) is amended and now reads: 'PSPs should have appropriate physical security measures in place, in particular to protect the ~~personal and~~ sensitive payment data of the PSUs as well as ~~its~~ the ~~information~~ ICT systems used to provide payment services. ~~Physical access to corresponding systems should be limited to authorised personnel only and regularly reviewed.~~'
[81]	GL 3.10	Some respondents raised concerns about the requirement that the right to authorise access be restricted to the management body or to senior management.	The EBA agrees. In order to accommodate large organisations in which authorising access is generally delegated by the management body or by senior management, for example, to middle management, the Guideline has been amended to remove the specific reference to the management body and to senior management.	GL 3.10 (now GL 4.9) is amended and now reads: 'Physical and logical access to ICT systems should be permitted only for authorised individuals ~~who are authorised by the management body or, where relevant, by senior management;~~. ~~a~~Authorisation should be assigned according to the staff's tasks and responsibilities, limited to individuals who are appropriately trained and monitored. PSPs should

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				institute controls that reliably restrict such access to ICT systems to those with a legitimate business requirement. Electronic access by applications to data and systems should be limited to the minimum that is required to provide the relevant service ~~possible.~~'
[82]	GL 3.10	One respondent also suggested providing further details in the event of outsourcing.	The EBA would like to clarify that risks related to outsourcing are already addressed by GL 1.7 and GL 1.8, now GL 2.7 and GL 2.8 respectively, and should apply throughout the requirements of these Guidelines.	None.
[83]	GL 3.10	Some respondents suggested calling out relevant controls such as the 'four-eyes principle'.	The EBA confirms that the 'four-eyes principle' is an example of a principle that can be used to implement 'defence-in-depth'. The EBA clarified this by making an explicit reference to the 'four-eyes principle' in GL 3.2 (now GL 4.2).	GL 3.2 (now GL 4.2) has been amended and now reads: 'PSPs should establish and implement a 'defence-in-depth' approach by instituting multi-layered controls covering people, processes and technology ~~related to the provision of payment services~~, with each layer serving as a safety net for preceding layers. Defence-in-depth should be understood as having defined more than one control covering the same risk such as the 'four-eyes principle', two-factor authentication, network segmentation and multiple firewalls.'

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[84]	GL 3.11	One respondent considered that it might be beneficial to add some reference to the need to have a priority focus on rules regarding the freedom and dignity of workers.	The EBA considers that these domains are out of scope of the mandate to draft these Guidelines given by PSD2.	None.
[85]	GL 3.12	One respondent suggested that there is need to clarify the meaning of 'critical IT components' and suggested using the definition in Payment Card Industry Data Security Standards v3.2 Requirements 7.1.2.	The EBA considers that critical IT components are those identified by the PSP when carrying out its risk assessment under GL 2.4 (now GL 3.4). Thus, the EBA does not agree that there is a need to amend the Guideline to clarify this term.	None.
[86]	GL 3.12	Some respondents considered that the requirement does not take into account mainframe systems, remote access to which may be gained via simple password emulation.	The EBA is not aware of any insurmountable obstacle preventing PSPs from implementing strong authentication, also called 'multi-factor authentication', to secure remote access to mainframe systems. Thus, the EBA does not agree that there is a need to amend the Guidelines in this respect.	None.
[87]	GL 3.12	Some respondents were concerned that strong authentication, as a set of at least two factors, may be difficult to apply in the case of remote administrative access. Therefore, they considered that clarification is needed on the validity of alternative measures such as client's MAC (media access control) address filtering or physical access controls.	The EBA clarifies that the term 'strong authentication' has the same meaning as 'strong customer authentication' set out in PSD2 and should be understood within the referred context. The EBA confirms that strong authentication should be based on a set of at least two independent factors in the areas of possession, knowledge and inherence. One factor may be a possession element, such as a specific computer located in a secured room dedicated to remote administrative access with strict physical access control.	None.
[88]	GL 3.12	One respondent suggested that remote administrative access should be given only for emergency cases, and that, in addition to strong authentication, close supervision and real-time monitoring would offer even better security.	The EBA considers that remote administrative access should be part of the supporting processes that are continuously assessed in terms of criticality by PSPs under GL 2.4 (now GL 3.4). In the EBA's opinion, a PSP may decide, based on the results of its risk assessment, to restrict remote administrative access to emergency cases, such as when recovery or contingency plans are activated. Continuous monitoring and detection of anomalous activities are already addressed by GL 4.1 (now GL 5.1).	None.
[89]	GL 3.13	One respondent suggested adding the following text at the end of the last sentence: 'procedures should be subjected to the same protection requirements'.	The EBA agrees. Therefore, the first sentence has been amended to include 'procedures' in the list of elements that should be protected.	GL 3.13 (now GL 4.13) has been amended and now reads: 'The operation of products, ~~and~~ tools and procedures related to access control processes should protect the access control processes from

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				being compromised or circumvented. This includes enrolment, delivery, revocation and withdrawal of corresponding products, tools and procedures.'
Feedback on responses to Question 5				
[90]	GL 4	Several respondents requested a more explicit reference to the EBA's final Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2) – EBA/GL/2017/10— in GL 4, specifically in GL 4.4, GL 4.5 and GL .6.	With regard to GL 4.4 (now GL 5.4), the EBA is of the opinion that PSPs, when determining appropriate criteria and thresholds for classifying an event as a security incident, should also consider EBA/GL/2017/10. The EBA is of the opinion that an explicit reference in GL 4.5 and GL 4.6 (now GL 5.5 and GL 5.6 respectively) to its Guidelines on major incident reporting EBA/GL/2017/10 is not appropriate, since neither the monitoring, handling and follow-up of an incident nor its reporting to the senior management is covered by the Guidelines on incident reporting.	None.
[91]	GL 4	One respondent suggested that GL 4 should cover not only technical, but also organisational processes.	The EBA is of the opinion that the current wording of GL 4 (now GL 5) covers organisational processes as well as technical ones. Hence, in this respect no amendment of the current wording of GL 4 (now GL 5) is considered necessary in this context.	None.
[92]	GL 4.1	One respondent suggested that GL 4.1 should include requirements for the monitoring and detection of anomalous activities for enrolment and issuing processes that intrusion detection systems will not be able to detect.	As the enrolment and issuing processes are considered part of the provision of payment services, the EBA does not see a need to change the wording of GL 4.1 (now GL 5.1) in this respect.	None.
[93]	GL 4.2	Several respondents required clarity on terms used in GL 4.2, specifically 'continuous monitoring and detection processes', 'internal and external factors', 'misuse of access', 'service providers' and 'advanced threat activities'.	The EBA points out that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. For the Guidelines to remain futureproof, the necessary flexibility of PSPs should not be restricted by definitions of terms for which a general understanding exists at the market. Furthermore, as related threats might change over the time, such definitions might become out of date quite soon. Therefore, the EBA is of the opinion that changing the wording of	GL 4.1 (now GL 5.1) is amended and now reads: 'PSPs should establish and implement processes and capabilities to continuously monitor business functions, supporting processes and information assets in order to detect anomalous activities ~~and events~~ in the provision of payment services. As part

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			GL 4.2 (now GL 5.2) would not be appropriate in line with the high level requirements defined in these Guidelines. Nevertheless, the EBA decided to redraft GL 4.1 (now GL 5.1) and GL 4.2 (GL 5.2) slightly to reduce the potential for ambiguity.	of this continuous monitoring, PSPs should have in place appropriate and effective capabilities for detecting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets used in the provision of payment services ~~intrusion detection capabilities in place.~~' GL 4.2 (now GL 5.2) is amended and now reads: 'The continuous monitoring and detection processes should cover: a) relevant internal and external factors, including business ~~line~~ and ~~IT~~ ICT administrative functions; b) ~~and~~ transactions, in order to detect misuse of access by service providers or other entities~~,~~; and c) potential ~~insider~~ internal and external threats ~~and other advanced threat activities~~'.
[94]	GL 4.2	One respondent stated that GL 4.2 should apply only to the PSP's own functionality.	The EBA is of the opinion that GL 4.2 (now GL 5.2) should apply regarding all relevant functions, which might also have their root outside the PSP's own functionality.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[95]	GL 4.3	One respondent requested an additional requirement to implement an overall ISMS for all internal and external reporting procedures, for example in accordance with the EBA Guidelines on incident reporting.	Although not explicitly mentioned, ISMSs are implicitly included in GL 5.5 and GL 5.6. Therefore, the EBA does not consider an amendment necessary.	None.
[96]	GL 4.3	One respondent requested further clarification with regard to 'detective measures to identify possible information leakages'.	The EBA points out that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. For the Guidelines to remain futureproof, the necessary flexibility of PSPs should not be restricted by definitions of terms that are generally understood on the market. Furthermore, as related threats might change over time, such definitions might become out of date quite soon. Therefore, the EBA is of the opinion that introducing the proposed definition would not be appropriate in line with the high level requirements defined in these Guidelines.	None.
[97]	GL-4.4	Several respondents asked the EBA to define and clarify the terms 'event', 'security incident' and 'warning indicators' and to introduce a reference to EBA/GL/2017/10.	The terms 'operational and security incident' are already defined in EBA/GL/2017/10. However, for greater clarity and consistency with the above Guidelines, the EBA has included the definition of the term 'operational or security incident' in the 'Definitions' section of the Guidelines. As regards the precise meaning of the terms 'operational incident' and 'security incident', the EBA found it inappropriate to further define such in these Guidelines, but since the general definition from EBA/GL/2017/10 has been adopted for the purpose of these Guidelines, both terms should be read in accordance with the explanatory notes to EBA/GL/2017/10, p. 41. The EBA considers that the word 'event' is commonly understood and self-explanatory, meaning something that happened. Furthermore, it is not defined in other EBA Guidelines either. For further clarity, please note that the term 'incident' is defined in the EBA Guidelines on incident reporting and that 'event', hence, has a broader meaning than 'incident', that is, an event or several events can result or not result in an incident. With regard to the determination of early warning indicators, the EBA is of the opinion that the PSPs should have the necessary flexibility to define these indicators themselves, as they depend on the specific business model and risk profile of the PSP. However, the EBA clarifies that an early	Additional definitions the section 'Subject matter, scope and definitions', which now reads: 'Operational or security incident: A singular event or a series of linked events unplanned by the PSP which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.' With regard to the determination of 'early warning indicators', the GL 4.4 (now GL 5.4) has

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			warning indicator should serve as an alert for the PSP, enabling early detection of operational and security incidents, and amended the Guideline accordingly. In addition, further changes have been introduced to avoid the Guideline being interpreted to mean that a PSP can redefine the terms set out in the Guidelines.	been amended and now reads: 'PSPs should determine appropriate criteria ~~definitions~~ and thresholds ~~and early warning indicators~~ for classifying an event as an operational or ~~a~~ security incident, as set out in the 'Definitions' section of these Guidelines, ~~in the provision of payment services~~ as well as early warning indicators that should serve as an alert for the PSP to enable early detection of operational or security incidents.'
[98]	GL 4.4	One respondent asked that all Guidelines and definitions regarding incident reporting are harmonised among the European authorities.	While drafting these Guidelines, the EBA considered to the extent possible the requirements stemming from other regulations and the requirements in these Guidelines are related only to the management of the operational and security risks. Due to the material differences in the addressees, objectives and scope of different regulatory requirements with regard to cyber risks and operational risks, it is impossible to merge or harmonise them to a greater extent, as these Guidelines relate only to managing operational and security risks in the provision of payment services. With regard to this particular comment, the EBA clarifies that in order to cater for a harmonisation of definitions at least among the regulations issued by the EBA itself, the definition of 'operational or security incident' from EBA/GL/2017/10 will also be applied in these Guidelines.	Please refer to amendment ref. no. [97]
[99]	GL-4.4	One respondent suggested that the definition of a major security incident, including, for example, a warning indicator, be determined directly by the EBA.	The EBA decided to rely for the term 'operational and security incident' on the definition provided in EBA/GL/2017/10. The EBA remarks that EBA/GL2017/10 defines the term 'major' with regard to reporting obligations to CAs. The internal definition of 'major incident' for a specific PSP might differ from the reporting context. With regard to the determination of early warning indicators, which was specifically requested, the EBA is of the opinion that PSPs should have the	Please refer to amendment ref. no. [97]

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			necessary flexibility to define these indicators themselves, in line with the principle of proportionality set out in GL 1.1, as they depend on the specific business model of the PSP.	
[100]	GL-4.5	One respondent was of the opinion that consistent and integrated reporting is not always possible due to fragmented and different reporting obligations. Since events are not always managed by the same department, a fully integrated reporting structure is more difficult to achieve.	Incident reporting as such is out of scope of these Guidelines, which focus only on the management of operational and security risks. However, the EBA would like to point out that, while drafting EBA/GL/2017/10, it considered to the extent possible its impact on other regulations. However, due to material differences in the addressees, objectives and scope of different regulatory requirements with regard to cyber and operational risks, it is impossible to merge or harmonise them to a greater extent.	None.
[101]	GL-4.6	Some respondents asked the EBA to introduce the wording 'major' security incidents in line with the guidelines on incident reporting (EBA/GL/2017/10) and limit the reporting to the senior management to these incidents.	The EBA is of the opinion that the current wording of the Guidelines offers each PSP the flexibility to define its internal reporting procedures according to its own needs. While, it could also be necessary, for internal needs, to report non-major incidents (in the sense of EBA/GL/2017/10) to the senior management, this could be done not as extensively as for major incidents.	None.
[102]	GL-4.6	One respondent asked that it be clarified that GL 4.6 includes establishing procedures with outsourcing service providers to inform the PSP about security incidents and security-related customer complaints.	As GL 1.7 and GL 1.8 (now GL 2.7 and GL 2.8) cover the aspect of outsourcing and GL 1.8 (now GL 2.8) also contains requirements regarding the contracts between the PSP and the outsourcing provider, the EBA does not see the need to amend GL 4.6 (now GL 5.6).	None.
Feedback on responses to Question 6				
[103]	GL-5	One of the respondents suggested decreasing the number of concepts in the Guideline on business continuity or providing definitions thereof. According to one respondent, this prevents PSPs from continuing to work with their current methodology and is too burdensome.	The EBA points out that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. In consideration of the above, the EBA is of the opinion that concepts and terms used in this specific Guideline are not specific and are rather high level, as well as already known and applied by PSPs. The Guideline uses only those concepts and terms that have a broad acceptance in the market. PSPs can have own methodologies established and still be	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			compliant with the Guidelines in line with the principle of proportionality set out in GL 1.1.	
[104]	GL-5	One respondent suggested removing GL 5 from these Guidelines and instead including it in a separate Guideline on business resilience.	In the EBA's view, the term 'business resilience' is more related to a strategic risk management approach and has a broader general scope which differs from the rather action-oriented concept of business continuity. Although the EBA regards business resilience as an important strategic approach, it also considers it out of the scope of these Guidelines. Therefore, the EBA does not see the need to amend GL 5 (now GL 6) in this respect.	None.
[105]	GL-5.1	One respondent requested clarification of the term 'Limit losses' and several respondents asked for a definition of 'severe business disruptions'.	In the EBA's view the term 'losses' could refer to financial as well as reputational losses and therewith loss of customers etc. All potential losses should be limited to the extent possible. PSPs 'limit losses' by maintaining the critical assets needed to keep their business functions and processes running. The meaning of criticality is defined in GL 2 (now GL 3). In addition, the EBA points out that, in its opinion, severe business disruption is a circumstance in which payment services cannot continue in the normal way. The operation of payment services can be described as normal when activity/operations are restored to the same level of service/conditions as defined by the PSP or laid out externally by a service-level agreement in terms of processing times, capacity, security requirements, etc., and contingency measures are not in place. Therefore, the EBA does not see the need to amend GL 5.1 (now GL 6.1) in this respect.	None.
[106]	GL-5.1	Several respondents requested that GL 5.1 clarifies the fact that payment services must be provided to the extent possible in the event of a severe business disruption.	The EBA agrees with the respondents. Under certain circumstances it might not be possible to continue payment services in the normal way. This means that BCPs can also define alternative procedures that are to be used if the 'normal' processes are not operational. The PSP should strive for a provision of services on an on-going-basis. In recognition of the comment the EBA decided to amend the relevant Guideline.	GL 5.1 (now GL 6.1) has been amended and reads: 'PSPs should establish sound business continuity management to ~~ensure~~ maximise their ability to provide payment services on an on-going basis and to limit losses in the event of severe business disruption.'

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[107]	GL-5.2	Several respondents requested that the terms 'critical functions, processes, systems, transactions and interdependencies' be clarified.	The EBA considers these terms to be part of a non-exhaustive list of issues that PSPs will consider during their risk assessment process. These are only examples of issues that could be considered for the prioritisation of business continuity actions. The terms have to be understood in a broad sense. Further clarification, according to the EBA's understanding, is provided below: - Which business functions are critical?: this depends on the conduct of a PSP's own risk assessment. For further clarity as to what criticality means, please refer to GL 2 (now GL 3). - Processes: these can be supporting business processes as well as supporting technical processes. - Systems: these are usually IT systems that support these processes. - Transactions: these are financial transactions. - Interdependencies: these can exist between all issues; in other words, if a specific system fails, the supported processes fail as well.	None.
[108]	GL-5.2	Several respondents considered that the requirements under GL 5.2 are the same as GL 2.	The EBA agrees to some extent with the respondents. A risk assessment that is required under GL 2 (now GL 3) is necessary but not sufficient in order to establish a BCP. A risk assessment such as that performed under GL 2 (now GL 3) can be used as a basis for the risk assessment in the context of business continuity. Nevertheless, the Guideline has been amended to clarify the possible interconnections with GL 2 (now GL 3).	GL 5.2 (now GL 6.2) has been amended and now reads: 'In order to establish sound business continuity management, PSPs should carefully analyse their exposure to severe business disruptions and assess, ~~(~~quantitatively and qualitatively~~)~~, their potential impact, using internal and/or external data and scenario analysis. ~~The PSP should identify its critical functions, processes, systems, transactions and interdependencies to~~ On the basis of the identified and classified critical

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				functions, processes, systems, transactions and interdependencies in accordance with GL 3.1 to GL 3.3, PSPs should prioritise business continuity actions using a risk based approach, which can be based on the risk assessments carried out under GL 3. Depending on the business model of the PSP, this may ~~depending on the design of the PSP~~ for example facilitate the further processing of critical transactions ~~for example~~ while remediation efforts continue.'
[109]	GL-5.2	One respondent suggested that international standards on operational continuity be taken into account and that the Guideline be rephrased as follows: 'In order to establish a sound business continuity management, PSPs should carefully evaluate the continuity and recovery priorities, objectives and targets, assessing the impacts of severe business disruptions and identifying, analysing and evaluating the risk of disruptive incidents to the PSP. The PSP should identify its critical functions, processes, systems, transactions and interdependencies to prioritise business continuity actions using a risk based approach, which may, depending on the design of the PSP, facilitate the processing of critical transactions, for example, while remediation efforts continue.'	In consideration of the comment the EBA has redrafted GL 5.2 (now GL 6.2) to make it clearer, but did not follow the proposed wording to avoid repeating the requirements stated in GL 3, to which an explicit reference has been provided.	GL 5.2 (now GL 6.2) has been amended and now reads: 'In order to establish sound business continuity management, PSPs should carefully analyse their exposure to severe business disruptions and assess, ~~(~~quantitatively and qualitatively~~)~~, their potential impact, using internal and/or external data and scenario analysis. ~~The PSP should identify its critical functions, processes, systems, transactions and interdependencies to~~ On the basis of the identified and classified critical

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				functions, processes, systems, transactions and interdependencies in accordance with GL 3.1 to GL 3.3, PSPs should prioritise business continuity actions using a risk based approach, which can be based on the risk assessments carried out under GL 3. Depending on the business model of the PSP, this may ~~depending on the design of the PSP~~ for example facilitate the further processing of critical transactions ~~for example~~ while remediation efforts continue.'
[110]	GL-5.3 (a)	One respondent requested clarification of the difference between 'Important business activities' and 'ordinary business procedures'.	In the EBA's view, 'ordinary business procedures' must be understood as the normal way for the PSP to conduct its payment services. 'Important business activities' must be understood as the payment services themselves offered by the PSP. The EBA clarifies that, as the wording 'ordinary business procedures' is not essential to the understanding of the requirement, it has decided to delete it from the sentence. In addition, for greater consistency across the Guidelines, the term 'most important' has been replaced with 'critical'. The meaning of criticality is defined in GL 2 (now GL 3).	GL 5.3 (a) (now GL 6.3 (a)) has been amended and now reads: '~~PSPs~~ to ensure that it can react appropriately to emergencies and is able to maintain its ~~most important~~ critical business activities ~~if there is a disruption of its ordinary business procedures~~; and'
[111]	GL-5.3 (a)	One respondent was of the opinion that contingency measures need to be in place also in the event of severe business disruption.	In the EBA's view, GL 5.3 (a) (now GL 6.3 (a)) implicitly includes the notion of severe business disruptions. However, it was not the intention of the Guideline to limit the scope of contingency plans and BCPs to severe business disruptions. Such plans should be in place regardless of whether the business disruption is severe, important or low.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[112]	GL-5.3 (a)	One respondent requested clarification of the terms 'contingency plan', 'business continuity plan' and 'mitigation measures'.	The EBA points out that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. For the Guidelines to remain futureproof, the necessary flexibility of PSPs should not be restricted by definitions of terms that are generally understood on the market. Therefore, the EBA is of the opinion that introducing the proposed definitions would not be appropriate in line with the high-level requirements defined in these Guidelines, as these are common and well-known terms in the context of business continuity. In the EBA's view, these terms refer to the following concepts: - 'Contingency plan' describes the emergency reactions of the PSP in the event of emergency situations (which are defined by the PSP). 'Contingency plans' are part of BCPs. - 'BCPs' describe important business activities which have to be maintained and also set out processes aimed at preventing business disruptions. - 'Mitigation measures' are measures that are implemented in order to avoid, as far as possible, adverse effects on payment systems and on PSUs in the event of disruptions.	None.
[113]	GL-5.3 (a)	One respondent requested that contingency and business continuity plan requirements be explained further.	The EBA points out that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. For the Guidelines to remain futureproof, the necessary flexibility of PSPs should not be restricted by definitions of terms that are generally understood on the market.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			Therefore, the EBA is of the opinion that introducing the proposed definitions would not be appropriate in line with the high-level requirements defined in these Guidelines, as these are common and well-known terms in the context of business continuity.	
[114]	GL-5.3 (a)	One respondent suggested clarifying that recovery plans are required for all PSPs, including AISPs and PISPs.	The EBA would like to refer to the addressees of the Guidelines. AISPs and PISPs are also classified as PSPs under PSD2 and the business continuity plans are therefore required for all PSPs, in line with the above notion of the addressees of these Guidelines.	None.
[115]	GL-5.3 (a)	Several respondents requested that GL 5.3 (a), GL 5.4 and GL 5.5 be merged.	The EBA disagrees with this proposal, as in its view, GL 5.3 (a), GL 5.4 and GL 5.5 (now under GL 6) are linked, but should be clearly separated as each of these is a distinct requirement on the PSPs. GL 5.3 (a) (now GL 6.3 (a)) requires that the PSP puts in place contingency and business continuity plans, then GL 5.4 (now GL 6.4) builds on this requirement by requiring the PSP to consider a range of different but plausible scenarios. Then GL 5.5 (now GL 6.5) requires that based on these plausible scenarios identified under GL 5.4 (now GL 6.4), the PSPs should develop a set of response and recovery plans that in turn should meet certain requirements. Therefore, all these three Guidelines are necessary in order to put in place contingency and business continuity plans.	None.
[116]	GL-5.3 (a)	Several respondents requested that it be required that contingency plans and BCPs be reviewed and updated on a regular basis, at least once a year.	The EBA is of the view that business continuity planning should be incorporated into the overall risk management process, which needs to be reviewed at least once a year. The EBA suggests that the respondents refer to GL 1.1 (now GL 2.1) and GL 1.4 (now GL 2.4) in this respect. Annual review of the plans is an implicit requirement because testing and review of the test results is required to be carried out at least annually. Therefore, the EBA deems that no changes to the commented Guideline are necessary.	None.
[117]	GL-5.3 (b)	Several respondents requested clarification on whether the definition of 'termination of its payment services' refers to the disruption of payment services or to the termination of payment services for the PSP. Additionally, some respondents asked what is meant by 'termination of existing contracts'.	The EBA is of the view that mitigation measures have to be put in place for business disruptions which may result in the termination of payment services. Disruptions may also be caused by unplanned termination of existing contracts, which should be covered by a BCP or the contract itself. In the case of planned termination of contracts, the contract should specify appropriate transitional measures and may need to cater for the possibility of new providers. The BCP should therefore include measures to accommodate the unplanned/unwanted termination of payment services as well as for unplanned/unwanted termination of contracts by the PSP.	GL 5.3 (b) (now GL 6.3 (b)) has been amended and now reads: 'mitigation measures to be adopted by the PSP in the event of termination of its payment services and termination of existing contracts, to avoid adverse effects on

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary. However, the EBA changed the wording of this Guideline to improve clarity, as the previous wording was difficult to follow and could have been misunderstood.	payment systems and on ~~payments services users~~ PSUs and to ensure execution of pending payment transactions ~~and termination of existing contracts.~~'
[118]	GL-5.4	Several respondents requested clarification of 'extreme but plausible scenarios'. One respondent suggested removing GL 5.4, since it is not sufficiently clear how to interpret this requirement.	Extreme but plausible scenarios should be considered and mitigation solutions be defined to the extent possible. The EBA wants to clarify that it does not expect the main focus of the BCP be on these scenarios. The EBA agrees with the respondents that not every extreme scenario can be tested under real or similar to real circumstances (e.g. a tsunami). The EBA further clarifies that, in any case, it is not the scenario itself that needs to be tested, but whether or not mitigation solutions (e.g. switchover to a secondary data centre) work properly. For this, a high-level simulation of the scenario should be considered (e.g. simulation of flooding of a data centre by a tsunami, leading to shut-down of the data centre). Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary. Nevertheless, the EBA introduced an amendment to improve the clarity of this Guideline.	GL 5.4 (now GL 6.4) has been amended and now reads: 'The PSP should consider a range of different ~~extreme but plausible~~ scenarios, including extreme but plausible ones, to which it might be exposed, and assess the potential impact such scenarios might have on the PSP.'
[119]	GL-5.4	One respondent suggested that the following four impact types would cover all possible scenarios requiring business continuity planning: (i) loss of primary office facility; (ii) significant staff unavailability; (iii) loss of vendor; and (iv) loss of business applications. The respondent suggested clarifying the Guidelines as appropriate.	The EBA is of the opinion that the four impact types will certainly cover the majority of all possible scenarios, but they are not exhaustive; It is up to each PSP to define its own scenarios in line with the principle of proportionality set out in GL 1.1. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.
[120]	GL-5.4	One respondent asked whether the Guideline is specific to payment services or is to apply to all critical services within the organisation.	To address this concern, the EBA would like to refer to the scope which is only limited to the provision of payment services, as well as to GL 5.1 (now GL 6.1). The EBA clarifies that the business continuity plan should be established by the PSP to maximise its ability to provide payment services on an on-going basis and to limit losses in the event of severe business disruption. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[121]	GL-5.5	Several respondents requested that, in the event of termination of operations, PSPs should ensure that all data are permanently erased once the applicable legal retention period has expired.	In the EBA's view, data protection issues are out of the scope of GL 5 (now GL 6), on business continuity planning. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary. However, the Guideline implicitly expects that PSPs define all necessary measures to comply with other regulations or laws, without explicitly mentioning these.	None.
[122]	GL-5.5	Several respondents were of the opinion that business continuity planning should be required regardless of the size, business model and complexity of activities.	The EBA agrees with the respondents but considers these aspects to be already covered in the Guidelines. Considering these aspects when developing BCPs should not result in different security levels. This constraint should simply clarify that security measures can differ in scale. However, the EBA understands and agrees that the wording in the Guideline could be misinterpreted and therefore it has been decided to be removed.	GL 5.5 (now GL 6.5) has been amended and now reads: 'Based on the analysis carried out under Guideline ~~5.1~~ 6.2 and plausible scenarios identified under GL ~~5.4~~ 6.4, the PSP should, ~~where appropriate for the size, business model and complexity of their activities,~~ develop ~~a set of~~ response and recovery plans, which […]'
[123]	GL-5.5	Several respondents raised a concern about the requirement for a 'set of' response and recovery plans. They suggested to be neutral and to mention the requirement of only 'a response and recovery plan' or 'a set of recovery plans appropriate for the size, business model and complexity …'	In the EBA's view 'a set of' does not imply multiple documents or impose any other requirement. However, it should be understood to mean that it is necessary to define one response and recovery plan for each scenario identified, which can be summarised under one common document. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.
[124]	GL-5.5	One respondent requested clarification of the circumstances in which a business continuity management analysis should be carried out: 1) severe 'business disruption' as a result of an extreme but plausible scenario or 2) severe 'business disruption' regardless of the cause.	In the EBA's view, a BCP has to be defined and to cater for any kind of disruption. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[125]	GL-5.5 (b)	Several respondents suggested removing the phrase 'physically separated' because this is an extremely tight requirement which leaves no room for any other equally safe solution.	The EBA agrees with the respondents. In the EBA's view, the crucial factor is that the documentation should be readily available in the event of an emergency. How this is achieved can be defined by the PSP. The EBA remarks that the principle of proportionality set out in GL 1.1 applies throughout the Guidelines, including to this requirement, and should be considered in defining the steps necessary to comply therewith. Nevertheless, the EBA amended the text of the Guideline to improve its clarity.	GL 5.5 (b) (now GL 6.5 (b)) has been amended and now reads: 'be ~~clearly~~ documented and made ~~. The documentation should be~~ available ~~within~~ to the business and support units and ~~stored on systems that are physically separated and~~ readily accessible in case of emergency; and'.
[126]	GL-5.6	Several respondents were of the opinion that annual testing of the BCP is too prescriptive. One proposition was to amend the Guideline by further differentiating systems into classes of criticality with varying test cycles, for example yearly in the case of highly critical systems, every three years in the case of systems of medium criticality and ever five years in the case of systems deemed to be of low criticality.	The EBA disagrees with the respondents. The EBA is of the opinion that BCPs need to be tested regularly, otherwise it cannot be ensured that the plans will work properly if the scenarios become real. The EBA remarks that the principle of proportionality set out in GL 1.1 applies throughout the Guidelines, including to this requirement and should be considered when defining the test cases. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.
[127]	GL-5.7	One respondent was of the opinion that plans should also be updated in the event of any changes in systems and processes.	The EBA points out that the list presented in GL 5.7 (now GL 6.7) is not intended to be exhaustive. However, the EBA agrees with the respondent that this issue is an important point and added a clarification to the Guideline.	GL 5.7 (now GL 6.7) has been amended and now reads: 'Plans should be ~~regularly~~ updated at least annually based on testing results, current threat intelligence, information-sharing and lessons learned from previous events, and changing recovery objectives, as well as analysis of operationally and technically plausible scenarios that have not

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				yet occurred, and, if relevant, after changes in systems and processes. PSPs should consult and coordinate with relevant internal and external stakeholders during the establishment of their BCPs.'
[128]	GL-5.7	Several respondents suggested replacing 'regularly' by 'at least annually' for consistency with GL 5.6.	The EBA is of the opinion that business continuity planning should be incorporated into the overall risk management process and that this needs to be reviewed on an on-going basis. The EBA also suggests that the respondents refer to GL 2.4. In the EBA's view, annual review of the BCP is implicit because testing and review of the test results is required to be carried out at least annually. To clarify this, the EBA has changed the wording in the Guideline.	GL 5.7 (now GL 6.7) has been amended and now reads: 'Plans should be ~~regularly~~ updated at least annually based on testing results, current threat intelligence, information-sharing and lessons learned from previous events, and changing recovery objectives, as well as analysis of operationally and technically plausible scenarios that have not yet occurred, and, if relevant, after changes in systems and processes. PSPs should consult and coordinate with relevant internal and external stakeholders during the establishment of their BCPs.'
[129]	GL-5.7	One respondent requested that PSPs be required to consult only competent stakeholders because of the confidentiality of specific information. This respondent also proposed the addition of 'supervisory and other competent authorities' to the list of stakeholders to be consulted about the BCP.	The EBA partly agrees with the respondent. Sometimes it might be vital for PSPs to coordinate their own BCPs with those of critical stakeholders, which the PSP has to define. PSPs might consider these to include only 'competent' ones. Therefore, in this context, the EBA cannot provide a unique definition for 'competent'. Moreover, the Guideline does not oblige PSPs to share confidential information with identified relevant	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			stakeholders if this is not deemed required by the PSP. If confidential information needs to be shared with other stakeholders, the EBA expects PSPs to have in place appropriate confidentiality agreements with these stakeholders. Furthermore, if PSPs need to consult supervisory or other authorities about their BCPs, apart from possible other legal obligations, they are free to do so, but there is no such obligation under these Guidelines. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	
[130]	GL-5.8 (a)	Several respondents requested that the phrase 'an adequate set of scenarios …' be used instead of 'a broad range of scenarios …'.	The EBA agrees with the comment and has amended the Guideline by removing text already included in GL 6.4 and providing a reference thereto instead.	GL 5.8 (a) (now GL 6.8 (a)) has been amended and now reads: 'include ~~a broad range~~ an adequate set of scenarios, as referred to in GL 6.4, ~~including simulation of extreme but plausible ones~~;'
[131]	GL-5.8 (a)	One respondent criticised the requirement to focus the BCP on extreme but plausible scenarios rather than on scenarios or events that pose real danger to the continuity of services provided.	The EBA does not agree that the Guideline places a focus on extreme but plausible scenarios. These scenarios should be considered merely as a subset of relevant scenarios, and mitigation solutions should be defined to the extent possible. The EBA agrees that not every extreme scenario can be tested under real or similar to real circumstances (e.g. a tsunami). It is the EBA's view that, in any case, it is not the scenario itself that needs to be tested but whether or not the mitigation solutions (e.g. switchover to a secondary data centre) work properly. To achieve the above objective, the EBA deems it necessary to consider a high-level simulation of the scenario (e.g. simulation of flooding of a data centre by a tsunami, leading to shutdown of the data centre). Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.
[132]	GL-5.8.c	One respondent requested clarification of the term 'unfamiliar scenarios'.	The EBA agrees with the respondent that the term 'unfamiliar' could be misinterpreted. The Guidelines meant the scenarios that are tested and are defined under GL 5.4 (now GL 6.4) and GL 5.8 (a) (now GL 6.8 (a)). However, the Guideline has been amended accordingly to reflect the concern of the respondent.	GL 5.8 (c), (now GL 6.8 (c)) has been amended and now reads: 'include procedures to verify the ability of its staff and processes to respond adequately to ~~unfamiliar~~ the scenarios above.'

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[133]	GL-5.9	One respondent suggested merging GL 5.9 with GL 5.8, because monitoring is part of the three phases of the BCP (i.e. design, implementation and effectiveness).	The EBA clarifies that GL 5.8 (now GL 6.8) refers to testing whereas GL 5.9 (now GL 6.9) sets requirements for monitoring. The EBA is of the view that these issues should be differentiated in the context of the Guidelines even though they might be interdependent, as both issues are deemed sufficiently important to be considered as separate requirements. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.
[134]	GL-5.10	One respondent was of the opinion that 'Incident management' should be treated as a distinct Guideline.	The EBA is of the view that it is not necessary for incident management to be explicitly included the BCP, as long are there are references to it. The EBA further clarifies that the intention of GL 5.10 (now GL 6.10) is to define an adequate communication process during a crisis. Incident management processes usually include communication procedures that can be used as a basis for further crisis communication. However, in order to avoid any misinterpretations in the context of GL 5.10 (now GL 6.10) the term 'Incident management' has been removed. General requirements on incident management are described under GL 4 (now GL 5).	The sub-heading over GL 5.10 (now GL 6.10) has been amended and now reads: ~~'Incident management and~~ cCrisis communication' GL 5.10 (now GL 6.10) has been amended and reads: 'In the event of a disruption or emergency, and during the implementation of the business continuity plans, ~~the~~ PSPs should ensure ~~it has~~ they have effective ~~incident management and~~ crisis communication measures in place so that all relevant internal and external stakeholders, including external service providers, are informed in a timely and appropriate manner. '
[135]	GL-5.10	One respondent requested clarification about '… informed in a timely and appropriate manner'.	The EBA clarifies that it is up to the PSP to define in its BCP the way in which, and how quickly, it will inform its various stakeholders, in accordance with the proportionality principle set out in GL 1.1. This may depend on the individual stakeholder and cannot be predefined by the	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			EBA. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	
Feedback on responses to Question 7				
[136]	GL 6 general response	Some respondents disagreed with the testing Guideline: most commonly, the responses mentioned that testing is not part of the mandate according to Article 95 of PSD2.	The EBA does not agree with the statement that testing is out of the scope of the mandate given by Article 95. Article 95 states that a PSP should have appropriate mitigation measures and control mechanisms to manage operational and security risks. Testing is important to ensure that the mitigation measures defined by a PSP are appropriate. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.
[137]	GL 6.1	One respondent mentioned the organisational requirements should not go beyond the PSP.	The EBA does not agree with the statement that testing is out of the scope of the mandate given by Article 95. Article 95 states a PSP should have in place appropriate mitigation measures and control mechanisms to manage operational and security risks. If organisational arrangements are necessary to ensure the efficiency and robustness of the mitigation measures and control mechanisms, then they need to be implemented to ensure compliance with the Guidelines. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.
[138]	GL 6.2	One respondent suggested replacing 'procedures' by 'processes'.	In consideration of the comment the EBA agrees to add reference to processes instead of replacing procedures by processes in the commented Guideline. The EBA is of the view that these two terms do not have the same meaning.	GL 6.2 (now GL 7.2) has been amended and now reads: '~~The PSP~~ PSPs should ensure that tests are conducted ~~to assess the robustness and effectiveness of the security measures~~ in the event of changes to the infrastructure, the processes or ~~and~~ procedures, and if changes ~~resulting from~~ are made as a consequence of major operational or security incidents.'.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[139]	GL 6.3	Several respondents stated that it would be difficult/almost impossible to adequately test the devices/terminals described as they are not under direct control of the PSP. The suggestion was to rely on the work performed as part of the independent security certification process of these devices.	The EBA agrees that it would be difficult to adequately test the security of payment devices and software used for the provision of payment services, the authentication of the PSU or the generation/receipt of authentication codes as most of these devices will be manufactured by other companies and these are 'black boxes' for the PSP. Although such devices might pass independent security certification processes at the vendor, such products should nevertheless be considered as 'standard products' which are purchased. It is important that the PSP has sufficient assurance of the security of the devices and terminals delivered by the manufacturer. It is the responsibility and task of the PSP to test all security measures before implementation and during operations. This includes the determination of the effectiveness of security measures in purchased products which are independently certified like devices, terminals, etc. How this should be done is up to the PSP, but the PSP should evidence the inclusion of such security measures relevant to externally sourced devices and software if requested.	None.
[140]	GL 6.3	One respondent suggested that the testing framework should also include security measures relevant to enrolment of PSUs and issuing PSUs with credentials.	The EBA is of the opinion that testing of security measures to enrolment of PSUs and issuing processes of PSUs credentials is implicitly included as part of the testing framework as the testing framework is related to all security measures and related processes and procedures of the payment services process. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.
[141]	GL 6.4	One respondent suggested that the testing should include hardware and software of the mentioned devices.	The EBA restates that all requirements relate to the scope of the Guidelines, which is limited to the provision of payment services. The EBA implicitly considers that testing requirements are related to the whole payment process including the hardware, software and infrastructure supporting this process. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.
[142]	GL 6.4	One respondent suggested that penetration testing should include technical and human testing.	In the EBA's understanding, vulnerability scans refer to the technical infrastructure. The EBA considers that penetration tests implicitly cover both the technical and social/human aspects. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.
[143]	GL 6.4	Two respondents suggested changing the order to clarify the relation between testing framework, security measures tests	The EBA points out that the list in GL 6.4 (now GL 7.4) is not meant to suggest a required order. The specific requirements indicate only the minimum required elements of the testing framework.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		and change management process (c → a, b → b and a → c) and also a suggestion for a text change of the old a) and new c).	Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	
[144]	GL 6.4	One respondent requested clarity on the frequency of vulnerability scanning. According to this respondent penetration testing could be risk based.	The EBA considers that vulnerability scanning and penetration testing are important elements to prove the effectiveness of the implemented security measures. However, the EBA points out that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This provides PSPs with also a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. The EBA is of the opinion that the high-level nature of the Guidelines means that they are unable to prescriptively define a minimum frequency of tests. In the EBA's opinion, this is already covered by the text of the requirement referring to the 'adequacy' of the tests to the level of risk identified. This should also imply adjusting the frequency of the tests in proportion to the identified risks. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.
[145]	GL 6.4	One respondent mentioned that the requirements of GL 6.3 are not in line with the agile method of development. The respondent proposed that the requirements should be less stringent. The respondent also mentioned that the overall Guideline is subject to the principle of proportionality. The respondent fears that larger PSPs will be made more accountable for security measures so suggested a risk-based approach.	In EBA's opinion the proportionality principle is sufficiently clear, as set out in GL 1.1 to provide adequate level of flexibility in compliance with the requirements of these Guidelines. The EBA does not share the opinion of the respondent that larger PSPs will be made more accountable. The EBA would like to highlight that a guiding principle of this Guideline is the risk-based approach. In line with the high-level character of these Guidelines, this Guideline does not prescribe the use of a particular testing system or method. The risk-based approach could also require a risk/impact analysis during the development phase, in line with the risk involved in the payments process. Therefore, the EBA deems that no changes to the substance of the commented Guideline are necessary.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[146]	GL 6.4	One respondent suggested that the testing framework should follow ISO/IEC 18045.	The EBA is of the view that no industry standards must be implemented to achieve compliance with the requirements set therein, since in the EBA's view this would go against the PSD2 objectives of ensuring technology and business model neutrality.	None.
[147]	GL 6.4	One respondent questioned the need for independent testers when staff numbers are limited. The respondent further indicated that it may sometimes make sense for testers to be involved in implementing appropriate mitigations to the weaknesses they have detected, in order to minimise the number of people who may be aware of such weaknesses.	As mentioned in the commented Guideline, testers must be independent of the developers. The EBA is of the opinion that developers should never perform any testing, to avoid risks and non-effective security measures. The EBA therefore does not agree that implementation of the suggested changes would be appropriate in view of the underlying risks.	None.
[148]	GL 6.4	One respondent mentioned that it should be clarified that, generally, PSP staff o are not excluded from carrying out testing as long as they not involved in the development of the security measures for the corresponding payment services. The respondent proposed that the Guideline be amended as follows: 'are carried out by independent testers who can be part of the own staff but are not involved in the development of the security measures for the corresponding payment services or systems that are to be tested, at least for final tests before putting security measures into operation, and'.	The EBA clarifies that it is not its intention to require a PSP to hire external staff to perform the testing. The requirements for testers that are mentioned in the Guideline specify only that developers of the security measures may not be involved in the testing. Furthermore, the testers are required to have sufficient knowledge, skills and expertise to be able to perform the tests. Therefore, for instance, in many situations penetration tests may be performed by external staff, but following the above conditions. Nevertheless, the EBA has amended the Guideline and included the specific requirements to be met by the testers.	GL 6.4 (b) (now GL 7.4 (b)) has been amended and now reads: 'are carried out by independent testers who ~~are not involved in the development of the~~ have sufficient knowledge, skills and expertise in testing security measures ~~for the corresponding~~ of payment services and are not involved in the development of the security measures for the corresponding payment services or systems that are to be tested, at least for final tests before putting security measures into operation; and'
[149]	GL 6.4	Another respondent suggested amending GL 6.4 (b) as follows: 'The testing framework should ensure that tests: […] b) are carried out by independent testers, i.e. that are not involved in the development of the security measures for the corresponding	The EBA appreciates and agrees with this comment, and consequently redrafted the Guideline to include the specific requirements to be met by the testers.	GL 6.4 (b) (now GL 7.4 (b)) has been amended and now reads: 'are carried out by independent testers who

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		payment services or systems that are to be tested, at least for final tests before putting security measures into operation.'		~~are not involved in the development of the~~ have sufficient knowledge, skills and expertise in testing security measures ~~for the corresponding~~ of payment services and are not involved in the development of the security measures for the corresponding payment services or systems that are to be tested, at least for final tests before putting security measures into operation; and'
[150]	GL 6.5	Several respondents mentioned the absence of a requirement to test periodically the non-critical systems also, as they too may pose a security risk, especially as the PSP can decide on their classification of criticality.	The EBA agrees with this comment. In the EBA's view, non-critical systems should also be tested on a regular basis. Depending on the results of a risk analysis these non-critical systems should be tested regularly and at least every three years. Therefore, the EBA has redrafted the commented Guideline accordingly.	GL 6.5 (now GL 7.5) has been amended and reads: 'PSPs should perform on-going and repeated tests of the security measures for ~~its~~ their payment services. For ~~critical~~ systems that are critical for the provision of their payment services (as described in ~~GL 2.2~~ GL 3.2), 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.'
[151]	GL 6.5	One respondent suggested amending the text in GL 6.5 as follows: '… these tests shall be performed on a regular basis based on the security policy and business continuity plan.'	The EBA recognises the importance of the requirement to have a security policy and a BCP, but does not agree with the comments that the regularity of testing should be based on these policies. Testing frequency should depend on risks and changes performed and should be sufficient to ensure the effectiveness of the security measures. The requirement for	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			regular testing (at least once a year in the case of critical systems) could be embedded in the security policy or BCP of a PSP, but the possibility of this being embedded in the security policy is an option and should not be a requirement. It is the responsibility of the PSP to ensure the testing frequency as per the guidelines. The EBA does not therefore agree that implementation of the suggested changes would be appropriate.	
[152]	GL 6.5	One respondent mentioned that the testing of critical applications should therefore be structured in compliance with the principle of proportionality.	The EBA remarks that the principle of proportionality set out in GL 1.1 applies throughout the Guidelines, including in this requirement, and should be considered in defining the steps necessary to comply therewith. Therefore, the EBA does not see any need to change this Guideline.	None.
[153]	GL 6.5	One respondent suggested incorporating GL 6.5 into GL 6.4 as the way in which GL 6.5 is drafted makes it seem that testing should be performed only as part of the change management process, rather than being performed on a regular basis.	The EBA does not support the conclusion of the respondent that testing should be performed only as part of the change management process. The EBA is of the view that because of the constant development of new threats, regardless of changes, the effectiveness of security measures should be tested at least once a year in the case of all critical systems and based on a risk analyses, but at least every three years, in the case of non-critical systems. These requirements were further specified in the redrafting of GL 6.5 (now GL 7.5).	GL 6.5 (now GL 7.5) has been amended and now reads: 'PSPs should perform on-going and repeated tests of the security measures for ~~its~~ their payment services. For ~~critical~~ systems that are critical for the provision of their payment services (as described in ~~GL 2.2~~ GL 3.2), 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.'
[154]	GL 6.5	Several respondents stated that the difference between a penetration test (see GL 6.4 (c)) and the required 'on-going and repeated tests of security measures' is not clear.	The EBA clarifies that in its opinion penetration testing is different from on-going and repeated tests of security measures. One major difference is that penetration tests are performed on the production processes while testing should for instance also be performed in a non-production environment.	None.
[155]	GL 6.6	Several respondents mentioned the lack of a deadline based on criticality by which to update the security measures based on the results of the tests conducted.	The EBA agrees with the response and has amended the Guideline accordingly. However, the EBA points out that it is difficult to include hard	GL 6.6 (now GL 7.6) has been amended and now reads:

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			deadlines in the Guideline as the time needed to implement security measures may vary among different PSPs.	'PSPs should monitor and evaluate the results of the tests conducted, and update ~~its~~ their security measures accordingly and without undue delay in the case critical systems.
Feedback on responses to Question 8				
[156]	GL-7	The majority of respondents welcomed the implementation of proposed information sharing, and training and awareness measures. However, some respondents were concerned that the scope of the Guidelines goes beyond the mandate of PSD2 Article 95 and suggested deletion of GL 7.	The EBA does not agree with the opinion that such security measures as training and awareness and monitoring of emerging risks and technologies go beyond the mandate of Article 95. However, to improve the clarity of the commented Guideline, the EBA decided to redraft this Guideline, decreasing the number of specific requirements. The EBA also clarifies that it has decided to remove the requirement on information sharing from GL 7 (now GL 8) as the practical implementation from the PSPs' side could be difficult and it would be challenging for CAs to consistently supervise this requirement. The EBA considers that such a requirement would not be proportional to the purpose of achieving broader awareness of payment fraud and security issues related to the provision of payment services. The EBA would nevertheless encourage all PSPs to participate in any platforms enabling the exchange of information on operational and security risks and threat intelligence with other PSPs and relevant third parties such as operators of payment systems, industry associations, etc., as long as these initiatives comply with applicable EU law, such as Directive (EU) 2015/2366 and Regulation (EU) 2016/679 or, if applicable, Regulation (EC) 45/2001, and neither favour nor disadvantage any particular type of provider over others.	GL 7.1 (now GL 8.1) has been redrafted and now reads: 'PSPs should establish and implement processes and organisational structures to identify and constantly monitor security and operational threats that could materially affect their ability to provide payment services. ~~This should include, but is not limited to:~~ ~~a) sharing information with third parties and PSPs to achieve broader awareness of payment fraud and cybersecurity issues;~~ ~~b) participating in information sharing arrangements with external stakeholders within and outside the payment industry;~~ ~~c) distilling key lessons from security incidents that have been identified~~

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				~~or have occurred within and/or outside the organisation, and updating the security measures accordingly~~. Additionally, based on point c) of the former GL 7.1, an additional GL 8.2 has been added and reads: 'PSPs should analyse operational or security incidents that have been identified or have occurred within and/or outside the organisation. PSPs should consider key lessons learned from these analyses and update the security measures accordingly.'
[157]	GL-7.1	Several respondents stated that information sharing in a cross-country dimension should not be mandatory.	The EBA clarifies that it has decided to remove the requirement on information sharing from GL 7 (now GL 8) as the practical implementation from the PSPs' side could be difficult and it would be challenging for CAs to consistently supervise this requirement. The EBA considers that such a requirement would not be proportional to the purpose of achieving broader awareness of payment fraud and security issues related to the provision of payment services. The EBA would nevertheless encourage all PSPs to participate in any platforms enabling the exchange of information on operational and security risks and threat intelligence with other PSPs and relevant third parties such as operators of payment systems, industry associations, etc., as long as these initiatives comply with applicable EU law, such as Directive (EU) 2015/2366 and Regulation (EU) 2016/679 or, if applicable, Regulation (EC) 45/2001, and neither favour nor disadvantage any particular type of provider over others.	See amendment ref. no. [156].
[158]	GL-7.1	Some respondents raised concerns that information sharing mentioned is only one way – from PSP to CA – but the other way is not explicitly stated. In addition, some expressed the view that	The EBA clarifies that it has decided to remove the requirement on information sharing from GL 7 (now GL 8) as the practical implementation from the PSPs' side could be difficult and it would be challenging for CAs to consistently supervise this requirement. The EBA considers that such a requirement would not be proportional to the purpose of achieving	See amendment ref. no. [156].

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		analysis based on the information collected is beneficial to the industry.	broader awareness of payment fraud and security issues related to the provision of payment services. The EBA would nevertheless encourage all PSPs to participate in any platforms enabling the exchange of information on operational and security risks and threat intelligence with other PSPs and relevant third parties such as operators of payment systems, industry associations, etc., as long as these initiatives comply with applicable EU law, such as Directive (EU) 2015/2366 and Regulation (EU) 2016/679 or, if applicable, Regulation (EC) 45/2001, and neither favour nor disadvantage any particular type of provider over others.	
[159]	GL-7.1	The majority of respondents suggested that EBA or CAs should be responsible for the establishment of a centralised body enabling firms to share information. In addition, the majority of respondents were concerned about sharing information with third parties, or outside the payment industry. A large number of respondents requested more clarity on information sharing in terms of what information should be shared, with whom and how. Some respondents were also concerned that sharing information would not be compliant with the GDPR (for example, sharing IP addresses).	Based on several comments received requesting clarifications with regard to sharing of the information on security and operational risks and reservations raised by the respondents over the issues of confidentiality and competition, the EBA has decided to remove the requirement on information sharing as the practical implementation from the PSPs' side could be difficult and it would be challenging for CAs to consistently supervise this requirement. The EBA considers that such a requirement would not be proportional to the purpose of achieving broader awareness of payment fraud and security issues related to the provision of payment services. The EBA would nevertheless encourage all PSPs to participate in any platforms enabling the exchange of information on operational and security risks and threat intelligence with other PSPs and relevant third parties such as operators of payment systems, industry associations, etc., as long as these initiatives comply with applicable EU law, such as Directive (EU) 2015/2366 and Regulation (EU) 2016/679 or, if applicable, Regulation (EC) 45/2001, and neither favour nor disadvantage any particular type of provider over others.	None.
[160]	GL-7.2	One respondent requested more clarity on whether 'developments' means general technological advancements or developments to proprietary payment systems.	In the EBA's opinion, GL 7.2 (now GL 8.3) refers to general security and technology developments related to operational and security risks in the payments industry.	None.
[161]	GL-7.2	One respondent suggested that, in terms of monitoring technology developments, PSPs should rely on the work performed centrally by the EBA or the CAs rather than doing this themselves, which may lead to inconsistency and gaps in the understanding of these developments by individual PSPs.	The EBA would like to clarify that GL 7.2 (now GL 8.3) refers to the responsibility of the PSPs to make efforts to monitor emerging risks and trends in the industry. Even if this type of information were to be provided not centrally by the EBA/CAs, but via dedicated information exchange platforms, this does not mean that PSPs should not consider this information in their monitoring of emerging risks.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[162]	GL-7.3	Some respondents suggested that more details be provided on the required frequency of the training and awareness (at least annually), on the scope of the delivery, and on the control mechanisms to ensure that training and awareness are effective.	The EBA accepts this comment that the frequency of the training and awareness should be specified in the Guidelines. Therefore, the EBA has amended the Guideline accordingly.	GL 7.3 (now GL 8.4) has been amended and now reads: 'PSPs should establish a training programme for all staff to ensure that ~~all their personnel are~~ they are trained to perform their duties ~~related to the provision of payment services~~ and responsibilities consistent with the relevant security policies and procedures in order to reduce human error, theft, fraud, misuse or loss. PSPs should ensure that the training programme provides for training staff members at least annually, and more frequently if required.'
[163]	GL-7.3	Some respondents were concerned about the practicality of delivery of training to third parties, as well as how to control this particular requirement.	The EBA clarifies that GL 7 (now GL 8) does not require PSPs to provide training to third parties. The Guidelines do not apply to outsourced functions as the training of employees of outsourced companies is the responsibility of the PSPs.	None.
[164]	GL-7.4	One respondent expressed concerns about identifying 'critical personnel' and suggested that due to certain regulatory restrictions they believe that a better term would be 'critical technical groups'	Following other comments referring to GL 2.1 (now GL 3.1), the EBA replaced the confusing reference to 'critical personnel' with the term 'key roles' and also amended the commented Guideline accordingly.	GL 7.4 (now GL 8.5) has been amended and now reads: 'PSPs should ensure that ~~critical personnel~~ key roles identified under ~~GL~~ GL 2 3.1 receive targeted information security training on annual basis or more frequently if required.'

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[165]	GL-7.5	Some respondents suggested that more details be provided on the frequency of security awareness training (at least annually), the scope of the delivery and on control mechanisms to ensure that training and awareness are effective.	EBA accepts this comment and agrees that training and awareness should be performed on a regular basis.	GL 7.5 (now GL 8.6) has been amended and now reads: 'PSPs should establish and implement periodic security awareness programmes in order to educate their personnel and to address information security related risks. ~~to the provision of payment services.~~ These programmes should require PSP personnel to report any unusual activity and incidents.
Feedback on responses to Question 9				
[166]	GL-8 in general	Several respondents commented that it should be made clear which guidelines apply to all PSPs and which specifically to ASPSPs, AISPs and PISPs. The reasons for this are (1) the information provided by each party to the PSU could be controversial; and (2) the requirements of GL 8.1, 8.2 and 8.3 are directed to all PSPs and, thus, the term PSP would be appropriate here. However, clauses 8.4, 8.5 and 8.6 apply only to ASPSPs. Establishing or disabling specific payment functionalities should be initiated and processed only by ASPSPs.	The EBA is of the view 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 GL 1.1, which means 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. In particular, for the business model and technological neutrality reasons stated above, the EBA does not agree that it is appropriate to limit to ASPSPs the requirement to offer the option to disable specific payment functionalities.	None.
[167]	GL-8 in general	Several respondents commented that the Guidelines should differentiate between consumer and corporate PSUs (i.e. between commercial and private customers) , although there may be room for assumptions on differences in the risk awareness of these two ideal groupings.	The EBA does not agree that it is feasible to differentiate between corporate and consumer PSUs in the Guidelines. It would be contrary to the EBA's mandate to develop these Guidelines, set out by PSD2, which does not differentiate between consumers and non-consumers as PSUs. The EBA recalls, however, that compliance with the Guidelines is subject to the principle of proportionality, set out in GL 1.1, which states that the	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			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.	
[168]	GL-8 in general	Several respondents commented that there is a need to make the relationship between TPPs and ASPSPs transparent to PSUs. The PSU should always be aware that the TPP is not acting on behalf of the ASPSP, and TPPs should make this clear in their communications with PSUs. GL 8 should require TPPs to clearly articulate to PSUs whether or not they are acting on behalf of the ASPSP.	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 'Rationale' section of the Guidelines.	An additional sentence to paragraph 37 of Section 2.2, Rationale, has been added and reads: '[…] In this context, the EBA stresses the importance of ensuring transparency, such that PSUs are always aware as to which PSP is responsible for providing them with the payment service.'
[169]	GL-8 in general	One respondent commented that some of the requirements detailed in this Guideline will introduce significant changes to the interaction of PSPs with PSUs while delivering marginal security benefits.	The EBA is of the opinion that most of the issues of GL 8 (now GL 9) already apply to PSPs as they already have to comply with the EBA Guidelines on the security of internet payments. Thus, the EBA does not regard the current requirements significantly more burdensome for the PSPs. Furthermore, the EBA is of the opinion that these Guidelines are needed to address the security risks identified in the drafting process.	None.
[170]	GL-8 in general	Several respondents commented that the Guidelines should generally not go beyond what is explicitly mandated by Article 95(3) of PSD2 and, therefore, suggested deleting 'Guideline 8: PSU relationship management'. This particularly holds true for information requirements that are already addressed conclusively in Article 52. The communication and reporting obligations as drafted in the Guidelines are too general and too broad and could cause information overload and phishing attacks against the PSUs. Requirements to allow for disabling of specific payment functionalities or requirement to allow for options to reduce payment limits are not included in the EBA mandate – Article 95(3) of PSD2.	The EBA points out that GL 8 (now GL 9) provides requirements on PSU awareness on security risks, PSU secure communication and reporting procedures. For this reason the EBA is of the opinion that it can be regarded as part of security measures, for which EBA is mandated to issue guidelines, as stated in Article 95(3) of PSD2. However, in recognition of the comment, the EBA has reviewed the commented Guidelines, added references to PSD2 and deleted some requirements that repeated requirements directly included in PSD2.	GL 8.3, GL 8.7 and GL 8.10 have been deleted.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[171]	GL-8 in general	One respondent commented that user education on security risks linked to payment services as referred to in GL 8 should not be the sole task of the market. Stipulating a national obligation (e.g. for CAs) in that regard is necessary, as cultural differences are quite striking, even within the EU, when it comes to the extent to which new online banking and payment services are used by consumers.	The EBA is of the view that CAs can provide some general information regarding the security of payments to the PSUs, for example by organising awareness campaigns targeting the general public. However, the EBA is of the view that such general awareness campaigns are insufficient and cannot replace information provided to PSUs by individual PSPs regarding secure use of the services they provide, required under the commented Guideline.	None.
[172]	GL-8 in general	One respondent commented that GL 8 mainly covers user protection which is originally not the topic of these Guidelines on operational and security risks. Therefore, the respondent suggested that this Guideline should be removed from these Guidelines.	The EBA is of the opinion that PSU protection and awareness can be regarded as part of security measures for operational and security risks relating to payment services, for which the EBA is mandated to issue Guidelines, as stated in Article 95(3) of PSD2. However, in recognition of the comment, the EBA has reviewed the commented Guidelines, added references to PSD2 and deleted some requirements that repeated requirements directly included in PSD2.	GL 8.3, GL 8.7 and GL 8.10 have been deleted.
[173]	GL-8 in general	One respondent commented that it is important that PSUs understand what they can do to stay secure. Effective 'consumer education' can be delivered through different channels, on different occasions and by different types of organisation, and there is no 'one size fits all' approach. Industry can best deliver effective communications by working together and with other participants, media, governments, organisations and authorities.	The EBA agrees that the Guidelines should not provide a 'one size fits all' approach. This is also reflected via the introduction of the proportionality principle in GL 1.1, according to which 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.	None.
[174]	GL-8 in general	One respondent commented that disabling specific payment functionalities and reducing payment limits upon PSU request should not be mandatory for all payment instruments but should be appropriate based on the actual risk of the programme and payment instrument.	The EBA does not agree with the comment. The Guidelines do not mandate the PSP to disable all payment instruments. In particular, GL 8.4 (now GL 9.3) only requires the PSP to allow the PSUs to disable specific payment functionalities. Nevertheless, Guideline 8 (now Guideline 9) has been redrafted to improve its clarity following several comments received.	GL 8.4 (now GL 9.3) has been amended and now reads: '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.'
[175]	GL-8 in general	One respondent asked how the rules in GL 8, on PSU relationship management, relate to the articles in the EBA RTS on strong	In the EBA's view there are no discrepancies or overlapping issues between the RTS on SCA and CSC and this Guideline. While drafting these Guidelines on security measures for operational and security risks, the EBA considered to the extent possible the requirements stemming from	GL 8.3, GL 8.7 and GL 8.10 have been deleted.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		customer authentication and secure communication (RTS on SCA and CSC).	other regulations and the requirements in these Guidelines are related only to the management of the operational and security risks. The EBA clarifies that there are material differences in the addressees, objectives and scope of different regulatory requirements with regard to cyber and operational risks. The scope of the RTS on SCA and CSC is limited to strong customer authentication and secure communication requirements whereas these Guidelines cover security measures more broadly. The EBA would like to confirm that following the revisions made in response to the comments received in the public consultation process, it has carefully reviewed the commented Guidelines, added references to PSD2 and deleted some requirements that were repeating requirements directly included in PSD2 or in the RTS on SCA and CSC. The EBA is of the opinion that there is no longer any duplication of or overlap between the content these Guidelines and the requirements of the RTS on SCA and CSC.	
[176]	GL-8 in general	One respondent commented that GL 8.4 to GL 8.6 set requirements on payment functionality rather than on the handling of awareness on security risks and could possibly stand in conflict. Another respondent requested that GL 8.4 and GL 8.6 be reviewed to make them more high-level.	The EBA clarifies that GL 8.4 to GL 8.6 (now GL 9.5 to GL 9.7) are related to PSU payments security. In view of this comment and other comments received on GL 8, GL 8 (now GL 9) has been redrafted and the sub-heading has also been amended accordingly.	The sub-heading for GL 8 (now GL 9) has been amended and now reads: 'Payment service user awareness on security risks and risk-mitigating actions' Additionally, GL 8.3, GL 8.7 and GL 8.10 have been deleted. Please also see the following amendments: – ref. no. [174] regarding GL 8.4 (now GL 9.3); – ref. no. [199] regarding GL 8.5 (now GL 9.4); and – ref. no. [203] regarding GL 8.6 (now GL 9.5)
[177]	GL-8 in general	One respondent commented that the EBA should consider the fact that a number of other respondents have suggested giving	The EBA acknowledges that PSPs will require time to implement the Guidelines. However, according to Article 5(1) of PSD2, the subset of legal entities that seek authorisation as payment or electronic money institutions are required to take these Guidelines into account when	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		the PSPs more time to implement security measures to comply with this Guideline.	applying for authorisation as of 13 January 2018, which is why the application date of the Guidelines cannot be delayed beyond that date. That said, the EBA acknowledges that PSPs will require time to implement the Guidelines and are therefore not expected to comply with the Guidelines until the EBA has published the translations of the Guidelines in all official EU languages, issued the compliance table, and the CAs have implemented the Guidelines into their national regulatory or supervisory frameworks.	
[178]	GL-8 in general	Some respondents were of the view that GL 8 (on PSU relationship management) is probably only partially applicable to acquiring services and therefore it would be better to specify which requirements apply and which not.	The EBA points out that all requirements in the Guidelines should be applicable to all PSPs, with due regard to the services they provide and, hence, their business functions. If it is not feasible for a PSP to implement a particular requirement in the Guidelines because it relates to a function which that PSP does not provide, such requirement can be considered as not applicable to that PSP. The EBA would also like to remind respondents that proportionality principle set out in GL 1.1 should also be applied. In relation to the particular comment, the EBA would like to point out that the users of acquirers are the merchants, towards whom the acquiring PSPs have responsibilities.	None.
[179]	GL-8 in general	Some respondents were of the opinion that the majority of the Guidelines are aligned with accepted information security standards with the exception of GL 8 – on PSU relationship management – which they also believe goes beyond the mandate given under Article 95 of PSD2. In particular, with regard to the information to be provided to PSUs under this Guideline, some respondents indicated that they do not expect to update PSUs on all such changes/emerging risks. Communication of such detailed information to PSUs could cause problems, damage confidence and provide malicious actors with information that would assist them. Furthermore, some respondents believe that some of the requirements included in GL 8 apply to only some PSPs (e.g. in some cases to AISPs, other cases to ASPSPs, etc.) and this should be reflected in the Guidelines.	The EBA is of the opinion that PSU protection and awareness can be regarded as part of security measures for operational and security risks relating to payment services, for which the EBA is mandated to issue Guidelines, as stated in Article 95(3) of PSD2. However, in recognition of the comment, the EBA has reviewed the commented Guidelines, added references to PSD2 and deleted some requirements that repeated requirements directly included in PSD2. Based on several similar comments received requesting clarifications with regard to sharing of the information on security and operational risks and reservations raised by the respondents over the issues of confidentiality and competition, the EBA has decided to remove the requirement on information sharing as its practical implementation from the PSPs' side could be difficult and it would be challenging for CAs to consistently supervise this requirement. The EBA considered that such a requirement would not be proportional to the purpose of achieving broader awareness of payment fraud and security issues related to the provision of payment services. The EBA would nevertheless encourage all PSPs to participate in any platforms enabling the exchange of information on operational and security risks and threat intelligence with other PSPs and relevant third parties such as operators of payment systems, industry associations, etc., as long as these initiatives comply with applicable EU law, such as	GL 8.3, GL 8.7 and GL 8.10 have been deleted.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			Directive (EU) 2015/2366 and Regulation (EU) 2016/679 or, if applicable, Regulation (EC) 45/2001, and neither favour nor disadvantage any particular type of provider over others.	
[180]	GL-8.1	One respondent commented that there is a need to clarify the scope and meaning of the obligation to provide assistance and guidance.	The EBA decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. Therefore, the EBA is of the opinion that the high-level nature of the Guidelines means that they are unable to provide a more prescriptive way of defining assistance and guidance measures. Such measures should be adapted as appropriate for the PSP and PSU in question, as well as for the specific situation.	None.
[181]	GL-8.1	One respondent requested that the EBA specify if the PSU referred in this Guideline is the PSU that has a contractual relationship with the PSP or all PSUs, including potential ones.	The EBA would like to confirm that it is indeed the purpose of this Guideline to refer to PSUs with whom the PSP has a contractual relationship and could refer also to potential ones. Thus, the PSP should enhance the awareness of PSUs who are or will be using its services regarding security risks linked to the payment services. However, the EBA does not regard it necessary to specify this in the actual Guidelines, as all guidelines relate to services actually offered or planned and to the PSUs served.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[182]	GL-8.1	One respondent commented that the lack of a contractual or legal relationship between the PSP and the PSU should not be a reason for failing to inform the PSU about security risks. However, in most cases payment initiation service providers and acquirers have no ways of communicating directly with the PSU (i.e. phone number or email address), although can interact to some extent with PSUs during the payment process and through the PSP's website. Therefore, it might be complex to implement all the provisions made in GL 8 for all the PSPs, more precisely: – 8.2 Changes should be communicated to the PSU. – 8.4 PSPs should allow PSUs to disable specific payment functionalities. – 8.5 PSPs should provide the payer with options to reduce these limits. – 8.6 PSPs should provide the option for PSUs to set alerts.	The EBA points out that all requirements in the Guidelines should be applicable to all PSPs, with due regard to the services they provide and, hence, their business functions. If it is not feasible for a PSP to implement a particular requirement in the Guidelines because it relates to a function which that PSP does not provide, such requirement can be considered as not applicable for that PSP. The EBA would also like to remind respondents that proportionality principle set out in GL 1.1 should also be applied. In relation to the particular comment, the EBA would like to point out that the users of acquirers are the merchants, towards whom the acquiring PSPs have responsibilities. In line with the above remarks, the EBA points out that the Guidelines do not have to be applied jointly, if this is not compatible with the business model of the given PSP.	None.
[183]	GL-8.1	One respondent proposed a redrafting of GL 8.1, in particular by adding the following two sentences: 'In this course, the PSP can assume differences in the awareness needs of its serviced PSUs. This may involve differences in the awareness needs of PSUs who are customers and PSUs that are corporates.'	The EBA would like to point out that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. Therefore, the EBA is of the opinion that the high-level nature of the Guidelines means that they are unable to provide a more prescriptive way of defining assistance and guidance measures. Such measures should be adapted as appropriate for the PSP and PSU in question, as well as for the specific situation. The EBA would also like to remind respondents that proportionality principle set out in GL 1.1 should also be applied. In the light of the above arguments, the EBA does not consider it appropriate to differentiate the Guidelines according to the customer base of the PSP. Following the principles stated above, it should be sufficient to adapt the internal measures to the requirements of the Guidelines where appropriate.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[184]	GL-8.1	One respondent suggested that GL 8.1 be amended as follows: 'PSPs should establish and implement processes to enhance the awareness of PSUs they have a contractual relationship with or are in its direct sphere of influence to security risks linked to the payment services through assistance and guidance to the PSUs.'	The EBA clarifies that the Guidelines do not state general requirements, but rather all Guidelines relate to the actually offered or planned services and the PSUs served. Thus the EBA points out that GL 8.1 (now GL 9.1) requires the PSP to enhance the awareness of PSUs, who are or will be using its services, to security risks linked to the payment services offered by the PSP. Therefore, the EBA does not regard it necessary to include the proposed redrafting in the said Guideline.	None.
[185]	GL-8.1	One respondent commented that reference to Article 52(5b) of PSD2 should be made in GL 8.1.	The EBA points out that Article 52(5b) of PSD2 sets out the procedures that PSPS should follow to notify PSUs of suspected or actual fraud or security threats. The EBA would like to point out that this issue is further detailed in GL 8.8 (now GL 9.6), which has been additionally redrafted to remove overlapping requirements in relation to the secure channel defined in the RTS on SCA and CSC.	GL 8.8 (now GL 9.6) has been amended and now reads: '~~The PSP~~ PSPs should keep PSUs informed about updates in security procedures which affect PSUs regarding the provision of payment services. ~~Any alerts about significant emerging risks should also be provided via a secured channel.'~~
[186]	GL-8.2	One respondent commented that 'constantly updated' is a burdensome and uncertain requirement. The respondent suggested the following rewording of GL 8.2: 'PSUs should be updated in a timely manner of any new material threats and vulnerabilities, and material changes to such should be communicated to the PSU.' The respondent further suggested that the word 'timely' is a legal concept. Another respondent suggested clarifying the term 'constantly' and that adding a clarification such as 'at least XXX' (e.g. semi-annually) would help.	The EBA agrees with the suggestion of removing the term 'constantly'. However, the EBA is of the opinion that it is not appropriate to specify the frequency with which the PSUs should be updated as this should be done whenever deemed necessary, in accordance with the proportionality principle set out in GL 1.1.	GL 8.2 (now GL 9.2) has been amended and now reads: 'The assistance and guidance offered to PSUs should be ~~constantly~~ updated in the light of new threats and vulnerabilities and changes should be communicated to the PSU.'
[187]	GL-8.3	One respondent commented regarding GL 8.1 and GL 8.3 that in the absence of a legally binding EU-wide common register of PSPs with licences it is impossible for PSUs (and also other PSPs) to recognise a legal provider.	The EBA clarifies that the issue of PSPs registers is out of the scope of this Guideline. However, given that the requirements in GL 8.3 are already included in PSD2, the EBA has decided to remove this Guideline.	GL 8.3 has been deleted.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[188]	GL-8.4	Several respondents commented that while in principle, the Guideline is of the utmost importance, the possibility of disabling or modifying settings of functionality has impact on a PSP's internal organisation.	Although the EBA agrees with the rationale of the comment, that the possibility of disabling and modifying settings of functionality indeed has an impact on PSPs' internal processes, it is of the view that PSPs will have to comply and, where product functionality permits, allow their PSUs to disable specific payment functionalities related to the payment services the PSP provides.	None. However, GL 8.4 (now GL 9.3) has been amended following comment under ref. no. [189] and now reads: '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.'
[189]	GL-8.4	Several respondents commented that there is a need for greater clarity or more details about disabling 'specific payment functionalities' (e.g. foreign payments, payments to certain counties or payments with high fraud risk).	The EBA agrees with the comment that the term 'specific payment functionalities' is quite a wide concept. The EBA clarifies that this is related to the payment services offered by the PSP to the PSU and where the product functionality permits. For greater clarity the EBA has redrafted the Guideline accordingly.	GL 8.4 (now GL 9.3) has been amended and now reads: '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.'
[190]	GL-8.4	One respondent requested that the EBA further specifies whether the limitation will automatically apply to all channels and to all PSPs (PSUs' direct access channels and all TPPS) or if separate limitations can be defined by the PSU. The respondent also referred to the final Guidelines on the security of internet payments , and more specifically, the internet payment functionality.	The EBA is of the view that it is already stated that the limitation applies to 'specific payment functionalities', not all channels and all PSPs. The EBA would also like to remind respondents that the proportionality principle set out in GL 1.1 should also be applied.	None. However, please see amendment ref. no. [189].
[191]	GL-8.4	Several respondents commented that the PSU should be able to disable specific payment functionalities with the ASPSP only and that this should be clarified in the Guidelines.	The EBA is of the view that all Guidelines should apply to all PSPs so as not to favour specific business models and 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 GL 1.1, which means that the steps that PSPs are required to	None. However, please see amendment ref. no. [189].

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			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. In particular, for the business-model and technological neutrality reasons stated above the EBA does not agree that it is only appropriate to limit to APSPS the requirement to offer the option to disable specific payment functionalities.	
[192]	GL-8.4	One respondent posed the following question: 'If payment functionalities disabled by PSU in ASPSP and explicit consent is however given to TPP, which of these have higher rank? Should customers be able to disable access to all/individual PSPs in their internet bank?'	The EBA would like to emphasise that, according to PSD2, PSUs have the right to use different types of payment initiation channels. Disabling of specific payment functionalities should apply regardless of whether the payment is initiated directly from the ASPSP or via a TPP, following a non-discriminatory approach.	None. However, please see amendment ref. no. [189].
[193]	GL-8.4	One respondent commented that allowing PSUs to disable specific functionalities as a measure is in line with the GDPR.	The EBA agrees with the respondent. The EBA considers the current wording of the Guideline to sufficiently cover this request, as it does not limit the purpose for which the customer may disable a functionality.	None. However, please see amendment ref. no. [189].
[194]	GL-8.4	Several respondents commented that it is not clear from the Guideline whether strong customer authentication would be required to manage the limitations of functionalities, which should be the case.	The EBA agrees that that the management of limitations of functionalities or spending limits should be made in line with the RTS on SCA and SC. As this issue is specified already in the RTS on SCA and SC, no addition is made to this Guideline. The EBA would also like to clarify that this requirement would also apply by virtue of Article 97 (1) of PSD2.	None. However, please see amendment ref. no. [189].
[195]	GL-8.4	One respondent commented that the requirement to have a unique solution for PSUs to disable specific payment functionalities is overly burdensome and would be difficult to achieve in practice.	The EBA would like to clarify that there is no requirement for a unique solution for PSUs to disable specific payment functionalities in the Guideline. Each PSP can implement it depending on its PSUs, business model and technical solutions used, etc. in accordance with the proportionality principle set out in GL 1.1.	None. However, please see amendment ref. no. [189].
[196]	GL-8.4	Several respondents commented that It should be ensured that this Guideline cannot be abused by ASPSPs, to discourage the usage of payment initiation services (PIS) and account information services (AIS). Potential disablement of payment functionality should be done only on a non-discriminatory basis, for example disabling the ability to initiate credit transfers, rather than disabling TPP/PIS payments. The disruption will be quite significant for PSPs that offer a limited set of payment services (for example, payment acquiring services). One respondent requested that the EBA considers removing this specific requirement.	The EBA is of the view that all Guidelines should apply to all PSPs so as not to favour specific business models and 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 GL 1.1, which means 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.	None. However, please see amendment ref. no. [189].

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			In particular, for the business-model and technological neutrality reasons stated above, the EBA does not agree that it is appropriate to limit to certain types of PSPs or payment services the requirement to offer the option to disable specific payment functionalities. In this context the EBA would also like to clarify that disabling of payment functionalities, such as contactless payments or remote payments, does not mean disabling of payment services.	
[197]	GL-8.5	Several respondents commented that the definition of spending limits should be more specific.	The EBA would like to clarify that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. Therefore, the EBA is of the opinion that the high-level nature of the Guidelines means that they are unable to provide more prescriptive way of defining an exhaustive set of spending parameters and limits.	None. However, please see amendment ref. no. [199].
[198]	GL-8.5	Some respondents commented that the option of allowing changes to spending limits is not the only way to help the PSUs identify the most suitable spending limit according to their risk appetite, so this option should not be prescriptive. Another way could be for the ASPSP to offer the user a choice between similar products which differ in terms of spending limits, with progressively lower thresholds.	The EBA would like to clarify that it decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. In the context of this particular comment, the EBA is of the opinion that GL 8.5 (now GL 9.4), now redrafted to also offer the option to increase limits, gives PSPS the freedom to offers PSUs different ways of setting spending limits.	None. However, please see amendment ref. no. [199].
[199]	GL-8.5	Several respondents commented that the PSP should provide the payer with the option to 'adjust' these limits, not just reduce them. One respondent requested that the last sentence in this Guideline be changed to: 'the PSP should provide the payer with options to reduce these limits or to request an increase of these limits.'	The EBA agrees with the rationale of this comment and hence has reflected the relevant amendment in GL 8.5 (now GL 9.4).	GL 8.5 (now GL 9.4) has been amended and now reads: 'Where, in accordance with ~~PSD2~~ ~~a~~Article 68 (1) of Directive (EU) 2015/2366, a PSP has

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				agreed with the payer on spending limits for payment transactions executed through specific payment instruments ~~or where a PSP has defined spending limits for specific payment services,~~ the PSP should provide the payer with the option to ~~reduce~~ adjust these limits up to the maximum agreed limit.'
[200]	GL-8.5	One respondent commented that 'payer' is mentioned in this Guideline and further asked for clarification whether the Guidelines draw a distinction between a 'PSU' and a 'payer'.	The EBA would like to clarify that in all cases the choice of the term 'PSU' or 'payer'/'payee' in the Guidelines was a deliberate one, taking into consideration the content of each Guideline. This requirement in GL 8.5 (now GL 9.4) was meant to cover only 'payers' because of their role in the payment process.	None. However, please see amendment ref. no. [199].
[201]	GL-8.5	One respondent commented regarding GL 8.5 and GL 8.6 that it is unrealistic to expect PSPs to have these functions ready in January 2018, because to set up those functionalities needs time and resources. These requirements should come into force together with the RTS on SCA and CSA or within another reasonable timeframe.	The EBA acknowledges that PSPs will require time to implement the Guidelines. However, according to Article 5(1) of PSD2, the subset of legal entities that seek authorisation as payment or electronic money institutions are required to take these Guidelines into account when applying for authorisation as of 13 January 2018, which is why the application date of the Guidelines cannot be delayed beyond that date. That said, the EBA acknowledges that PSPs will require time to implement the Guidelines and are therefore not expected to comply with the Guidelines until the EBA has published the translations of the Guidelines in all official EU languages, issued the compliance table, and the CAs have implemented the Guidelines into their national regulatory or supervisory frameworks.	None. However, please see amendment ref. no. [199].
[202]	GL-8.6	Some respondents commented that the idea of the continuous alerting services is too prescriptive (also related to PSD2) and should be altered or removed.	The EBA would like to clarify that GL 8.6 (now GL 9.5) does not require 'continuous' alerts. This Guideline requires that PSPs should give PSUs the option to receive alerts on initiated and/or failed attempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their account. Like all requirements, this Guideline should be applied in accordance with the proportionality principle set out in GL 1.1.	None. However, please see amendment ref. no. [203].

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[203]	GL-8.6	One respondent commented that the generation of multiple alert messages for a single transaction can confuse the PSU and increase the number of interactions that PSPs have with the PSP customer service team and proposed that PSU alerts are limited to transaction execution outcomes.	The EBA clarifies that GL 8.6 (now GL 9.5) requires PSPs to offer PSUs the option to receive alerts on initiated and/or failed attempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their account. Therefore, GL 9.5 does not entail the requirement to provide all messages for a single transaction suggested by the respondent. However, the Guideline has been amended in view of this concern.	GL 8.6 (now GL 9.5) has been amended and now reads: 'PSPs should provide PSUs with the option ~~to set~~ to receive alerts on initiated ~~related to the initiation, the execution~~ and/or failed attempts to initiate ~~a~~ payment transactions, enabling them to detect fraudulent or malicious use of their account. ~~, in the context of the PSU profile management services platform provided to the PSU, where relevant.~~'
[204]	GL-8.6	Several respondents questioned the requirements regarding PSU alerts as currently it is necessary only to inform PSUs that their payment request will be initiated or not by the PSP. The respondents suggested that this requirement is excessive and stricter than PSD2. They further elaborated that it is especially excessive as instant payments are becoming more widely available.	The EBA would like to clarify that, even though PSD2 does not require PSPs to implement an alert mechanism as the GL 8.6 (now GL 9.5) describes, the EBA considers this risk-mitigating measure to be of particular importance and remains in the scope of the EBA's mandate granted in PSD2 for these Guidelines to define detailed security measures. It is even more important in the case of instant payments, as giving PSUs timely information on the initiation of an unauthorised payment is crucial for mitigation of subsequent fraud.	None. However, please see amendment ref. no. [203].
[205]	GL-8.6	Several respondents commented that GL 8.6 appears to impose stricter obligations than PSD2.	The EBA would like to clarify that even though PSD2 does not require that the PSPs must implement an alert mechanism as the GL 8.6 (now GL 9.5) describes, the EBA considers this risk-mitigating measure to be of particular importance and remains in the scope of the EBA's mandate granted in PSD2 for these Guidelines to define detailed security measures. It is even more important in the case of instant payments, as giving PSUs timely information on the initiation of an unauthorised payment is crucial to mitigation of subsequent fraud.	None. However, please see amendment ref. no. [203].
[206]	GL-8.6	One respondent commented that it should be added that PSPs should provide the option for PSUs to set alerts related to the	Although the EBA agrees in principle with the comment that giving PSUs the option to set alerts during the enrolment and credential-issuing processes would reduce operational and security risks, these processes	None. However, please see amendment ref. no. [203].

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		enrolment and issuing of PSUs' credentials (e.g. in the event that PSU did not receive the requested credentials).	are outside the scope of the mandate. Enrolment and the provision of PSCs are regulated by the RTS on SCA and CSC.	
[207]	GL-8.6	One respondent commented that the ability for a customer to set alerts related to the initiation, execution and failed attempt to initiate a payment transaction offers very little tangible benefit for the customer as the transaction would undergo thorough transaction risk analysis and, if appropriate, authentication before initiation.	The EBA clarifies that such risk-mitigating measures are intended to increase security (e.g. regarding fraud) and that it considers the reduction of risk and assurance offered to the PSU as a tangible benefit. It is also one of the several security measures of the risk management framework to make it efficient.	None. However, please see amendment ref. no. [203].
[208]	GL-8.6	One respondent commented that there is a risk that the information communicated regarding security issues is not sufficiently clear to enable a customer to understand which PSP they should contact in a given scenario. The respondent further recommended that PISPs be required to communicate that the customer must contact their ASPSP in the event of identifying an unauthorised transaction as part of their wider security issues process.	The EBA clarifies that it is a generic requirement for any type of PSP to communicate with the PSU they are providing their service to with regard to the initiated and/or failed attempts to initiate payment transactions via its services or ASPSP for the transactions initiated directly.	None. However, please see amendment ref. no. [203].
[209]	GL-8.7	One respondent commented that, in addition to PSUs being informed of suspected security breaches, this Guideline should indicate that any PSP indirectly affected by the suspected breach should also be informed by the PSP directly affected.	Based on several comments received requesting clarifications with regard to sharing of the information on security and operational risks and reservations raised by respondents over the issues of confidentiality and competition, the EBA has decided to remove the requirement on information sharing as the practical implementation from the PSPs' side could be difficult and it would be challenging for CAs to consistently supervise this requirement. The EBA considered that such a requirement would not be proportional to the purpose of achieving broader awareness of payment fraud and security issues related to the provision of payment services. The EBA would nevertheless encourage all PSPs to participate in any platforms enabling the exchange of information on operational and security risks and threat intelligence with other PSPs and relevant third parties such as operators of payment systems, industry associations, etc., as long as these initiatives comply with applicable EU law, such as Directive (EU) 2015/2366 and Regulation (EU) 2016/679 or, if applicable, Regulation (EC) 45/2001, and neither favour nor disadvantage any particular type of provider over others.	GL 8.7 has been deleted.
[210]	GL-8.7 general	One respondent commented that GL 8.7 appears to impose stricter obligations than PSD2.	The EBA clarifies that the purpose of the Guidelines, in line with PSD2, is to provide more precise requirements with regard to the management of	GL 8.7 has been deleted.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
			operational and security risks related to the payment services that the PSPs provide, as mandated in Article 95. However, given that the requirements in GL 8.7 are already included in PSD2, the EBA has decided to remove this Guideline.	
[211]	GL-8.7 general	One respondent commented that the Guidelines could add that PSUs should have the right to revoke the consent given to a PSP for storing and using their PSCs.	The EBA would like to clarify that the requirements related to the safeguarding of the PSU credentials (PSC) at all stages from creation to revocation or deactivation are already regulated under the RTS on SCA and CSC and thus out of scope of these specific EBA Guidelines.	None.
[212]	GL-8.7 (c)	Several respondents commented that informing the PSU of the potential security breaches and attacks is excessive and should be on a best effort basis (to avoid conflict with other regulations such as the GDPR, Directive (EU) 2016/1148 on the security of network and information systems (NIS) and RTS related to PSD2).	The EBA considers that this mitigating measure is sound and reduces security and operational risks in payment services. However, given that the requirements in GL 8.7 are already included in PSD2, the EBA has decided to remove this Guideline.	GL 8.7 has been deleted.
[213]	GL-8.7 (c)	Several respondents required that the word 'potential' be deleted from this sentence as this communication could cause customers to panic, lead to mistrust of payment systems, and cause reputational and economic damage.	Given that the requirements in GL 8.7 are already included in PSD2, the EBA has decided to remove this Guideline.	GL 8.7 has been deleted.
[214]	GL-8.7 (c)	One respondent commented that it should be clarified whether the client should be notified in real time of potential incidents or session threats.	Given that the requirements in GL 8.7 are already included in PSD2, the EBA has decided to remove this Guideline.	GL 8.7 has been deleted.
[215]	GL-8.7 (c)	One respondent invited the EBA to provide guidance to the relevant CAs on identifying the relevant PSU notification trigger conditions and ensuring that PSU notification of security breaches is applied consistently by all PSPs.	Given that the requirements in GL 8.7 are already included in PSD2, the EBA has decided to remove this Guideline.	GL 8.7 has been deleted.
[216]	GL-8.7 (c)	One respondent commented that PSPs should not be obliged to inform PSUs of internal regulatory reporting requirements for security breaches.	Given that the requirements in GL 8.7 are already included in PSD2, the EBA has decided to remove this Guideline.	GL 8.7 has been deleted.
[217]	GL-8.7 (c)	One respondent commented that the risks attributable to new threats and vulnerabilities relate to the technical side (i.e. the IT technologies used in the PSP payment processes), so the GL cannot specify precisely what threshold the PSP should use to determine when to inform PSUs.	Given that the requirements in GL 8.7 are already included in PSD2, the EBA has decided to remove this Guideline.	GL 8.7 has been deleted.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[218]	GL-8.7 (c)	One respondent commented that the aim of GL 8 is that PSUs be aware of threats and vulnerabilities and their associated risks. The respondent further elaborated that, if any of the parties involved in this process use this information channel to their own benefit, the right channels to correct the situation should have been already established. Article 68(5) of PSD2 lays down the conditions necessary to deny access to the payment account in the event of unauthorised or fraudulent actions.	Given that the requirements in GL 8.7 are already included in PSD2, the EBA has decided to remove this Guideline.	GL 8.7 has been deleted.
[219]	GL-8.8	Some respondents commented that the term 'secured channel' should be defined.	The EBA would like to clarify that the requirements concerning 'secure channel' are already specified in the RTS on SCA and CSC (EBA/RTS/2017/02) and has therefore decided to remove this part of the Guideline to eliminate overlap.	GL 8.8 (now GL 9.6) has been amended and now reads: '~~The PSP~~ PSPs should keep PSUs informed about updates in security procedures which affect PSUs regarding the provision of payment services. ~~Any alerts about significant emerging risks should also be provided via a secured channel.'~~
[220]	GL-8.8	One respondent commented that the notification of significant risks has to be provided through a safe channel. The respondent asks that EBA specifies the meaning of 'secured channel' and how it differs from 'secure channel'.	The EBA would like to clarify that the requirements concerning 'secure channel' are already specified in the RTS on SCA and CSC (EBA/RTS/2017/02) and has therefore decided to remove this part of the Guideline to eliminate overlap.	GL 8.8 (now GL 9.6) has been amended and now reads: '~~The PSP~~ PSPs should keep PSUs informed about updates in security procedures which affect PSUs regarding the provision of payment services. ~~Any alerts about significant emerging risks should also be provided via a secured channel.'~~
[221]	GL-8.8	Some respondents commented that it makes sense to inform customers of general changes to security procedures which	In consideration of this comment, the EBA amended the Guideline in question to limit the security alerts to those affecting the particular PSU.	GL 8.8 (now GL 9.6) has been amended and now reads:

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		affect them, but some changes to internal security procedures need be communicated to PSUs only on specific request.		'The PSP PSPs should keep PSUs informed about updates in security procedures which affect PSUs regarding the provision of payment services. Any alerts about significant emerging risks should also be provided via a secured channel.'
[222]	GL-8.8	One respondent disagreed that informing PSUs about emerging risks should be done using a secure channel.	While the EBA agrees in principle with the comment, it would like to clarify that, since the requirements concerning 'secure channel' are already specified in the RTS on SCA and CSC (EBA/RTS/2017/02), it has decided to remove this part of the Guideline to eliminate overlap.	None. However, please see amendment ref. no. [221].
[223]	GL-8.8	Several respondents commented that the second topic of GL 8.8 relates to emerging risks and should be part of GL 8.2.	The EBA clarifies that GL 8.2 (now GL 9.2) requires PSPs to provide assistance and guidance to PSUs on security risks and risk-mitigating actions in the light of new threats and vulnerabilities, whereas GL 8.8 (now GL 9.6) refers to updates to security procedures which affect the PSUs and information about specific imminent threats.	None. However, please see amendment ref. no. [221].
[224]	GL-8.8	One respondent suggested that GL 8.8 should be deleted as PSPs have no influence outside their own sphere. The respondent further commented that a clear definition of the stakeholders in the payment chain and their sphere of influence is required.	The EBA would like to clarify that GL 8.8 (now GL 9.6) does not require PSPs to implement changes which are outside their sphere of influence. GL 8.8 (now GL 9.6) requires PSPs to inform PSUs of updates to its own security procedures that affect PSUs.	None. However, please see amendment ref. no. [221].
[225]	GL-8.9	Several respondents commented that it should be possible to provide assistance via PSPs' normal 'helpline' (online, phone) during normal service times and that there is no need to give assistance 24/7.	The EBA would like to clarify that the Guideline does not prescribe such 24/7 assistance. It is up to the PSP based on the principle of proportionality to define the way and frequency in which the PSU will be assisted.	None. However, please see amendment ref. no. [227].
[226]	GL-8.9	Some respondents commented that it should be clarified that the PSP support does not include any form of assistance for equipment/devices belonging to the PSU.	The EBA would like to clarify that it does not prescribe or impose any specific way on how the assistance/support will be provided. It is up to the PSP based on the principle of proportionality to define the way assistance/support will be provided to the PSU.	None. However, please see amendment ref. no. [227].
[227]	GL-8.9	One respondent commented that it is not clear why this request specifically references internet payments. The respondent further questioned whether PSPs that do not provide such services are not required to provide such support. The	In recognition of this comment, the EBA has amended GL 8.9 (now GL 9.7) accordingly.	GL 8.9 (now GL 9.7) has been amended and now reads:

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		respondent asked that the EBA considers whether this specific requirement delivers real security benefits to the PSPs and PSUs.		'~~The~~ PSPs should provide ~~the~~ PSUs with assistance on all questions, ~~complaints,~~ requests for support and notifications of anomalies or issues regarding security matters related to ~~incidents internet payments and related~~ payment services. PSUs should be appropriately informed about how such assistance can be obtained.
[228]	GL-8.9	One respondent commented regarding communication channel in GL 8.8 that a new sentence should be added: 'This does not exclude online communication.'	The EBA clarifies that the commented Guideline does not prescribe any specific way of communication on how the customer should be informed. In EBA's view the PSP has an adequate level of flexibility to define its way communication subject to the principle of proportionality as defined in GL 1.1.	None. However, please see amendment ref. no. [227].
[229]	GL-8.10	One respondent commented that GL 8.10 also covers cases in which the PSP may not be allowed to notify the PSU pursuant to applicable AML regulations, financial sanctions or anti-fraud law. The respondent suggested that GL 8.10 should be limited accordingly.	Given that the requirements in GL 8.10 are already included in PSD2, the EBA has decided to remove this Guideline.	GL 8.10 has been removed.
Feedback on responses to Question 10				
[230]	General responses	Several respondents were of the view that the extension of applicability of the requirements of these Guidelines to the context of acquiring services should be described more clearly, especially with reference to the applicability of the single Guidelines. They were of the view that not all the Guidelines could be applicable to acquiring services.	The EBA points out that all requirements in the Guidelines should be applicable to all PSPs, with due regard to the services they provide and, hence, their business functions. If it is not feasible for PSPs to implement a particular requirement in the Guidelines, for example because it relates to a function which that PSP does not provide, such requirement can be considered as not applicable to that PSP.	None.
[231]	General responses	One respondent was of the view that the Guidelines should specify on the reporting frequency and other requirements imposing more scrutiny on newly incorporated PSPs or PSPs acquired by another business.	The EBA would like to clarify that reporting requirements should be applied in the same way to all PSPs, whether newly incorporated or already functioning. Regarding the acquired PSPs, their activity will be reported within the holding company.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[232]	General responses	One respondent asked if a larger PSP should organise additional assurance such as mentioned in the Guidelines, given the fact that a PSP may have an obligation to have a certified advanced measurement approaches framework.	The EBA points out that the Guidelines have been drafted taking into account the proportionality principle. Any additional assurance required should be taken in addition to the Guidelines ,provided that it would not contradict the relevant requirements.	None.
[233]	General responses	One respondent was of the view that a definition of the term 'operational risk' should be introduced as it is crucial for the application of the requirements set out in the Guidelines related to the treatment of such 'operational risks'.	The EBA is of the view that the term 'operational risk' is a term commonly used in PSD2 and EBA Guidelines. The EBA further points out that any attempt to introduce a definition of the term in these Guidelines will create legal concerns on what the term means in other parts of PSD2.	None.
[234]	General responses	One respondent was of the view that the use of existing requirements as input for the Guidelines is problematic since some of them do not apply to all PSPs but only to credit institutions (e.g. Basel Committee on Banking Supervision (BCBS) principles on operational risk; Capital Requirements Regulation (CRR) 575/2013). With regards to the above observations, the respondent therefore suggested, in consideration of the principle of proportionality, that the term 'operational risk' be applied to those PSPs which are regulated as credit institutions with a dedicated regulated concept for operational risk, which is not the case for payment institutions and electronic money institutions.	The EBA points out that, when drafting these Guidelines, it included only those requirements that apply to all PSPs and not only to PSPs that are credit institutions. It should also be noted that the EBA considered existing international guidance documents and frameworks as part of the process in developing the resultant Guidelines and adopted those elements that could be applicable to all PSPs.	None.
[235]	General responses	One respondent was of the view that the requirements in the Guidelines are not sufficient as some major points are missing in terms of methods, processes and definition of threshold parameters/matrices. One respondent suggested differentiating between 'audit' and 'certification' as well as specifying the timescales for initial certification, audits and recertification.	The EBA is of the view that the proposed additional points that the respondent suggests be included in the Guidelines are very detailed and cannot be generalised for all sizes of PSPs. The EBA is of the view that the inclusion of a definition on 'certification' and a timescale for the certification process is not in the scope of these Guidelines, as explained in one of the previous responses. The EBA also acknowledges that given that (i) no national authority requires such certification processes at present, (ii) the EBA is not mandated to make certification processes compulsory and (iii) the alternative of market-driven certification processes is voluntary, the EBA has concluded that there is little subject matter that could conceivably be harmonised throughout EBA Guidelines. The Guidelines therefore stay silent on this particular topic for now, which may change at some point in the future, should market or regulatory practices have changed such that the Guidelines need to be amended during the regular reviews that the EBA will carry out.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[236]	General responses	One respondent was of the view that there should be more clarification and differentiation with regards to those PSPs that are also CRR credit institutions. The respondent further elaborated that, in order to implement appropriate security measures for operational and security risks of payment services under PSD2, the general treatment of areas that are not directly linked to payments should be clarified. Furthermore, the respondent commented that the additional financial services offered by CRR credit institutions should not be subject to these Guidelines.	The EBA points out that the requirements in these Guidelines are applicable to PSPs which are also credit institutions. The EBA further clarifies that these Guidelines regulate only the provision of payment services and not other PSP activities.	None.
[237]	General responses	One respondent was of the view that the Guidelines are not focused enough on the provision of security measures.	The EBA is of the opinion that the Guidelines are adequately focused on identifying the security measures for PSPs taking into consideration the outcome of its risk analysis, which focused on the provision of payment services by PSPs.	None.
[238]	General responses	One respondent suggested deleting GL 6 to GL 8 as they go beyond what is required by Article 95(3) of PSD2.	The EBA is of the view that, as set out in the requirements of the Guideline on business continuity, testing and situational awareness, it is very important for PSPs to implement, test and continuously evolve their security measures, thus ensuring the effectiveness of their security and operational risk framework.	None.
General feedback				
[239]	General responses	A few respondents requested the inclusion of the EBA risk assessment referred to in section 4.2.9 of the 'Rationale' section of the Guidelines.	The EBA would like to point out that it considers that it would not be appropriate to publish the risk assessment upon which these Guidelines were based, as it could be exploited and contravene the objectives of the Guidelines.	None.
[240]	General responses	One respondent considered that the objectives for ASPSPs are missing from the current draft.	The EBA would like to remind respondents that ,based on the risk analysis ,the security objectives described in these Guidelines apply to all types of PSPs, as explained in paragraph 23 of the Rationale.	None.
[241]	General responses	One respondent was of the opinion that elements of duplication appeared across the Guidelines but did not specify the particular areas where such repetitions could be found.	The EBA would like to confirm that following the revisions made in response to the comments received in the public consultation process, it has carefully reviewed the Guidelines and has removed all identified duplications.	Please see redrafting of a number of Guidelines (i.e. under GL 9)

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[242]	General responses	One respondent requested clarification of whether requirements which are duplicated across Guidelines are expected to be undertaken separately or once only (e.g. GL 2.1 to GL 2.3 and GL 5).	The EBA would like to confirm that following the revisions made in response to the comments received in the public consultation process (with regard to GL 2.1-2.3 and GL 5), it has carefully reviewed the Guidelines and is of the opinion that no duplication of the substance of the requirements remains.	Please see redrafting proposed above for these Guidelines.
[243]	General responses	One respondent suggested that some Guidelines should not be addressed to all PSPs, and it should be specified which Guidelines apply to all PSPs and which apply only to SPSPs, PISPs and/or AISPs.	The EBA would like to restate that all requirements in the Guidelines should be applicable a, with due regard to the services they provide and hence the business functions they have. If it is not feasible for a PSP to implement a particular requirement because it relates to a function which that PSP does not provide, such requirement can be considered as not applicable to that PSP.	None.
[244]	General responses	One respondent suggested that it would also be helpful if the EBA was more specific about the risks relating to the provision of payment services	The EBA would like to remind respondents that since the scope of the Guidelines is limited to the provision of payment services, as indicated in the 'Scope of application' section, the risk assessment performed by the EBA and on which the requirements set out in these Guidelines were based was strictly limited to the risks inherent in payment services.	None.
[245]	General responses	One respondent indicated that the Guidelines do not , in the case of devices used in a payment process, distinguish between those owned and controlled by the PSP and those owned and controlled by PSUs. Therefore, the respondent suggested that a clear distinction be made in the areas such as protection, detection, testing, etc., between the PSU-controlled devices and PSP-controlled devices.	The EBA is of the view that, as a rule, and as prescribed in GL 1.8 (now GL 2.8), PSPs should enter into a contract with their outsourcing providers of equipment or software used for the provision of payment services. By means of such contracts they should enforce outsourcing providers' compliance with these Guidelines. In addition, it should be noted that all requirements need to be complied with, paying due attention to the proportionality principle. For example, if the business model includes the use of third-party devices, this should be taken into account in the risk assessment and the risks should appropriately be mitigated throughout different requirements, by other available controls.	None.
[246]	General responses	One respondent advised that EBA should consider appropriate and practical timelines for assessment and testing.	The EBA recognises the requirement to have a security policy and a BCP, but does not agree that regular testing should be performed based on these policies. Testing should be based on risks and changes performed and on regular basis to ensure the effectiveness of the security measures. The requirement for regular testing (at least once a year in the case of critical systems) could be embedded in the security policy or BCP of a PSP, but should not be a requirement. This is the responsibility of the PSP.	None.
[247]	General responses	One respondent proposed that the EBA challenges the overall Guidelines by clarifying (i) in which context of the Guidelines, even more detailed but simple EU-wide standard templates	The EBA decided to draft high-level requirements, which allow PSPs to adapt those requirements to the developments in the PSPs ecosystem. This also provides PSPs with a degree of flexibility to adapt their legal and	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		could reduce the burden on CAs and (ii) in which context regulatory compliance could be supported by existing/upcoming technology.	institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. It is therefore impossible to define more detailed conditions for compliance.	
[248]	General responses	One respondent suggested that the Guidelines be restructured to include separate categories such as (a) security; (b) business resilience including business continuity; and (c) IT resilience.	The EBA decided on the current structure because in its view it is logical. As the structure has not been contested by other respondents, the EBA has decided to keep it unchanged.	None.
[249]	General responses	One respondent criticised the need to apply the whole set of Guidelines to all PSPs and suggested making all Guidelines applicable only to credit institutions and conferring powers on CAs to apply a narrower selection of Guidelines to other PSPs in consideration of the principle of proportionality respecting the size and business model/risks profile of a PSP.	The EBA clarifies that application of the proportionality principle when developing BCPs should not result in different security levels.	None.
[250]	General responses	Several respondents indicated that there is a lack of reference to certification processes. They pointed out that certificates facilitate the documentation of security standards and this will be helpful in the context of an application for authorisation. Certificates may also allow customers to quickly assess the level of security of relevant services and facilitate the provision of services at the EU level and enhance transparency.	The EBA acknowledges that given that (i) no national authority requires such certification processes at present, (ii) the EBA is not mandated to make certification processes compulsory and (iii) the alternative of market-driven certification processes is voluntary, there is little subject matter that could conceivably be harmonised throughout EBA Guidelines. The Guidelines therefore stay silent on this particular topic for now, which may change at some point in the future, should market or regulatory practices change such that the Guidelines need to be amended during the regular reviews that the EBA will carry out.	None.
[251]	General responses	Two respondents were of the opinion that the EU (and more specifically the Commission and ENISA) should develop a pan-European security framework similar to the US National Institute of Standards and Technology (NIST) framework.	The EBA would like to clarify that this comment is out of the scope of these Guidelines. Article95(3) of PSD2 mandates the EBA, in close cooperation with the ECB, and after consulting all relevant stakeholders, to issue Guidelines with regard to the establishment, implementation and monitoring of the security measures that PSPs must take to manage operational and security risks relating to the payment services they provide. Therefore, any frameworks developed by the commented institutions are out of the scope of the mandate.	None.
[252]	General responses	One respondent asked that a 'Lessons learned' section be included in the Guideline.	This comment is out of scope of these Guidelines, but will be considered in the future review of the application of these Guidelines.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[253]	General responses	Several respondents noted that the scope of the assessment needs to be extended beyond payment process to, for example, enrolment, identity proving, regulatory risks, etc., but one stated that the assessment needs to be limited in scope to payment services.	The EBA would like to clarify that the scope of the Guidelines is limited to the provision of payment services, as indicated in the 'Scope of application' section. Therefore, the EBA points out that other processes or activities undertaken by PSPs are out of the scope of these Guidelines.	None.
[254]	General responses	One respondent asked for more clarity on what requirements are mandatory and what constitutes best practice.	The EBA would like to remind respondents that all the requirements set out in these Guidelines should apply to all PSPs so as not to favour specific business models and 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 GL 1.1, which means 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.	None.
[255]	General responses	One respondent asked the EBA to reconsider the definition of security risks mentioned in the EBA's risk analysis.	The EBA clarifies that it reconsidered the definition of the security risk and is of the opinion that it is compatible with the mandate given to the EBA to deliver these Guidelines.	None.
[256]	General responses	One respondent asked whether national and European regulations will be repealed and replaced by these Guidelines, thus avoiding any overlaps or conflicts between the various rules.	The EBA would like to point out that it is not its intention that these Guidelines repeal any binding European or national regulations in force, but, in the case of overlapping requirements, such regulations could be repealed by other regulatory means, out of the scope of these Guidelines. Nevertheless, the EBA has reviewed all requirements in the Guidelines and introduced amendments wherever it deems this to be necessary.	Please see redrafting proposed above for certain Guidelines (e.g. former GL 8 – now GL 9).
[257]	General responses	One respondent considered that Article 33.3 of the Draft RTS on SCA and CSC as amended by the European Commission is redundant and duplicates these Guidelines.	The EBA clarifies that this proposal on RTS on SCA and CSC is out of the scope of these Guidelines.	None.
[258]	General responses	One respondent proposed to include a specific reference to provisions for recovery or anonymisation of sensitive data.	The EBA clarifies that the Guidelines have been brought into alignment with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (the GDPR) wherever this was deemed applicable.	Please see redrafting proposed above for the relevant Guidelines.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[259]	General responses	One respondent commented that the Guidelines are based on requirements for banks in other regulations or regulators' recommendations (e.g. NIST, ISO 27001, CRD IV). So while the EBA's proposed Guidelines will be additional rules for banks, these Guidelines will be the only set of security measures that also include requirements for TPPs. The respondent asked that the EBA provide additional clarity to ensure not only that the Guidelines will remain in line with what is already required for banks, but also that the rules for TPPs align with current best practices in the payment industry.	The EBA clarifies that the Guidelines can only set out binding requirements for the addressees, and therefore are not appropriate to prescribe best practices. The scope of the Guidelines is limited to the provision of payment services, as indicated in the 'Scope of application' section. Other processes or activities undertaken by the PSPs are out of the scope of these Guidelines, but may be subject to other regulatory requirements due to different legal considerations. Industry standards and other self-regulatory initiatives are also out of scope of these Guidelines and cannot be enforced in the EBA regulatory acts. In addition, the EBA is of the view that, if the Guidelines were to refer to particular requirements set out in other regulations, a maintenance issue would be introduced inasmuch as the Guidelines would possibly have to be updated when the frameworks or other regulation are altered.	None.
[260]	General responses	One respondent requested that the Guidelines explicitly state that, since banks are also subject to many regulations on security measures for operational and security risks (e.g. NIST, ISO 27001, CRD IV) other than these Guidelines, other PSPs, such as TPPs and other providers of payment-related services (not clear if TPPs are meant or also outsourcing providers) should treat the Guidelines as minimum standard and also adopt the best practices related to security common in the payment industry.	The EBA clarifies that the Guidelines on the security measures for operational and security risks can only set out binding requirements for the addressees, and therefore are not appropriate to prescribe best practices. The scope of the Guidelines is limited to the provision of payment services, as indicated in the 'Scope of application' section. Other processes or activities undertaken by the PSPs are out of the scope of these Guidelines, but may be subject to other regulatory requirements due to different legal considerations. Industry standards and other self-regulatory initiatives are also out of the scope of these Guidelines and cannot be enforced in the EBA regulatory acts.	None.
[261]	General responses	One respondent requested that the Guidelines explicitly state that certain levels of security can be achieved by different means and suggested that the EBA should maintain technological neutrality when setting risk management Guidelines. The respondent was of the opinion that this practice is not followed in GL 3.8.	The EBA concurs with the view that the Guidelines should not favour specific business models and ensure technological neutrality, which was consistently applied by the EBA in the drafting. 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. In addition, the Guidelines are subject to the principle of proportionality, set out in GL 1.1, which means 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. With regard to this particular comment, the EBA would like to point out that GL 3.8 (now GL 4.7) has been redrafted to clarify scope, content and frequency of the control and is therefore deemed technologically neutral.	GL 3.8 (now GL 4.7) has been amended and now reads: '~~Upon access to the payment service,~~ PSPs should regularly check that the software used for the provision of payment services including the users' payment related software, is up to date and that critical security patches are deployed. PSPs should ensure that integrity checking

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				mechanisms are in place in order to verify the integrity of software, firmware and information on their payment services.'
[262]	General responses	Several respondents, while agreeing that the objectives of the Guidelines identified by the EBA are generally plausible, raised concerns on proportionality and recommended that the level playing field objective should be clarified to confirm that the level and detail of the information expected is proportionate to the size and complexity of the applicant and the risk that the applicant poses to consumers.	The EBA is of the view that all Guidelines should apply to all PSPs so as not to favour specific business models and 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 GL 1.1, which means that the steps that PSPs are required to take to be compliant may differ between PSPs depending on their on their size and the nature, scope, complexity and riskiness of the particular service(s) they provide or intend to provide.	None.
[263]	General responses	Many respondents suggested that the Guidelines should include guidance on how to apply the principle of proportionality. They also believed that proportionality may be applied to BCPs but not to cybersecurity of physical security measures.	The EBA would like to restate that the principle of proportionality should be applied throughout the Guidelines. Therefore, the Guidelines require all security measures to be complied with by each PSP in relation to the payment services they provide regardless of the size of the PSP and the business model followed. The principle of proportionality states 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. The EBA is of the opinion that the high-level nature of the Guidelines means that they are unable to provide a more prescriptive way of application of the proportionality principle, which specifies only criteria on the extent to which concrete steps to comply with the Guidelines are to be taken by the addressees.	None.
[264]	General responses	Several respondents also suggested that, in order to adequately address the broad variety of business models and risks implied by payment services provided by very differently structured and regulated PSPs, the principle of proportionality should be applied in a broader sense than proposed by the EBA and include the risk profile of a given PSP or the role it plays in the payment chain.	The EBA agrees with the comment; hence, the risk profile of a given PSP has been included in the principle of proportionality. The EBA Is of the view that this element should be taken into account when determining the precise steps a given PSP needs to take in order to comply with the Guidelines. Furthermore, the EBA would like to point out that the risk profile of a given PSP or the role it plays in the payment chain should be included in the risk assessment that is used to produce the risk management framework of every PSP. In recognition of the importance of the proportionality principle, it has also been moved to GL 1.	Paragraph 7 of the consultation paper rationale has been redrafted and moved to GL 1.1. It now reads: 'All PSPs should comply with all the provisions set out in these Guidelines. The level of detail should be proportionate to the

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				PSP's size and to the nature, scope, complexity and riskiness of the particular services that the PSP provides or intends to provide.'
[265]	General responses	One respondent remarked that, given that the Guidelines require all PSPs to draft every year, or at more frequent intervals, an assessment of the operational and security risks, clear criteria should be included in the Guidelines. The respondent was of the opinion that the certification process should be defined and agreed at a European level.	The EBA acknowledges that given that (i) no national authority requires such certification processes at present, (ii) the EBA is not mandated to make certification processes compulsory and (iii) the alternative of market-driven certification processes is voluntary, the EBA has concluded that there is little subject matter that it could conceivably be harmonised throughout EBA Guidelines. The Guidelines therefore stay silent on this particular topic for now, which may change at some point in the future, should market or regulatory practices change such that the Guidelines need to be amended during the regular reviews that the EBA will carry out.	None.
[266]	General responses	Several respondents were of the view that there is an overlap between different reporting obligations to which they are subject to, concerning cyber risks and operational risks so they propose greater harmonisation. In particular, they refer to PSD2,the NIS, the GDPR and eIDAS. They also referred to the definition of 'Security risk' on page 16 of this Final Report and point out that it is not in line with the definition included in EBA/GL/2017/05 (SREP).	The EBA clarifies that the Guidelines on ICT risk assessment under the SREP provide a definition of the term 'ICT security risk' which is narrower than the definition of security risks in the context of these Guidelines. While drafting these Guidelines, the EBA considered to the extent possible the requirements stemming from other regulations and the requirements in these Guidelines apply only to the management of the operational and security risks relating to the payment services provided by PSPs. Due to the material differences in the addressees, objectives and scope of different regulatory requirements with regard to cyber risks and operational risks, it is impossible to merge or harmonise them to a greater extent, as these Guidelines relate only to managing operational and security risks in the provision of payment services. More generally, the EBA notes that the various sets of Guidelines and RTS that the EBA has developed are mostly in fulfilment of specific mandates that different EU Directives have conferred on the EBA. The EBA has no role in the development of Directives and is not in a position to change the scope of the mandates received. However, when delivering the mandates, the EBA does its best to identify existing requirements, and either cross-refer to those other requirements or copy and paste the content, rather than developing different requirements. One constraint in this process is that different Directives apply to different sets of financial institutions. For example, while CRD IV applies only to credit institutions in the EU, PSD2 applies also to payment institutions.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[267]	General responses	Several respondents requested the harmonisation of all Guidelines and definitions from different regulatory authorities regarding incident reporting.	The EBA would like to point out that, while drafting these Guidelines, it considered to the extent possible the requirements stemming from other regulations and the requirements in these Guidelines apply only to the management of the operational and security risks relating to the payment services provided by the PSPs. Therefore, due to the material differences in the addressees, objectives and scope of different regulatory requirements with regard to incident reporting, it is impossible to merge or harmonise them to a greater extent.	None.
[268]	General responses	A few respondents were of the view that the CAs should provide support to the smaller PSPs that are expected to enter the market once PSD2 is adopted, in order to help them set up and apply the requirements of the Guidelines (e.g. by establishing contact points for answering questions and queries).	The EBA is of the view that the referred request is out of the scope of the Guidelines. However, the EBA considers that CAs already have contact points for the submission of applications for authorisations and these should be suitable addresses for any queries.	None.
[269]	General responses	Few respondents suggested that the PSPs' licensing process should take into consideration the existence of an adequate operational and security risk management framework according to these GLs.	The EBA clarifies that this proposal is out of the scope of these Guidelines and relates to the Guidelines on the information to be provided by applicants intending to obtain authorisation as payment and electronic money institutions as well as to register as an AISP under PSD2 (EBA/GL/2017/09).	None.
[270]	General responses	One respondent was of the opinion that the EBA should make it clear throughout the Guidelines that the risk policy setting the 'risk appetite' should be the prerogative of the management of the PSP.	The EBA agrees with the comment and points out that GL 1.1 (now GL 2.1) now states, 'PSPs should establish an effective operational and security risk management framework (hereafter 'risk management framework'), which should be approved and reviewed, at least once a year, by the management body and, where relevant, by the senior management […]'. GL 1.2 (now GL 2.2) follows and states that the risk management framework should be consistent with the risk appetite of the PSP.	GL 1.1 (now GL 2.1) has been redrafted and now reads: 'PSPs should establish an effective operational and security risk management framework (hereafter 'risk management framework') ~~for the provision of payment services~~, which should be approved and reviewed, at least once a year, by the management body and where relevant, by the senior management […]'

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				GL 1.2 (now GL 2.2) has also been redrafted and now reads: The risk management framework should: a) include a comprehensive security policy document as referred to in Article 5(1)(j) of Directive (EU) 2015/2366; ~~which sets the risk appetite of the PSP, its security objectives and measures;~~ b) be consistent with the risk appetite of the PSP; ~~b~~c) define and assign key roles and responsibilities as well as the relevant reporting lines required to enforce the security measures and to manage security and operational risks ~~related to the provision of payment services~~; d) establish the necessary procedures and systems to identify, measure, monitor and manage the range of risks stemming from the ~~provision of payment~~

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
				~~services~~ payment-related activities of the PSP and to which the PSP is exposed to including business continuity arrangements.
[271]	General responses	Some respondents commented that the implementation date (13 January 2018), assuming that there is a period of six months between the date originally foreseen in PSD2 for the issuance of these Guidelines (13 July 2017) and the stated date of their applicability (13 January 2018), seems to be too early for a proper implementation. One respondent suggested that the Guidelines should allow for a period of at least six months from the publication date of the final Guidelines by the EBA to their application date. Anther respondent suggested that the EBA clarify its expectations around the effective date of implementation of the requirements.	The EBA acknowledges that PSPs will require time to implement the Guidelines. However, according to Article 5(1) of PSD2, the subset of legal entities that seek authorisation as payment or electronic money institutions are required to take these Guidelines into account when applying for authorisation as of 13 January 2018, which is why the application date of the Guidelines cannot be delayed beyond that date. That said, the EBA acknowledges that PSPs will require time to implement the Guidelines and are therefore not expected to comply with the Guidelines until the EBA has published the translations of the Guidelines in all official EU languages, issued the compliance table, and the CAs have implemented the Guidelines into their national regulatory or supervisory frameworks.	None.
[272]	General responses	One respondent was of the view that the goals of the Guidelines are not clearly defined.	Given that no concrete proposal was received on how to improve this and given that no other similar concerns have been received from the market, the EBA is of the opinion that the objectives of the Guidelines are well set out in chapter 2 'Subject matter, scope and definitions'.	None.
[273]	General responses	One respondent was concerned that there is misconception in the market that ASPSPs are responsible for controlling and monitoring TPPs and, therefore, suggested that the Guidelines should it make clear that the security measures applicable to TPPs are their responsibility.	The EBA is of the view that all Guidelines should apply to all PSPs so as not to favour specific business models and 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 GL 1.1, which means 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.	None.
[274]	General responses	One respondent was of the view that the Guidelines should not impose the same level of requirements on the new types of PSPs introduced with PSD2 (PISPs and AISPs), as with the PSPs	The EBA is of the view that all Guidelines should apply to all PSPs so as not to favour specific business models and 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.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		that actually handle customers' funds, and this proportionality should be stated clearly in the Guidelines.	However, the Guidelines are subject to the principle of proportionality, set out in GL 1.1, which means 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. In particular, for the business-model and technological neutrality reasons stated above, the EBA does not agree that it is appropriate to apply different regulatory requirements to different types of PSPs.	
[275]	General responses	Several respondents were concerned that there are overlaps and inconsistencies between different regulatory documents, for example ICT Risk SREP/other regulations of German authorities (MaRisk) or EBA Guidelines 44, which should be avoided. They were of the view that the regulators should establish a unified set of security standards for TPPs and the banks. One such respondent also suggested that a list of all recommendations: these EBA Guidelines and other EBA Guidelines and industry standards, such as the Payment Card Industry Data Security Standard, should be drafted so that banks/PSPs have a complete view of all security measures that are applicable to them.	While drafting these Guidelines, the EBA considered to the extent possible the requirements stemming from other regulations and the requirements in these Guidelines apply only to the management of the operational and security risks. Due to the material differences in the addressees, objectives and scope of different regulatory requirements, it is impossible to merge or harmonise them to a greater extent.	None.
[276]	General responses	One respondent was of the view that it should be taken into account that many risk measures also arise from the EU framework on banking regulation. The respondent proposed the following additional sentence in Section 2, 'Subject matter, scope and definition', paragraph 9, 'Scope of application': 'As CRR credit institutions are obliged to establish, implement and monitor security measures for operational and security risks by banking law, the content of these Guidelines affect them exclusively in their role as payment service provider.'	The EBA points out that, while drafting these Guidelines, it considered to the extent possible the requirements stemming from other regulations and the requirements in these Guidelines apply only to the management of the operational and security risks relating to the payment services provided by the PSPs. Due to the material differences in the addressees, objectives and scope of different regulatory requirements, it is impossible to merge or harmonise them to a greater extent.	None.
[277]	General responses	One respondent suggested that it is very important that EU-wide activities such as PSD2 and GDPR be coordinated in order to create common core documents for the risk management framework.	While drafting these Guidelines, the EBA considered to the extent possible the requirements stemming from other regulations and the requirements in these Guidelines apply only to the management of the operational and security risks relating to the payment services provided by the PSPs. Due to the material differences in the addressees, objectives and scope of different regulatory requirements, it is impossible to merge or harmonise them to a greater extent.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[278]	General responses	One respondent was concerned that these Guidelines have been drafted prior to the finalisation of the ITS and RTS on the EBA Register (or finalisation of the RTS on SCA and CSC) and this makes it difficult to assess the impact that AISPs and PISPs will have on the relationship with the PSPs and their PSUs so they advise that EBA review again the Guidelines on operational and security risks once there is more clarity.	With regard to the RTS/ITS on the EBA Register, the EBA does not see any potential conflicts. Regarding the reference to the EBA RTS on SCA and CSC, this EBA product is now public and the EBA has taken the requirements set therein into account when developing these Guidelines. In addition, pursuant to Article 95.3 of PSD2 the EBA shall in close cooperation with the ECB review the Guidelines referred to in first subparagraph on a regular basis and in any event at least every two years.	None.
[279]	General responses	One respondent enquired if there is a specific security standard proposed as a benchmark where there is reference in the Guidelines for 'adequate' and 'appropriate' levels of security.	While the EBA agrees in principle with the comment, it acknowledges that there are certification processes in some jurisdictions. The EBA clarifies that in those jurisdictions where these are required by national regulation, Competent Authorities can request the referred from the PSPs. However, the Guidelines do not detail the specific standards that must be implemented since in the EBA's view this would go against PSD2 objectives of ensuring technology and business model neutrality.	None.
[280]	General responses	A few respondents suggested that some Guidelines should not be addressed to all PSPs, and it should be specified which Guidelines apply to all PSPs and which only to ASPSPs, PISPs and/or AISPs.	The EBA is of the view that all Guidelines should apply to all PSPs so as not to favour specific business models and 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 GL 1.1, which means 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.	None.
[281]	General responses	One respondent requested providing additional detail on how the EBA suggests testing compliance with the Guidelines and the acceptable controls in order to strike the right balance between the efforts for achievement a 'fully compliant' status and the actual and proportionate supervisors' expectations.	The legal instruments of the EBA do not foresee any additional guidance on their application (or assessing compliance with them), such as assessment guides. Instead, any requirements that apply to PSPs are set out in the Guidelines themselves. The EBA decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. This also provides PSPs with a degree of flexibility to adapt their legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. The EBA therefore finds it inappropriate to define more detailed conditions for compliance.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
[282]	General responses	One respondent suggested that the EBA issue Guidelines on the practical implementation expectations of these and other Guidelines.	The legal instruments of the EBA do not foresee any additional guidance on their application (or assessing compliance with them), such as the suggested 'Guidelines on practical implementation'. Instead, any requirements that apply to the PSPs are set out in the guidelines themselves. The EBA decided to draft high-level requirements, which allow PSPs to adapt those requirements to the development of the payment services they offer and related threats. It also leaves a level of flexibility to adapt the PSP's legal and institutional solutions to comply with the requirements set out in the Guidelines. Technological neutrality was also an important guiding principle and the high-level character of the Guidelines should enable the PSPs to adapt their security measures to technology changes. The EBA therefore finds it inappropriate to define more detailed conditions for compliance.	None.
[283]	General responses	One respondent questioned the EBA mandate, suggesting that it does not refer to all tasks to be implemented by EU Member States pursuant to Article 95(1) or (2) PSD2 and does not refer to operational risk. The respondent suggested that the EBA's mandate is restricted to 'security measures' under Article 95(3) PSD2 and does not include setting out rules with comprehensive impact on the internal governance arrangements of PSPs.	The EBA points out that these Guidelines, according to the mandate conferred on the EBA pursuant to Article 95(3) of PSD2, refer to both operational and security risks connected with the provision of payment services. The EBA is of the opinion that the mandate conferred on it by Article 95(3) should be read jointly with Article 95(1) of PSD2.	None.
[284]	General responses	One respondent suggested that GL 1 and GL 6 to GL 8 all cover general compliance aspects which are indicated neither by Article 9 (3) nor by Article 5(2)(j) of PSD2 (implying that they are out of scope). The respondent suggested deleting GL 6 to GL 8 and replacing them with a general requirement: 'The PSP should ensure adequate monitoring of internal and external developments, adapt its security framework to mitigate emerging risks, threats and vulnerabilities and ensure appropriate testing of the effectiveness of the security framework as a whole.'	The EBA is of the opinion that the commented Guidelines are in line with the mandate conferred on the EBA pursuant to Article 95(3) of PSD2, as they refer to the operational and security risks connected with the provision of payment services.	None.
[285]	General responses	One respondent questioned the need for the Guidelines to set explicit timeframes within which certain measures and/or procedures need to be reviewed (e.g. in GL 5/5.6 'are tested at least annually') and suggested that it is out of the scope of EBA mandate as opposed to Member States responsibilities under art. 95 (2) (requiring Member States to ensure that PSPs provide to the CA on an annual basis, or at shorter intervals as determined by the CA, an updated and comprehensive assessment of the operational and security risks relating to the	The EBA is of the opinion that the setting of timeframes related to different requirements is of great importance to the development of dynamic and agile risk management framework, with appropriate mitigation measures and control mechanisms to address current and future threats and vulnerabilities by the PSPs and is thus in line with the mandate conferred on the EBA pursuant to Article 95(3) of PSD2.	None.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposal
		payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks).		