EBA/CP/2017/04

05 May 2017

Consultation Paper

Draft Guidelines on the security measures for operational and security risks of payment services under PSD2

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 11 mandates conferred on EBA, as specified in Article 95 of PSD2, relates to the development, in close cooperation with the European Central Bank (ECB), of Guidelines 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 risk and has adapted them where appropriate to the specificities of payment services. EBA and ECB have also carried out a risk analysis to determine the main threats and vulnerabilities to which payment service providers are currently exposed.

These resultant Guidelines proposed in this Consultation Paper set out the requirements that payment service providers should implement in order to mitigate operational and security risks derived from the provision of payment services. They cover the governance, including on the operational and security risk management framework, the risk management and control models, and outsourcing; risk assessment, including the identification, classification and risk assessment of functions, processes and assets; the protection of the integrity of data, systems and confidentiality, physical security and asset control.

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

Next steps

The consultation period will run from 5 May 2017 to 7 August 2017. The final Guidelines will be published after this consultation.

2. Abbreviations

BCBS	Basel Committee on Banking Supervision
CP	Consultation Paper
CPMI	Committee on Payments and Market Infrastructures
EBA	European Banking Authority
ECB	European Central Bank
GL	Guideline
IOSCO	International Organisation of Securities Commissions
NIS Directive	Directive on security on network and information systems
NIST	National Institute of Standards and Technology
PSD	Payment Service Directive
PSP	Payment service provider
PSU	Payment Service User

3. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2.

Comments are most helpful if they:

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

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 07.08.2017. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

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

Data protection

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

4. Background and rationale

4.1 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. The PSD2 has conferred 11 mandates on the EBA, one of which relates to the development, in close cooperation with the European Central Bank (ECB), of the Guidelines on the security measures for operational and security risks of payment services (Article 95 of the 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, payment service providers 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 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 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 draft 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, EBA shall promote cooperation, including the sharing of information, in the area of operational and security risks associated with payment services among the competent authorities, and between the competent authorities and the ECB and, where relevant, the European Union Agency for Network and Information Security (ENISA).

6. The draft Guidelines are one of the three security related mandates conferred on the EBA in PSD2, and that the EBA has developed in cooperation with the ECB. They complement the *Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication* that were submitted to the European Commission for adoption 23 February

2017,[1] and the *Guidelines on Major Incidents Reporting* for which public consultation finished on 7 March 2016.[2]

7. The draft Guidelines are subject to the principle of proportionality, which means that all PSPs are required to be compliant with all Guidelines, but the precise steps that they are required to take to be compliant may differ between PSPs, depending on their size, business model and complexity of their activities.

8. In what follows in the rationale section below, this Consultation Paper explains the approach the EBA has taken to developing the Guidelines proposed in this Consultation Paper, the reasoning for some of the options that have been considered and the decisions that have been taken.

4.2 Rationale

9. Prior to developing the draft Guidelines, the EBA performed a comprehensive risk analysis in order to understand and identify the threats and vulnerabilities to which PSPs are exposed.

10. Based on this risk analysis, the EBA concluded that the type and nature of the threats are evolving rapidly, and that the draft 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.

Question 1: Do you agree with the level of detail set out in the draft Guidelines as proposed in this Consultation Paper or would you have expected either more or less detailed requirements on a particular aspect? Please provide your reasoning.

11. The EBA risk analysis identified a wide range of threats and vulnerabilities including (i) inadequate protection of communication channels used for payments; (ii) inadequately secured systems and devices including but not limited to applications, servers, user's payment devices; (iii) unsafe behaviour of users or PSPs' staff; (iv) increased complexity of the payments environment; and (v) technological advancements and tools that are available to potential fraudsters or malicious attackers.

12. Although these were the currently identified threats and vulnerabilities, the threat landscape is constantly evolving and as such, the EBA arrived at the view that the draft Guidelines should be developed such 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.

[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

13. In terms of the key objectives, the EBA considered that, for the purpose of managing operational and security risks in the provision of payment services, PSPs should establish and implement security measures to prevent, react to and correct the unauthorized use, disclosure, access, modification, and accidental or malicious damage or loss of their logical and physical assets, including in particular the payment service user's data, his sensitive payment data and the personalized security credentials delivered by a PSP to the payment service user for the use of a payment instrument.

14. Furthermore, the EBA considered that PSPs should mitigate risks resulting from inadequate or failed internal processes and systems, inappropriate people's behaviour or from external events. In particular, PSPs should pay special attention to the risks stemming from inadequate physical security, cyber-attacks and inadequate design or implementation of security policies.

15. Finally, the EBA considered that security measures should be implemented in accordance with Article 95 PSD2 and should be, as defined in these draft Guidelines, fully integrated into their overall risk management processes and constantly monitored. To this end, PSPs should conduct periodic reviews of their security measures and should ensure effective reporting mechanisms to the management body and to the senior management responsible for the provision of payment services, with a view to monitoring on a continuous basis compliance of the implemented security measures with the established operational and security policies and procedures.

16. In order to achieve the above objectives, and to address the threats and vulnerabilities identified in the risk analysis, the EBA considered and reviewed existing international guidance documents and frameworks as part of the process in developing the draft Guidelines. In particular, the EU Network and Information Systems (NIS) Directive[3], the BCBS principles on operational risk[4] , the US NIST Framework,[5] and the CPMI-IOSCO Guidance[6] on cyber resilience for financial market infrastructures were used as a basis.

17. Furthermore, the EBA *Guidelines on the Security of Internet Payments* (EBA/GL/2014/12),[7] as well as earlier work of the European Forum on the Security of Retail Payments (SecuRe Pay) on the security of mobile payments and payment accounts access services was also taken into account.

18. The EBA also concluded that the Guidelines proposed in this Consultation Paper should encapsulate categories on governance, risk assessment, protection, detection and business continuity.

19. However, given the rapidly evolving threat landscape as well as changes in a PSP's vulnerabilities, the EBA also concluded that the part of the EBA mandate related to the monitoring of the

[3] NIS: EU Directive on Network and information systems (NIS) , July 2016

[4] BCBS Review of the Principles for the Sound Management of Operational Risks, October 2014

[5] NIST Framework for Improving Critical Infrastructure Cybersecurity, February 2014

[6] CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure, June 2016

[7] See http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments

security measures would need to be interpreted in an extensive manner, in order to ensure that PSPs adapt their measures frequently to the changing landscape.

20. As a result, additional categories on testing, situational awareness and continuous learning have been added, to ensure that the PSP is continually monitoring internal and external developments, internalising these to adapt its framework, when required, to mitigate emerging risks, threats and vulnerabilities and thereafter testing the effectiveness of the framework as a whole. Finally, a category on payment service user (PSU) relationship management has been included, given its importance to the PSP and the wider ecosystem; PSPs will be required to ensure that their measures are well communicated to their user base, to reduce risks to and from them.

21. An effective framework should consist of the above eight components, and within each of these, the requirements should prescribe the establishment of the appropriate roles and responsibilities, structures, systems, policies and procedures with regard to the necessary security measures. These should thereafter be implemented and should finally be monitored to ensure they are implemented effectively.

22. The structure of the Guidelines has been set accordingly, with each Guideline corresponding to one of the eight components. Guideline 1 on *Governance* is consistent with effective management of other forms of risk faced by a PSP, as sound governance is key for the management of operational and security risks. The requirements around sound governance refer to the arrangements a PSP puts in place to establish, implement and monitor its approach to managing operational and security risks.

23. As such, Guideline 1 proposes that effective governance should start with defining a clear and comprehensive operational and security risk management framework. The framework should be guided by security objectives and proportional to the underlying risks. It is essential that the framework is supported by clearly defined roles and responsibilities, and it is incumbent upon the senior management to create a culture which recognises that staff at all levels has important responsibilities in ensuring the PSP's security. Guideline 1 includes requirements on the basic elements of a PSP's operational and security risk management framework and how a PSP's governance arrangements should support that framework, so as to foster a culture of risk monitoring and continuous learning and evolving.

Question 2: Do you agree with the proposed Guideline 1 on Governance? If not, please provide your reasoning.

24. Guideline 2 on *Risk assessment* covers requirements for PSPs to identify their critical business functions and supporting information assets that should be protected, in order of priority, against operational and security risks. Guideline 2 therefore outlines how a PSP should identify and classify business processes, information assets, system access and external dependencies as well as the necessity for the PSP to identify potential risks imposed on PSU, and conduct risk assessments of the aforementioned to ensure the appropriate level of security measures are

applied. This is aimed at helping the PSP better to understand its internal situation, the operational and security risks that it bears and that it poses to entities in its ecosystem, and how it can best design its security measures to ensure safety and security as a whole.

Question 3: Do you agree with the proposed Guideline 2 on Risk assessment? If not, please provide your reasoning.

25. Guideline 3 on *Protection* recognises that a PSP's security depends on effective security controls that protect the confidentiality, integrity and availability of its assets, including the provision of its services. Guideline 3 therefore requires PSPs to implement appropriate and effective controls and design systems and processes to prevent, limit and contain the impact of a potential security incident.

26. At the heart of this, PSPs are required to take a defence-in-depth approach by instituting multi-layered protection controls, with each layer serving as a safety net for preceding layers. Guideline 3 also includes requirements related to the authentication for the conduct of payment services from an internal point of view (i.e. authentication procedures of personnel to access payment services systems) without prejudice to the requirements of the regulatory technical standards on strong customer authentication and secure communication.

Question 4: Do you agree with the proposed Guideline 3 on Protection? If not, please provide your reasoning.

27. Guideline 4 on *Detection* requires a PSP to build up an ability to detect the occurrence of anomalies and events indicating a potential security incident as this is essential for achieving strong security. Early detection provides a PSP with useful lead time to mount appropriate countermeasures against a potential incident, and allows proactive containment of actual incidents.

28. Given the stealthy and sophisticated nature of certain threats where multiple entry points exist through which a compromise could take place, Guideline 4 requires proportionate monitoring tools and organisational processes and structures to be used by a PSP for the detection of security incidents.

29. With regard to reporting procedures, these are taken into account from the PSP point of view, focusing on internal classification and reporting to senior management without prejudice to the requirements of the separate EBA Guidelines on Major Incident Reporting under PSD2, which set out requirements for the classification of major incidents for the reporting to competent authorities (EBA-CP-2016-23).

Question 5: Do you agree with the proposed Guideline 4 on Detection? If not, please provide your reasoning.

30. Guideline 5 on *Business continuity* recognises that it is critical that a PSP's arrangements are designed such that it is able to resume critical operations rapidly, safely and with accurate data, in order to guarantee the continuity of the provision of payment services and limit negative impact on PSPs and PSUs in the event of severe business disruption. Guideline 5 therefore requires PSPs to have capabilities to respond to, and recover from, a broad range of scenarios, and the need for strong crisis communications and incident management processes.

Question 6: Do you agree with the proposed Guideline 5 on Business continuity? If not, please provide your reasoning.

31. Guideline 6 on *Testing of security measures* requires that the elements of its operational and security risk management framework should be rigorously tested before and after implementation to determine their overall effectiveness. Sound testing regimes produce findings that should be used to identify gaps against stated security objectives and provide credible and meaningful inputs to the PSP's management of operational and security risks. Guideline 6 therefore sets out the areas that should be included in a PSP's testing programme and how results from testing should be used to improve its operational and security risk management framework.

Question 7: Do you agree with the proposed Guideline 6 on Testing of security measures? If not, please provide your reasoning.

32. Guideline 7 on *Situational awareness and continuous learning* covers requirements to ensure strong situational awareness that can significantly enhance a PSP's ability to understand and pre-empt security events, and to effectively detect, respond to and recover from scenarios that are not prevented. Specifically, a solid understanding of the threat landscape can help a PSP better identify and understand the vulnerabilities in its critical business functions, and facilitate the adoption of appropriate risk mitigation strategies. Guideline 7 therefore requires PSPs to proactively monitor the threat landscape and to acquire and make effective use of actionable threat intelligence to validate its risk assessments, processes, procedures and controls, with a view to building strong security measures.

33. Guideline 7 also stresses the importance of a PSP's active participation in information-sharing arrangements and collaboration with external stakeholders. In fostering strong situational awareness, the PSP should also implement an adaptive operational and security risk management framework that evolves with the dynamic nature of risks to enable effective management of those risks. Achieving this will require PSPs to instil a culture of continuous learning and security awareness and demonstrate ongoing re-evaluation and improvement of their security posture at every level within the organisation.

Question 8: Do you agree with the proposed Guideline 7 on Situational awareness and continuous learning? If not, please provide your reasoning.

34. Lastly, Guideline 8 on *PSU relationship management* stipulates that, in implementing the security measures, the PSP also has a responsibility to its PSUs, who are the most critical stakeholders in the overall process. Strengthening the PSUs' understanding of the security measures, enhancing their understanding of the threats and vulnerabilities, and establishing effective channels of communication with the PSP, will improve the overall security of the ecosystem and potentially reduce risks to and from the PSPs. The section on external relationship management sets out the steps a PSP must take to improve the situational awareness of its user base, and the reporting mechanisms that should be in place to facilitate this overall process.

Question 9: Do you agree with the proposed Guideline 8 on PSU relationship management? If not, please provide your reasoning.

35. Finally, EBA is of the view that, in the context of the provision of acquiring services, aspects related to the storing, processing or transmitting of sensitive payment data by payees could be addressed taking into account the security measures specified in these guidelines, however being applicable as requirements only to PSPs as such.

Question 10: Do you consider the extent of the requirements proposed in the Guidelines to be sufficient and clear? If not, please provide your reasoning.

5. Draft Guidelines

Draft Guidelines

on the security measures for operational and security risks of payment services under PSD2

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains draft guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/20108. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.

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

Reporting requirements

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

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

[8] 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 definition

Subject matter

5. These Guidelines derive from the mandate given to EBA in Article 95(3) of Directive (EU) 2015/2366[9] (PSD2).

6. These Guidelines define requirements for the establishment, implementation and monitoring of security measures that payment service providers (hereinafter PSPs), in accordance with Article 95 of the PSD2, shall adopt to manage the current and future operational and security risks relating to the payment services they provide.

Scope of application

7. These Guidelines apply in relation to the establishment, implementation and monitoring of the security measures for operational and security risks, including certification processes, by payment service providers for the provision of payment services.

8. The Guidelines are subject to the principle of proportionality, which means that all PSPs are required to be compliant with each Guideline, but the precise steps that they are required to take to be compliant may differ between PSPs, depending on their size, business model and complexity of their activities.

Addressees

9. These Guidelines are addressed to payment service providers 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 competent authorities as defined in point (i) of Article 4(2) of that Regulation by reference to the PSD2.

Definitions

10. 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; - For PSPs other than credit institutions, this term means 'directors or persons responsible for the management of the PSP, with decision-making power on the overall strategy, objectives and direction of the PSP, or with power to effectively direct its business.'

[9] 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 (PSD2).

'Senior management'	- 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; - For PSPs other than credit institutions, this term means 'natural persons who exercise executive functions within a PSP and who are responsible, and accountable to the management body, for the day-to-day management of the PSP.
'Security risk'	- The risk resulting from inadequate or failed internal processes or external events affecting availability, integrity, confidentiality of Information and Communication Technology (ICT) systems and/or information used for payment services. This includes risk from cyber-attacks or inadequate physical security.

Implementation

11. These guidelines apply from 13 January 2018.

3. Guidelines

Guideline 1: Governance

Operational and security risk management framework

1.1 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 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.

1.2 The risk management framework should:

a) include a comprehensive security policy, which sets the risk appetite of the PSP, its security objectives and measures;

b) 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;

c) establish the necessary procedures and systems to identify, measure, monitor and manage the range of risks stemming from the provision of payment service and to which the PSP is exposed to.

1.3 PSPs should ensure that the risk management framework is properly documented and reviewed on an ongoing basis, by the management body and where relevant, by the senior management, and updated with 'lessons learned' during its 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.

1.4 PSPs should ensure that before a major change of infrastructure, processes or procedures and after each major incident affecting the security of provision of payment services, they review whether changes or improvements to the risk management framework are needed.

Risk management and control models

1.5 PSPs should ensure that they have 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.

1.6 The security measures set out in the Guidelines should be audited by internal or external independent and qualified auditors 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 experts should be

involved in any way in the development, implementation or operational management of the payment services provided.

Outsourcing

1.7 PSPs should ensure the effectiveness of the security measures to mitigate the operational and security risks in the provision of payment services that are outsourced.

1.8 PSPs should ensure that appropriate and proportionate security objectives, measures and performance targets are built into contracts and service level agreements with their outsourcing providers for the provision of payment services. PSPs should monitor and seek assurance on the outsourcing providers' level of compliance with the security objectives, measures and performance targets.

Guideline 2: Risk assessment

Identification of functions, processes and assets

2.1 PSPs should identify, establish and regularly update an inventory of their business functions, critical human resources (especially those with privileged system access or performing sensitive business functions), and supporting processes in order to map the importance of each function and supporting processes, and their interdependencies related to operational and security risks in the provision of payment services

2.2 PSPs should identify, establish and regularly update an inventory of the information assets used for the provision of payment services, such as systems, their configurations, other infrastructures and also the interconnections with other internal and external systems, in order to know the critical assets that support their business functions and processes for the provision of payment services.

Classification of functions, processes and assets

2.3 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 which have been detected in the provision of payment services.

Risk assessments of functions, processes and assets

2.4 PSPs should ensure that they continuously monitor threats and vulnerabilities and regularly review the risk scenarios impacting their assets, critical processes and business functions. PSPs should carry out and document risk assessments of the functions, processes and assets they have identified and classified in order to identify and assess key operational and security risks for the provision of payment services. Assets, processes and functions should be prioritised according to their criticality.

2.5 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 security incidents, fraud and potential disruptive effects in the provision of payment services and to their payment service users.

Guideline 3: Protection

3.1 PSPs should establish and implement preventive security measures against identified operational and security risks. These measures should ensure an adequate level of security according to the risks identified.

3.2 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.

3.3 PSPs should protect 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 payment service users against abuse, attacks and inappropriate access and theft.

3.4 On an ongoing 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 for the risk involved. These changes should be part of the PSP's formal change management process ensuring 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.

Data and Systems Integrity and Confidentiality

3.5 PSPs should implement measures to protect sensitive data, including sensitive payment data, user data, personalised security credentials and certificates from unauthorized disclosure or modification, whether at rest or in transit. PSPs should protect their critical resources from unauthorised access or modification. Integrity checking mechanisms should be deployed by PSPs in order to verify the authenticity and integrity of software, firmware, and information.

3.6 In designing, developing and maintaining payment services, PSPs should ensure that segregation of duties and "least privilege" principles are applied. PSPs should pay special attention to the segregation of information technology environments, in particular to the development, testing and production environments.

3.7 In designing, developing and maintaining payment services, PSPs should ensure that data minimisation is an essential component of the core functionality: the gathering, routing, processing, storing and/or archiving, and visualisation of sensitive data should be kept at the absolute minimum level.

3.8 Upon access to the payment service, PSPs should check that the software used for the provision of payment services is up to date.

Physical security

3.9 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. Physical access to corresponding systems should be limited to authorised personnel only and regularly reviewed.

Access control

3.10 Physical and logical access to systems should be permitted only for individuals who are authorised by the management body or, where relevant, by senior management; authorisation should be assigned according to 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 systems to those with a legitimate business requirement. Electronic access by applications to data and systems should be limited to the minimum possible.

3.11 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.

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

3.13 The operation of products and tools 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 4: Detection

Continuous monitoring and detection

4.1 PSPs should establish and implement processes and capabilities to continuously monitor and detect anomalous activities and events in the provision of payment services. As part of this continuous monitoring, PSPs should have appropriate and effective intrusion detection capabilities in place.

4.2 The continuous monitoring and detection processes should cover relevant internal and external factors, including business line and IT administrative functions and transactions in order to detect misuse of access by service providers or other entities, potential insider threats and other advanced threat activities.

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

Monitoring and reporting of security incidents

4.4 PSPs should determine appropriate definitions, thresholds and early warning indicators for classifying an event as a security incident in the provision of payment services.

4.5 PSPs should establish appropriate processes and organizational structures to ensure the consistent and integrated monitoring, handling and follow-up of security incidents.

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

Guideline 5: Business continuity

Business continuity management

5.1 PSPs should establish a sound Business Continuity Management to ensure their ability to provide payment services on an on-going basis and to limit losses in the event of severe business disruption.

5.2 In order to establish a 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 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.

5.3 On the basis of the above analysis, a PSP should put in place:

a) contingency and business continuity plans to ensure a PSP reacts appropriately to emergencies and is able to maintain its most important business activities if there is a disruption of its ordinary business procedures; and

b) mitigation measures to be adopted by the PSP in case of termination of its payment services, to avoid adverse effects on payment systems and on payments services users ensuring execution of pending payment transactions and termination of existing contracts.

Scenario based business continuity planning

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

5.5 Based on the analysis carried out under Guideline 5.1 and plausible scenarios identified under Guideline 5.4, the PSP should, where appropriate for the size, business model and complexity of their activities, develop a set of response and recovery plans, which should:

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

b) be clearly documented. The documentation should be available within the business and support units and stored on systems that are physically separated and readily accessible in case of emergency.

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

Testing of Business Continuity Plans

5.6 The PSP should test its business continuity plans, and ensure that the operation of its critical functions, processes, systems, transactions and interdependencies are tested at least annually. The plans should support objectives to protect and, if necessary, re-establish integrity and availability of its operations, and the confidentiality of its information assets according to the PSP's size, business model and complexity of the activities;

5.7 Plans should be regularly updated based on testing results, current threat intelligence, information-sharing and lessons learned from previous events, changing recovery objectives, as well as analysis of operationally and technically plausible scenarios that have not yet occurred. The PSP should consult and coordinate with relevant internal and external stakeholders during the establishment of its business continuity plans.

5.8 The PSP's testing of its business continuity plans should:

a) include a broad range of scenarios, including simulation of extreme but plausible ones;

b) be designed to challenge the assumptions of business continuity practices, including governance arrangements and crisis communication plans; and

c) include procedures to verify the ability of its staff and processes to respond to unfamiliar scenarios.

5.9 The PSP should periodically monitor the effectiveness of its business continuity plans, and document and analyse any challenges or failures resulting from the tests.

Incident management and crisis communication

5.10 In the event of a disruption or emergency, and during the implementation of the business continuity plans, the PSPs should ensure it has 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.

Guideline 6: Testing of security measures

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

6.2 The PSP should ensure that tests are conducted to assess the robustness and effectiveness of the security measures in cases of changes to the infrastructure and procedures and changes resulting from major incidents.

6.3 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.

6.4 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 that 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.

6.5 PSPs should perform ongoing and repeated tests of the security measures for its payment services. For critical systems (as described in GL 2.2), these tests shall be performed at least on an annual basis.

6.6 PSPs should monitor and evaluate the results from the tests conducted, and update its security measures accordingly.

Guideline 7: Situational awareness and continuous learning

Threat landscape and situational awareness

7.1 PSPs should establish and implement processes and 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 or have occurred within and/or outside the organisation, and updating the security measures accordingly.

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

Training and security awareness programs

7.3 PSPs should ensure that all their personnel 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.

7.4 PSPs should ensure that critical personnel identified under GL 2.1 receive targeted information security training.

7.5 PSPs should establish and implement security awareness programmes in order to educate their personnel and to address information security related risks to the provision of payment services. These programs should require their personnel to report any unusual activity and incidents.

Guideline 8: PSU relationship management

Payment service user awareness on security risks

8.1 PSPs should establish and implement processes to enhance the awareness of PSUs to security risks linked to the payment services through assistance and guidance to the PSUs.

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

8.3 PSPs should also ensure that PSUs are provided, on an ongoing or, where applicable, ad hoc basis, and via appropriate means, with clear and straightforward instructions explaining their responsibilities regarding the secure use of the service.

8.4 PSPs should allow PSUs to disable specific payment functionalities.

8.5 Where, in accordance with PSD2 article 68 (1), PSP has agreed with the payer on spending limits for payment transactions executed through payment instruments or where a PSP has defined spending limits for specific payment services, the PSP should provide the payer with options to reduce these limits.

8.6 PSPs should provide the possibility for PSUs to set alerts related to the initiation, the execution and failed attempt to initiate a payment transaction, in the context of the PSU profile management services platform provided to the PSU, where relevant.

PSU secure communication and reporting procedures

8.7 The PSP should inform PSUs on the reporting procedure for suspected security breaches, in particular:

a) the procedure for PSUs to report to the PSP suspicious incidents or anomalies during the payment services session;

b) how the PSP will respond to the PSU; and

c) how the PSP will notify the PSU about (potential) security breaches or the non-initiation of payment transactions, or warn the PSU about the occurrence of attacks.

8.8 The PSP should keep PSUs informed about updates in security procedures regarding payment services. Any alerts about significant emerging risks should also be provided via a secured channel.

8.9 The PSP should provide the PSU with assistance on all questions, complaints, requests for support and notifications of anomalies or incidents regarding internet payments and related services. PSUs should be appropriately informed about how such assistance can be obtained.

8.10 PSPs should set out the method and terms of the PSU notification, in case PSP has blocked a specific transaction or payment instrument, and define how the PSU can contact the PSP to have the payment transaction or payment instrument 'unblocked'.

6. Accompanying documents

6.1 Draft 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 European Banking Authority (EBA), in coordination with the European Central Bank (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 payment service providers (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 annex contains the impact assessment on PSPs, payment service users (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 of 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 continuous changes raise concerns about the current trend of rising frauds, especially, but not limited to, in the field of internet payments.[10]

The risk analysis exercise conducted by the EBA and the ECB has identified various threats and vulnerabilities, which PSPs are currently exposed to 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.

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

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 against with the current security systems in place.

User of payment services are further increasingly concerned about the security along the payment process. The level of consumer awareness about potential (cyber) risks and about consumer protection measures available in the payment sector is low.11 Lower user confident affects the payment systems because the perception of failing payment security affects the way in which consumers make payment choices. As consumer confidence in specific payment instruments is undermined, they 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. Financially little literate and unsophisticated users further facilitate the work of fraudster 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, which is reflected in the current unequal occurrences of online banking fraud between Member States.

To address these issues, the draft Guidelines proposed in this Consultation Paper (CP) 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 CP introduces eight draft 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 to enhance regulatory and supervisory convergence and to protect users of payment services in the EU[12] by ensuring that PSPs' security measures are established, implemented and monitored consistently, efficiently and effectively across the European Union.

[11] European Commission (2015): Special Eurobarometer 423 – Cyber Security Report, February 2015, http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf.

[12] EBA Work Programme (2017), https://www.eba.europa.eu/about-us/work-programme/current-work-programme.

More specifically, these Guidelines aim to help PSPs to insure integrity, availability, confidentiality, authenticity and continuity of payment-related services and avoid incidents during the payment service process. They further aim to help them avoiding 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 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 forms of incidents.

C. Options considered and preferred option

To improve the overall resilience of PSPs against operational and systemic risks, PSPs security systems shall cover eight elements. 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, 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 operational and security systems 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 the 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 PSPs in the way how they establish, implement and monitor their security systems 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 the PSPs' security system. Accordingly, PSPs will need to establish systems that allow to monitor and to analyse all of their processes and occurred incidents and to anticipate possible threats and the environment it operates in. PSPs are further required to set sound response and recovery arrangement and to set systems which allow the efficient exchange of information with other PSPs which are/could be exposed to the same risks.

The security and reporting systems which PSPs will need to have are expected to raise one–off implementation costs to set up the technical, personal and administrative processes. Relating to the continuous monitoring exercise, it is expected that PSPs will need further staff which will operate the new security systems and ensures continuous adaption of the technology.

Prior to the adaption of the 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, [13] which came into force on the 1st of August 2015, and the ECB Recommendations for the security of internet payments,[14] 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 the 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 their operations by aiming to ensure that their services are not interrupted and provided by the guaranteed standards. This avoids costs stemming from fallout of the services, reconciliation and loss in reputation.

PSUs will benefit from the requirements as it decreases 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 adaption of these draft Guidelines will prevent the occurrence of incidents and will in the long run discourage fraudster from future actions. This will lead to the strengthening of the payment system and the use of money.

[13] 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.
[14] 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.

6.2 Overview of questions for consultation

Question 1: Do you agree with the level of detail set out in the Guidelines as proposed in this Consultation Paper or would you have expected more or less detailed requirements on a particular aspect of the Guidelines? If not, please provide your reasoning.

Question 2: Do you agree with the proposed Guideline 1 on Governance? If not, please provide your reasoning.

Question 3: Do you agree with the proposed Guideline 2 on Risk assessment? If not, please provide your reasoning.

Question 4: Do you agree with the proposed Guideline 3 on Protection? If not, please provide your reasoning.

Question 5: Do you agree with the proposed Guideline 4 on Detection? If not, please provide your reasoning.

Question 6: Do you agree with the proposed Guideline 5 on Business continuity? If not, please provide your reasoning.

Question 7: Do you agree with the proposed Guideline 6 on Testing of security measures? If not, please provide your reasoning.

Question 8: Do you agree with the proposed Guideline 7 on Situational awareness and continuous learning? If not, please provide your reasoning.

Question 9: Do you agree with the proposed Guideline 8 on PSU relationship management? If not, please provide your reasoning.

Question 10: Do you consider the extent of the requirements proposed in the Guidelines to be sufficient and clear? If not, please provide your reasoning.