Public Hearing on the CP on the Guidelines on the security measures for operational and security risks of payment services under PSD2

Laura Diez Perez, European Banking Authority
Chrissanthos Tsiliberdis, European Central Bank

Public Hearing, EBA, London, 20 June 2017

Agenda

1. **Introduction to the EBA**
   - > The creation of the EBA, and its scope of action
   - > Legal instruments and output to date
   - > Mandates conferred on the EBA under the PSD2
   - > The purpose of public hearings
2. **The mandate in PSD2, and the approach taken by the EBA & ECB**
   - > The wording of the mandate in PSD2
   - > Approach taken by EBA and ECB
3. **Guidelines as proposed in the CP**
   - > Subject matter, scope and definitions
   - > Structure
   - > Substance of the requirements
   - > Next steps

Introduction to the EBA

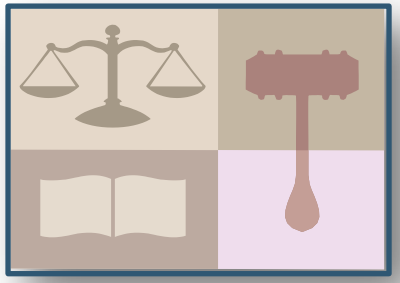
The creation of the EBA

- The EBA was established by Regulation (EC) No. 1093/2010 of the European Parliament and EU Council;
- came into being on 1 January 2011;
- took over all existing tasks and responsibilities from the Committee of European Banking Supervisors (CEBS);
- took on additional tasks, incl. consumer protection, the monitoring of financial innovation, and payments;
- is an independent authority;
- is accountable to the EU Parliament and Council;
- has as its highest governing body the EBA Board of Supervisors, comprising the Heads of the 28 national supervisory authorities.

Legal instruments available to the EBA

The EBA has different types of legal instruments at its disposal that differ in terms of purpose, legal status, and possible addressees.

- Technical standards
- Guidelines and recommendations
- Opinions / Technical Advice
- Warnings
- Temporary prohibitions
- Joint Positions
- Breach of Union law investigations
- Binding and non-binding mediation



The EBA's scope of action

The EBA's regulatory remit is defined by the EU Directives and Regulations that fall into its 'scope of action', either because they are listed in the EBA's founding regulation or because they confer tasks on the EBA. They include:

- Capital Requirements Directive (CRR/D IV)
- Deposit Guarantee Scheme Directive (DGSD)
- Mortgage Credit Directive (MCD)
- Payment Accounts Directive (PAD)
- Electronic Money Directive (EMD)
- Payment Services Directive (PSD1 + forthcoming PSD2)
- Anti–Money Laundering Directive (AMLD)
- Markets in Financial Instruments Directive (MiFID/R, for structured deposits)

Output of the EBA to date

Since its creation in 2011, the EBA has issued more than 200 legal instruments, plus more than 100 reports and other outputs.

	2011	2012	2013	2014	2015	2016	Total
Regulatory Technical Standards	-	1	39	22	15	15	92
Implementing Technical Standards	-	-	21	10	10	7	48
Guidelines	2	6	2	17	19	12	58
Opinions / Technical Advice	1	6	6	14	21	17	65
Published reports	6	12	26	23	34	37	138
Recommendations	2	-	4	1	2	1	10
Breach of Union Law investigations	-	-	-	1	-	-	1
Mediations	-	2	5	-	-	-	7
Peer reviews	-	-	1	1	1	2	5
Warnings	-	-	2	-	-	-	2
Stress tests	1	-	1	-	1	1	4

Progress of PSD2 Mandates

The purpose of EBA public hearings

For many of its Technical Standards and Guidelines the EBA organises 'public hearings, with a view to allow interested parties to ask clarification questions.

- **An EBA hearing takes place during the consultation period, usually a month or so before the submission deadline of responses to the Consultation Paper (CP).**

- **The purpose of the hearing is for the EBA to present a summary of the CP, re-produce the questions of the CP, and asks attendees whether they require additional explanations or clarifications from the EBA so as to be able to answer the questions in the CP.**

- **The public hearing does therefore not replace written responses to the CP, as it is only through written responses that the EBA is able to give the views of stakeholders the required consideration.**

The mandate in PSD2, and the approach taken by EBA and ECB

The wording of the mandate in PSD2

Article 95(3) of PSD2 confers on the EBA the following mandate:

"By 13 July 2017, EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, 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.

EBA shall, in close cooperation with the ECB, review the guidelines referred to in the first subparagraph on a regular basis and in any event at least every 2 years."

Approach to the development of the Guidelines

Existing requirements that were used as input for the EBA Guidelines

EU

- EBA Guidelines on the Security of Internet Payments
- Earlier SecuRe Pay Guidance issued on security of mobile payments and payment accounts access
- EU Network and Information Systems (NIS) Directive;

Beyond EU

- BCBS principles on operational risk;
- US NIST Framework; and,
- CPMI-IOSCO Guidance on cyber resilience for FMIs.

Main threats and vulnerabilities for PSPs

The EBA & ECB carried out a comprehensive risk analysis in order to understand and identify the threats and vulnerabilities to which PSPs are exposed to.

- Inadequate protection of communication channels used for payments;
- Inadequately secured systems and devices including but not limited to applications, servers, user's payment devices;
- Unsafe behaviour of users of PSPs staff;
- Increased complexity of the payments environment; and,
- Technological advancements and tools that are available to potential fraudsters or malicious attackers.

Main findings of the risk assessment

- The RA concluded that the type and nature of PSP security threats and vulnerabilities are evolving rapidly
- The Guidelines should remain flexible so they can be adaptable to the changing risk landscape.
- 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;
- PSPs should mitigate risks resulting from inadequate or failed internal processes and systems, inappropriate people's behaviour or from external events; and,
- The security measures should be fully integrated into their overall risk management processes and constantly monitored:
  - periodic reviews and effective reporting mechanisms should be implemented
  - Compliance with the policies and procedures should be continuously monitored

Subject matter, scope and definitions

- The guidelines set out requirements on security measures for PSPs to mitigate operational and security risks derived from the provision of payment services;
- 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.
- Definitions on “management body” and “senior management” are provided based on existing Directive.
- A new definition on “security risk” has been introduced in the Guidelines:
  - **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.*
- A definition on “operational risk” is not provided due to the fact that there are already definitions in other EU/International regulations (e.g. EBA GL, BCBS)
- A definition on “security measures” is not provided since it is a term widely used in the PSD2 and could led to legal risks;

Structure of the Guidelines

- Given the mandate and the input derived from the documentation review and risk analysis, EBA decided to encapsulate requirements for security measures into 8 different guidelines:

Guideline	Tittle
GL 1	Governance
GL 2	Risk assessment
GL 3	Protection
GL 4	Detection
GL 5	Business Continuity
GL 6	Testing of security measures
GL 7	Situational awareness and continuous learning
GL 8	PSU relationship management

Structure of the Guidelines (cont.)

- The additional categories on testing, situational awareness and continuous learning have been added, to ensure that the PSP is:
  - ✓ continually monitoring internal and external developments,
  - ✓ adapting its security framework to mitigate emerging risks, threats and vulnerabilities
  - ✓ Continuously testing the effectiveness of the framework as a whole.

- The 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 security measures are well communicated to their user base, to reduce risks to and from them.

- An effective framework should:
  - ✓ consist of the eight categories
  - ✓ the requirements within each category should prescribe the establishment of the appropriate roles and responsibilities, structures, systems, policies and procedures with regard to the necessary security measures.

Q1: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.

Guideline 1: Governance

- The requirements on the Guideline 1 on Governance are divided into three groups:
  - Operational and security risk management framework
  - Risk management and control models
  - Outsourcing

Main requirements:

- Mainly refer to the arrangements a PSP should put in place to establish, implement and monitor its approach to managing effectively operational and security risks.
- PSPs should implement a clear and comprehensive operational and security risk management framework which is supported by clearly defined roles and responsibilities, guided by security objectives which are proportional to the underlying risks.
- Implement three lines of defence, or an equivalent internal risk management and control model, to identify and manage operational and security risks.
- Ensure security objectives, measures and performance targets are build into contracts and SLA with the outsourcing providers.

Q2: Do you agree with the proposed Guideline 1 on Governance? If not, please provide your reasoning.

Guideline 2: Risk assessment

- The requirements on Guideline 2 Governance are divided into three groups:
  - Identification of functions, processes and assets
  - Classification of functions, processes and assets
  - Risk assessments of functions, processes and assets

Main requirements:

- PSPs should identify, establish and regularly update and inventory of their business functions […], critical human resources and supporting processes in order to map the its importance […] and their interdependencies related to operational and security risks.
- The inventory of information assets for the provision of payment services should be mapped as well considering the interconnections with other internal and external systems.
- PSPs should classify the identified business functions, supporting processes and information assets in terms of criticality.
- 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.

Q3: Do you agree with the proposed Guideline 2 on Risk assessment? If not, please provide your reasoning.

Guideline 3: Protection

- Guideline 3 on Protection is divided into three groups:
  - Data and systems Integrity and Confidentiality
  - Physical security
  - Access control

Main requirements:

- PSPs should establish and implement a 'defence-in-depth' approach by instituting a multi-layered controls covering people, processes and technology.
- implement measures to protect sensitive data, including sensitive payment data, user data, personalised security credentials and certifications from unauthorised disclosure or modification.
- ensure that segregation of duties and the "least privilege" principles are applied.
- Ensure that physical access to corresponding systems should be limited to authorised personnel only and regularly reviewed.
- Authorisation should be granted by management body, or where relevant by senior management and should be assigned according to the staff's talks and responsibilities.

Q4: Do you agree with the proposed Guideline 3 on Protection? If not, please provide your reasoning.

Guideline 4: Detection

- The requirements on Guideline 4 Detection are divided into three groups:
  - Continuous monitoring and detection
  - Monitoring and reporting of security incidents
  - Risk assessments of functions, processes and assets

Main requirements:

- PSPs should establish and implement processes and capabilities to continuously monitor and detect anomalous activities.
- The detection process should cover relevant internal and external factors […]
- determine appropriate definitions, thresholds and early warning indicators for classifying and event as a security incident.
- Other issues covered in this Guideline include the handling and follow-up of security incidents, reporting procedures related to customer complaints to its senior management.

Q5: Do you agree with the proposed Guideline 4 on Detection? If not, please provide your reasoning.

Guideline 5: Business continuity

- Guideline 5 on Business Continuity is divided into three groups:
  - Business continuity management
  - Scenario based business continuity planning
  - Testing of Business Continuity Plans

Main requirements:

- Establishment of a sound Business Continuity Management framework in the PSP
- Develop and implement contingency and business continuity plans to ensure appropriate reaction to emergencies and mitigation measures to be adopted in case of termination of its payment services.
- Develop a range of different extreme but plausible scenarios to which the PSP might be exposed, and assess the potential impact.
- Where appropriate for the size, business model and complexity of their activities, PSPs should develop a set of response and recovery plans […]
- Testing of the business continuity plans, and ensure that the operation of its critical functions, processes, systems, transactions and interdependencies are tested at least annually.
- Plans should be updated based on testing results, current threat intelligence information-sharing and lessons learned.

Q6: Do you agree with the proposed Guideline 5 on Business continuity? If not, please provide your reasoning.

Guideline 6: Testing of security measures

Main requirements:

- Guideline 6 on Testing of security measures requires that PSPs should establish and implement a testing framework that validates the robustness and effectiveness of the security measures and that is adapted considering new threats and vulnerabilities.
- The Guideline 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.
- It requires PSPs to conduct tests in cases of changes to the infrastructure and procedures and changes resulting from major incidents.
- Tests should
    - performed as part of the PSPs' formal change management process;
    - be carried out by independent testers not involved in the development of the security measures; and
    - include vulnerability scans and penetration tests adequate to the level of risk identified.

Q7: Do you agree with the proposed Guideline 6 on Testing of security measures? If not, please provide your reasoning.

Guideline 7 : Situational awareness & learning

- Guideline 7 on Situational awareness and continuous learning is divided into two groups:
  - Threat landscape and situational awareness
  - Training and security awareness programs

Main requirements:

- strong situational awareness 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.
- 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.
- 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 that can be achieved by instilling a culture of continuous learning and security awareness.

Q8: Do you agree with the proposed Guideline 7 on Situational awareness and continuous learning? If not, please provide your reasoning.

Guideline 8 : PSU relationship management

- Guideline 8 is divided into two groups:
  - Payment service user awareness on security risks
  - PSU secure communication and reporting procedures

Main requirements:

- This Guideline 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 strengthen the PSUs' understanding of the security measures, enhance their awareness to security risk linked to the payment services through assistance and guidance, ensure their understanding of the threats and vulnerabilities.
- Ensure that PSPs have a process in place to inform PSUs on the reporting procedure for suspected security breaches and the procedure for blocking /unblocking of specific transactions.

Q9: Do you agree with the proposed Guideline 8 on PSU relationship management? If not, please provide your reasoning.

Next steps

- **7 August 2017:** Consultation period ends;
- **Q3/Q4 2017:** EBA assesses CP responses to decide which, if any, changes will be made to the Guidelines before finalization;
- **Q4 2017:** EBA will publish the Final Guidelines, in English language. The Guidelines will be part of a 'Final Report', which will also contain a 'feedback table' that lists all concerns raised by respondents, and the EBA's assessment of whether changes were required;
- **Dec 2017:** EBA will publish the translations in all official EU languages. National authorities will then have two months to submit to the EBA compliance notifications stating whether or not they comply
- **13 January 2018:** Guidelines apply