Public Hearing

Consultation Paper (CP) on Guidelines on ICT and security risk management

13 February 2019

1. **Introduction and Welcome –** Slavka Eley – Head of Banking Markets, Innovation and Products Unit
2. **Overview of the Draft Guidelines-** Michiel Le Comte, Head of IT supervision and Operational risk, DNB and Co Chair of Task Force on IT risk supervision, EBA and Nicola Yiannoulis, Policy Expert, Banking Markets, Innovation and Products Unit
3. **Questions and Comments**
4. **Close**

CP on Guidelines on ICT and security risk management

Michiel Le Comte, Head of IT supervision & Operational risk and Co-chair of EBA Task Force on IT risk supervision, De Nederlansche Bank

Nicola Yiannoulis, Policy Expert, Banking markets, innovations and products, EBA

Public Hearing – 13 February 2019

Guidelines for ICT and security risk management

Background to the development

- ICT risks including security risks are increasing.
- Article 95 PSD2 recognises the need for security measures for payment services.
- ICT risks including security are not only relevant for payment services.
- The 'GLs on security measures for operational and security risks' published by EBA in Dec 2017 are not only relevant for PSPs. They apply to credit institutions for their payment services however other activities and investment firms are out of scope.
- Option to create a new set of GLs was considered but would have resulted in overlap of requirements and confusion.
- New set of GLs developed which integrate the 'GLs on security measures' and will repeal them when these GLs become applicable.

Guidelines

Addressees:

PSPs for their payment services

Credit institutions and Investment firms for all activities

Collectively 'financial institutions'

Legal basis:

Article 74 CRD on Internal Governance (own initiative)

Article 95 PSD2 on the management of operational and security risks. (mandate for GLs)

Also, request from EC FinTech Action Plan for Guidelines.

Scope of Application:

Measures to mitigate ICT risks including security risks

Art 95 PSD2 mandate for GLs on security measures of operational and security risks => Operational risks for payment services relate to those over electronic systems and security risks for payment services relate to the security of the technology. Therefore for purposes of these guidelines, the term 'ICT risks' is used.

Content

1. **Proportionality** –Ensuring a proportionate application.
2. **ICT governance and strategy** –management body buy-in for mitigating ICT risks from the top and having a clear strategy in place.
3. **ICT Risk Management framework** –risk management organisation and process.
4. **Information security** –establishment of strong security measures, testing, awareness and training this section implicitly covers cybersecurity as a part of information security.
5. **ICT Operations management** –logging and monitoring procedures for critical ICT operations, ICT asset inventory and incident and problem management process.
6. **ICT Project and Change management** –acquisition, development and changes to ICT systems.
7. **Business continuity management** –BCP and recovery and response planning, testing and crisis communications.
8. **Payment service user relationship management** - applies only to PSPs – wording unchanged from GLs on security measures.

Changes from Guidelines on security measures under PSD2

Guidelines on security measures for operational and security risks
1. General Principle
2. Governance
Operational and security risk management framework
Risk management and control models
Outsourcing
3. Risk assessment
Identification of functions, processes and assets
Classification of functions, processes and assets
Risk assessment of functions, processes and assets
4. Protection
Data systems integrity and confidentiality
Physical security
Access control
5. Detection
Continuous monitoring and detection
monitoring and reporting of operational or security incidents
6. Business continuity
Scenario based continuity planning
Testing of business continuity plans
Crisis communication
7. Testing of security measures
8. Situational awareness and continuous learning
Threat landscape and situational awareness
Training and security awareness programmes
9. Payment service user relationship management
Payment services user awareness on security risks and risk-mitigating actions

- Fully mapped into new Guidelines
- Consulted with drafters of original guidelines
- Changes include new structure and additional, relevant but proportional requirements.
- No new topics

Guidelines on ICT and security risk management
1. Proportionality
2. ICT governance and strategy
Governance
Strategy
Use of third party providers
3. ICT risk management framework
Organisation and objectives
Identification of functions, processes and assets
Classification and risk assessment
Risk Mitigation
Reporting
Audit
4.Information security
Information security policy
Information security function
Logical security
Physical security
ICT operations security
Security monitoring
Information securit reviews and testing
Information security training and awareness
5. ICT operations management
ICT incident and problem management
6. ICT project and change management
ICT project management
ICT systems acquisition and development
ICT change management
7. Business continuity management
Business Impact Analysis
Business continuity planning
Response and recovery plans
Testing of plans
Crisis communication
8. Payment service user relationship management

Next steps

- February 2019 – public hearing
- 13 March 2019– public consultation close
- End Sept 2019 (anticipated) – final publication
- 6 months after publication (estimated) – GLs become applicable and GLs on security measures are repealed.

EUROPEAN BANKING AUTHORITY

Floor 46, One Canada Square, London E14 5AA

Tel: +44 207 382 1776
Fax: +44 207 382 1771

E-mail: info@eba.europa.eu
http://www.eba.europa.eu