Guidance Payment Service Directive 2

Practical guidance for Internal Auditors on the annual audit of PSD2 related to strong customer authentication and common and secure communication and security measures for operational and security risks

Version 1.2

March 2023

Table of Contents

Version control

Version	Date	Explanation
Version 1.0	25 April 2022	Send to NOREA
Version 1.1	7 June 2022	Adjustment based on NOREA feedback
Version 1.2	30 March 2023	Update Guidelines on security measures for operational and security risks under the PSD2

1. Introduction

This document contains practical audit guidance for the audit of PSD2 (i.e. Payment Service Directive 2). The guidance is based on the Regulatory Technical Standards and Guidelines that are related to PSD2 and is focussed on the following two RTS and guideline in particular:

1) Regulatory technical standards for strong customer authentication and common and secure open standards of communication (2018/389); and
2) Guideline on the security measures for operational and security risks of payment services under Directive (EBA/GL/2017/17).

In this guidance, a control matrix is presented which describes the steps to be taken in order to carry out a PSD2 audit. The following phases are taken into account: scoping, risk assessment, planning, fieldwork and reporting phases.

As a result of the PSD2 legislation, a PSD2 manual was issued earlier. This was aimed at the guideline (Regulatory Technical Standard) for Strong Customer Authentication. In this second MVP, guidance about security measures for operational and security risks has been added.

2. Control matrix

During several meetings from November 2021 through March 2022, representatives of the Workgroup Payments Services of NOREA discussed the required audit approach for PSD2, i.e. Payment Service Directive 2. The main goal was to improve the available standardised and pragmatic audit approach. The renewed approach should meet regulatory requirements and should be supported by financial institutions involved. Furthermore it should be useable for all institutions –in PSD2 terminology: ASPSPs, i.e. Account Servicing Payment Servicing Providers – that were not involved in those discussions. The result as described in this document is a structure that offers flexibility of approach and re-use of previously planned audit activities. The approach can easily be adjusted – if so required – to meet ever changing regulations. We focus on the requirements for security measures for operational and security risks and strong customer authentication as these have been set in 2017 respectively 2019 by the European Banking Association which are an essential part of the new PSD2 requirements. The proposed audit approach can easily be translated to other EBA guidelines for PSD2 which together should support fulfilment of audit requirements[1]. The EBA guidance on PSD2 is being finetuned continuously. Therefore we recommend to monitor PSD2 developments to ensure that the right audit activities are performed.

The practical guidance as described in this document consists, in addition to this document, of two other documents, namely

- PSD2 Practical guidance worksheet, this concerns an Excel list in which the framework of standards of the two guidelines are displayed, namely: Regulatory technical standards for strong customer authentication and common and secure open standards of communication and Guidelines on the security measures for operational and security risks; and
- PSD2 presentation, which contains an explanation of PSD2 and which RTS and guidelines are subject to PSD2.

3. Standard control matrix

This chapter describes the control matrix. The control matrix describes the audit approach focused on the scoping of the audit, risk assessment, planning, fieldwork and reporting phases. Beginning with scoping, the scoping describes which topics can be considered before the PSD2 audit can be started.

[1] See Annex 1 – Relevant guidelines. In this Annex you find the EBA 'Regulatory technical standard for strong customer authentication and common and secure open standards of communication', the PSD2 Directive and other relevant guidelines.

Notes on scoping:

- The practical guidance has been set up referring to audit activities in the Netherlands. When successfully adopted in the Netherlands, expansion of geographical scope could be considered;
- Focus is on PSD2 shared services (APIs and API gateway(s) and others, versus local sourcing systems);
- Assurance is not explicitly required by the RTS, unless specifically mentioned (e.g. fall back exemption);
- Design, implementation and operating effectiveness aspects should be given appropriate attention following the risk assessment results. Specific underlying audit approaches can be chosen by the auditor;

Risk assessment

Payment service providers 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 overall risk management processes.

Based on the audit approach, a 'standard control matrix' has been defined which can be used by internal auditors as a tool to identify audit activities to be done and performed. We have added the practical guidance as part of the control matrix regarding the Guidelines on SCA and security, see here for the Excel file PSD2 Practical guidance worksheet.

Planning

For the planning and risk assessment purpose, a standard control matrix is defined for the internal auditor. Underlying principle of using the control matrix PSD2 is that the potential large amount of required PSD2 audit activities is executed in the most efficient and effective way. Audit activities can be planned based on a multi-year schedule (see standard control matrix), in line with the risk-based audit approach of the ASPSP.

Control matrix fields to be filled in by the internal auditors of an ASPSP as part of the PSD2 audit approach are related to the *Planning phase:*

- Control environment (column F): reference to control objectives and measures specific to the institution;
- Application landscape (column G): reference to applications relevant to the institution's control environment (column F);
- Residual risk (column H);
- Audit activity planned (column I): audit work planned based on (annual) risk assessment of the institution. Activities to be dispersed into three categories:
    1. Coverage based on standard audit approach (e.g. no coverage, sample based, annually, or once each two or three year), direct or indirect (audits with full focus on PSD2 items versus audits having PSD2 aspects in scope besides the main item);
    2. Coverage based on activities within three lines of defence (e.g. business monitoring, internal control, compliance, risk management);
    3. Coverage based on continuous (business) monitoring, data analytics.

    (NB The three categories of coverage, as well as the various types of coverage they comprise of, can be adjusted to updated regulations.)

- Audit activity performed (column J): either comply (planned audit work performed) or explain (clarification for audit work not performed, or alternative audit work performed);
- Audit result (column K): audit opinion on control effectiveness.

The hereby used columns 'Audit activity performed' and 'Audit result' constitute the basis for the institutions periodic reporting on PSD2.

Reporting

The internal auditor will report about performed audit activities annually. The objective is to be transparent about what has been done to fulfil the regulatory PSD2 obligations. The internal auditor's report will include an overview of the audit activities performed and audit results based on the standard control matrix PSD2 structure. The report format and review process will be determined by the auditor depending on the objectives of the report and local practice. Audit conclusions will be based on professional judgement and available standards and guidelines.

Annex

Annex 1. Overview PSD2 Regulatory Technical Standards and Guidelines

The requirements for the audit activities of PSD2 are set in the EU Payment Services Directive (PSD2). They are specified in the EBA document Guidelines on the security measures for operational and security risks under Article 95 of Directive 2015/2366 (PSD2) and Regulatory Technical Standards (RTS) on strong customer authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)[2].

Beside the guideline on the security measures for operational and security risks and the regulatory technical standards for strong customer authentication and common and secure open standards of communication, the following Regulatory Technical Standards and Guidelines should also be considered in the PSD2 audit approach:

Overview PSD2 RTS/GL related to involved parties

1) Payment Services Directive (PSD2) (2015/2366/EU)	Articles	AIS	PIS	ASPSP
1) Regulatory Technical Standards on strong customer authentication and secure communication under PSD2	Article 98	V	V	V
1) Guidelines on the conditions to be met to benefit from an exemption from contingency measures	Article 98	V	V	V
2) Guidelines on security measures for operational and security risks under the PSD2	Article 95	V	V	V
3) Guidelines on fraud reporting under PSD2	Article 96(6)	-	V	V
4) Guidelines on major incidents reporting under PSD2	Article 96(1/4)	V	V	V
5) Regulatory Technical Standards on Home-Host cooperation under PSD2	Article 29(6)	V	V	V
6) Regulatory Technical Standards on central contact points under PSD2	Article 29(4/5)	V	V	V
7) Guidelines on the limited network exclusion under PSD2	Article 3/37	-	V	V
8) Guidelines on authorisation and registration under PSD2	Article 5/33	V	V	V
9) Guidelines on the criteria minimum monetary amount of the professional indemnity insurance under PSD2	Article 5(4)	V	V	-
10) Guidelines on procedures for complaints of alleged infringements of the PSD2	Article 99/100	-	-	-
11) Technical Standards on the EBA Register under PSD2	Article 15	-	-	-
12) Guidelines for complaints-handling for the securities (ESMA) and banking (EBA) sectors	Article 33	-	-	-
13) Regulatory Technical Standards on passporting under PSD2	Article 28(5)	-	-	-

Legenda
V = applicable appointed party, guidance audit approach is available
V = applicable appointed party, guidance audit approach is not available
- = not applicable appointed party

https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money

Standards and guidance for auditing purposes

1) Payment Services Directive (PSD2) (2015/2366/EU)	Audit framework (see Annex 1)
1) Regulatory Technical Standards on strong customer authentication and secure communication under PSD2	NOREA Guidance on audit approach PSD2
1) Guidelines on the conditions to be met to benefit from an exemption from contingency measures	EBA Final report page 18 - 24
2) Guidelines on security measures for operational and security risks under the PSD2	NOREA Guidance on audit approach PSD2
3) Guidelines on fraud reporting under PSD2	EBA Final report page 16 - 23
4) Guidelines on major incidents reporting under PSD2	EBA Final report page 16 - 29
5) Regulatory Technical Standards on Home-Host cooperation under PSD2	EBA Final report page 12 - 22
6) Regulatory Technical Standards on central contact points under PSD2	EBA Final report page 9 - 12
7) Guidelines on the limited network exclusion under PSD2	EBA Consultation Paper page 26 - 32
8) Guidelines on authorisation and registration under PSD2	EBA Final report page 18 - 71
9) Guidelines on the criteria minimum monetary amount of the professional indemnity insurance under PSD2	EBA Final report page 14 - 21

[2] NBA standard 3000a is not applicable here. Goal of this document is to facilitate internal auditors.

Annex 2. Relevant guidelines

PSD2 directive
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=NL
Important part is chapter 5, article 95 “Management of operational and security risks” and article 98 “Regulatory technical standards on authentication and communication”. These articles resulted in “EBA Guidelines Security measures for operational & security risks of payment services” and “Regulatory technical standards for strong customer authentication and common and secure open standards of communication”

EBA Guideline Security measures for operational & security risks of payment services
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf
Most relevant is guideline 2.6 with a (generic) description of required audit activities.

Regulatory technical standards for strong customer authentication and common and secure open standards of communication
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=NL
Most relevant for this document is are article 3 with a (generic) description of required audit activities, article 1 with a (generic) description of the scope of required audit activities. and article 18 that includes a description of additional required audit activities in case of an exemption.

EBA Payment services and electronic money regulatory output
https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money

Annex 3. Credits

Members of the PSD2 Discussion Group that gave support to the delivery of the practical guidance for PSD2 were:

Mike Leeman – ABN AMRO
Hans Koster - NOREA, ABN AMRO
Frank Waatjes – NOREA, ING

Several other individuals and professional parties gave their feedback during the public consultation round amongst others the Vaktechnische Commissie of NOREA. We really appreciate all their support and feedback!

Questions or feedback can be sent to mike.leeman@nl.abnamro.com and hans.koster@nl.abnamro.com.