Hans Koster and Tom van de Ven
9 October 2019
Minimum Viable Product 1 - version 3.2

Management Summary
This document contains practical audit guidance for the audit of PSD2. The guidance is based on the Regulatory Technical Standards for Strong Customer Authentication. The guidance has been delivered by Representatives of the Workgroup Payments Services of NOREA, Dutch Payments Association (Betaalvereniging) and the Workgroup IT Auditing of the Nederlandse Vereniging van Banken (NVB/WgCIA). The approach can be used as a starting point for the annual audit activities for PSD2. The audit activities can be executed in co-operation with 2LoD and 1Lod parties. The guidance has been finetuned and validated in a public consultation round in the summer of 2019. However the requirements for PSD2 and PSD2 auditing are a dynamic field. We therefore recommend users of the practical guidance to monitor PSD2 developments. Specific regulatory requirements for the execution of audit activities might also differ for different EU countries. The guidance can be adapted to your own situation.

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

During several meetings from April through June of 2019, representatives of the Workgroup Payments Services of NOREA, Dutch Payments Association (Betaalvereniging) and the Workgroup IT Auditing of the Nederlandse Vereniging van Banken (NVB/WgCIA) discussed the required audit approach for PSD2. One of the goals of these discussions was to set up a pre-agreed, standardised and pragmatic audit approach. The approach should meet regulatory requirements and should be endorsed by all financial institutions involved. Furthermore it should be useable for all institutions -or in PSD2 terminology: ASPSP's / Account Servicing Payment Servicing Provider's-that were not involved. 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 strong customer authentication as these have been set in 2019 by EBA 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 executed.

Annual audit of PSD2 related to strong customer authentication and common and secure communication)

The requirements for the audit activities of PSD2 are set in the EU Payment Services Directive (PSD2). They are more specified in the EBA document Regulatory Technical Standards (RTS) on strong customer authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)'. Based on the RTS (Chapter 1, Article 3 'Review of the security measures') the next practical guidance pointers (1-4) for the annual audit of PSD2 have been formulated (see below)[2].

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 (API's & 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 appropiate attention following the risk assessment results. Specific underlying audit approaches can be chosen by the auditor;
- in this document we focus on the specific EBA document 'Regulatory Technical Standards (RTS) on strong customer authentication and common and secure communication. Be aware that in other EBA documents for the audit of PSD2 have been set (see Annex 2). The approach offered in this practical guidance can easily be extended to other guidelines.

Practical guidance (1), on risk assessment: The internal auditor should frequently (at least yearly) make a risk assessment of the PSD2 environment. The risk assessment could be supported by underlying risk assessments of 1LoD and/or 2LoD.

Based on the proposed audit approach and recommendations, 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.

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

Practical guidance (2), on planning: The internal auditor could use the standard control matrix PSD2 (refer Annex 1) for risk assessment and planning purposes. 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 multiple year schedule (see standard control matrix), in line with the risk-based audit approach of the institution.

Control matrix fields to be filled in by the internal auditors of an institution 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:
    - Coverage based on standard audit approach (e.g. no coverage, sample based, annually, biannually, triennial), direct or indirect (= audits with full focus on PSD2 items versus audits having PSD2 aspects in scope besides the main item)
    - Coverage based on activities within three lines of defence (e.g. business monitoring, internal control, compliance, risk management)
    - 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.)

and the *Reporting phase.*

- 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 audit results for PSD2 related to strong customer authentication and common and secure communication)

The RTS (see Chapter 1, Article 3) states that 'This audit shall present an evaluation and report on the compliance of the payment service provider's security measures with the

requirements set out in this Regulation. The entire report shall be made available to competent authorities upon their request'.

Practical guidance (3), on reporting: The internal auditor yearly will report about performed audit activities. 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 1

A risk and control overview based on the RTS is available. See separate attachment *Control matrix PSD2_meeting 17 June.*

2019-07-02 Control matrix PSD2.xlsx

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://eba.europa.eu/documents/10180/2060117/Final+report+on+EBA+Guidelines+on+the+security+measures+for+operational+and+security+risks+under+PSD2+(EBA-GL-2017-17).pdf/d53bf08f-990b-47ba-b36f-15c985064d47
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 Opinion on the implementation of the RTS on SCA and CSC
https://eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+(EBA-2018-Op-04).pdf
This document elaborates on parts from the RTS on SCA and CSC (no additional requirements).

Credits

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

- Gert van Rhee - ING, gert.van.rhee@ing.com
- Gulnur Orpak - ABNAMRO, gulnur.orpak@nl.abnamro.com
- Hans Koster - NOREA, ABNAMRO, hans.koster@nl.abnamro.com
- Huib Posthumus - ING, huib.posthumus@ing.com
- Irene Vettewinkel – NVB/WgCIA, ABNAMRO, Irene.Vettewinkel@nl.abnamro.com
- Joost Beljaars - de Volksbank, joost.beljaars@devolksbank.nl
- Joost van Lier- Rabobank, joost.van.lier@rabobank.nl
- Kamal Loihabi - Rabobank, Kamal.Loihabi@rabobank.nl
- Kees Valk - Rabobank, Kees.Valk@rabobank.nl
- Max Geerling - Betaalvereniging, m.geerling@betaalvereniging.nl
- Stefan Maas - Rabobank, Stefan.Maas@rabobank.nl
- Suren Balraadjsing NVB/WgCIA, Betaalvereniging, s.balraadjsing@betaalvereniging.nl
- Tom van de Ven – NVB/WgCIA, De Volksbank, tom.vandeven@devolksbank.nl

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 hans.koster@nl.abnamro.com and tom.vandeven@devolksbank.nl.