Hans Koster and Tom van de Ven
19-07-2019
version 1.4

final draft for feedback purposes

Consultation paper – Practical guidance for Internal Auditors on the annual audit of PSD2

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 that meets regulatory requirements and that is endorsed by all financial institutions involved (and useable for all institutions that were not involved). The preliminary result is a structure that offers flexibility of approach, re-use of previously planned audit activities and that can easily be adjusted – if so required - to meet ever changing regulations.
In this consultation paper you will find an outline of a proposed audit approach: goal is to gather feedback that can be used for further improvement and / or refinement of the Practical guidance on the annual audit of PSD2 accordingly.

Questions or feedback can be sent to hans.koster@nl.abnamro.com and tom.vandeven@devolksbank.nl, ultimately by August 31th 2019. The feedback will be processed in a document 'Practical guidance for the audit of PSD2' which is planned to be distributed in September 2019.

Annual audit of PSD2

The requirements for the audit activities of PSD2 are set in the EU Payment Services Directive (PSD2) and 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)' [1]. 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].

[1] Link to RTS: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R0389&from=EN
[2] NBA standard 3000a is not applicable here. Goal of this document is to facilitate internal auditors.

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 API's & API gateway(s) and PSD2 shared services (versus local sourcing systems);
- Assurance is not explicitly required by the RTS, unless specifically mentioned (e.g. fall back exemption);
- Design, existence and operational effectiveness aspects should be given sufficient attention following the risk assessment results;
- The members of the PSD2 discussion group have chosen to use the RTS as a starting point. Internal auditors could also use standards defined by the Berlin Group, NISP-NL or IIA if these are more appropriate within their institution.

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.

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

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.

Condition

If strong customer authentication is not applied, additional requirements for the audit activities have been set (see RTS Article 3.2 [3] and Article 18 [4])

Practical guidance (4), on strong customer authentication exemption: The internal auditor should determine whether this condition applies to his/her environment. If so, the audit approach should be strengthened in line with the RTS requirements.

[3] RTS article 3.2 also includes 'However, payment service providers that make use of the exemption referred to in Article 18 shall be subject to an audit of the methodology, the model and the reported fraud rates at a minimum on a yearly basis. The auditor performing this audit shall have expertise in IT security and payments and be operationally independent within or from the payment service provider. During the first year of making use of the exemption under Article 18 and at least every 3 years thereafter, or more frequently at the competent authority's request, this audit shall be carried out by an independent and qualified external auditor'.

[4] Article 18: 'Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risks (..)'

Credits

Members of the PSD2 Discussion Group that came together at 3 and 24 April, 7 May and 17 June 2019 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

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