Impact PSD2 op IT audit

Marcel van Beek 5 juli 2018

DeNederlandscheBank

EUROSYSTEEM

Wie is Marcel van Beek?

- ✓ Bsc in Hydrographic Surveying (Amsterdam – London) en IT audit – TIAS
- ✓ Sinds 1 januari 1987 werkzaam in de financiële sector
- ✓ 1987 – 2005: 19 jaar ABN AMRO;
  IT architecture, Business Analyst, sectiehoofd binnen Regional Information Management Department Europe, senior IT auditor
- ✓ 2006 – 2009: De Nederlandsche Bank - IT toezichthouder
- ✓ 2009: ING senior Compliance officer OIB - IT & Operations
- ✓ 2010 – heden: Toezichthouder specialist - PSD2, IT risico, Information Security, Digitale Identificatie & Authenticatie, Uitbesteding & Cloud, vergunningaanvraag, BCM
- ✓ Sinds september 2004 NOREA IT auditor
- ✓ PSD2: lid van Securepayforum

  Mede schrijver: GL on security measures; GL on incident reporting; vereisten, invoering e-IDAS certificaten

  Tegenlezer en backup: RTS SCA & CSC en bijbehorende documenten.

Agenda

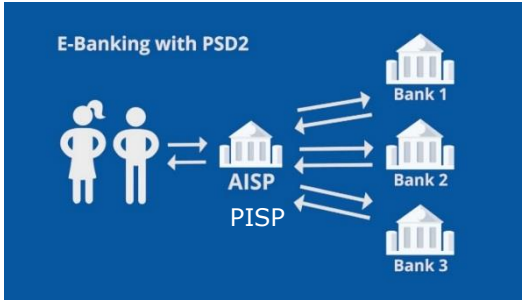
1. PSD2: Doelstellingen en belangrijkste wijzigingen
2. Status PSD2
3. Audit vereisten vanuit PSD2
4. Audit verwachtingen mbt PSD2
5. Consequenties voor Audit
6. Any other issues

PSD2: Doelstellingen

- PSD2 is herziening van Payment Service Directive richtlijn uit 2007
- Stimuleren van innovatie
- Meer openheid betaaldata
- Meer bescherming consument / betaaldienstgebruiker
- Veiliger betalingsverkeer

PSD2: Belangrijkste wijzigingen

1. **Access to accounts: Account Information Service Providers (AISP)**
2. **Initiate e-payments: Payment Initiation Service Provider (PISP)**
3. **Strong Customer Authentication & Common and Secure Communication**
4. **Security measures for Operational & Security risks**
5. **Incident, Fraud, Risk, Performance and Audit reporting**
6. Centralisation at EBA / ECB: Registers, reporting ?
7. Changes in exemptions for licences
8. Declaration of No-Objections for shareholders (>10%)



Status PSD2

PSD2 inwerkingtreding officieel	**13 januari 2018**
Invoering in Nederlandse wetgeving	**?**
EBA Regulatory Technical Standards	
• Central contact points	Pending EBA
• Passporting notifications under PSD2	Finalised
• Strong Customer Authentication and Common & Secure Communication	Finalised - September 2019
• Coordination between home and host authorities	Pending EBA
EBA Guidelines	
• Fraud reporting under PSD2	Finalisation Q3 / Q4 2018
• Professional indemnity insurance under PSD2	Finalised
• Security measures for operational and security risks	Finalised
• Procedures for complaints of alleged infringements of the PSD2	Finalised
• Major incident reporting	Finalised
• Authorisation and registration	Finalised
• Conditions to be met exemptions art 33.6 RTS SCA & CSC	In consultation
Opinion document on elements of RTS SCA & CSC	Published
EBA Q&A tool	Open

Audit vereisten vanuit PSD2 - A

RTS on Strong Customer Authentication & Common and Secure Communication

***Article 3* Review of the security measures**

1.The implementation of the security measures referred to in Article 1 shall be documented, periodically tested, evaluated and ***audited*** *in accordance with the applicable legal framework of the payment service provider by* ***auditors with expertise in IT security and payments*** *and operationally independent within or from the payment service provider.*

2.The period between the ***audits*** *referred to in paragraph 1 shall be determined taking into account the relevant accounting and statutory audit framework applicable to the payment service provider.*

Audit vereisten vanuit PSD2 - B

RTS on Strong Customer Authentication & Common and Secure Communication

***Article 18* Transaction Risk Analysis**

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 risk according to the transaction monitoring mechanisms. However, payment service providers that make use of this exemption 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 this exemption 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.

Audit vereisten vanuit PSD2 - C

GL on security measures for security and Operational risks

2.6 The security measures set out in these Guidelines should be ***audited by auditors with expertise in IT security and payments*** *and operationally independent within or from the PSP. The frequency and focus of such audits should take the corresponding security risks into consideration.*

Audit verwachtingen m.b.t. PSD2

- PSD2 opnemen in (meer jaren) audit planning & audit charter en tijdig uitvoeren van verplichte onderzoeken
- Betrokkenheid van audit bij ontwikkeling van APIs (**zeer strakke tijdslijnen!**)
- Audit opinion over API bij indienen goedkeuring en bij indienen exemptions
- Betrokkenheid / Audit opinion jaarlijks in te leveren Risk Framework (artikel 95 lid 2)
- Fraud reporting proces opgenomen in Audit cycle
- Incident reporting proces opgenomen in Audit cycle
- Auditors met ruim voldoende kennis en ervaring over de combinatie: Betalingsverkeer – Identificatie & Authenticatie – Security (technisch)

Consequenties voor Audit

- Organisatie en audit dient diepgaande kennis te hebben over het gehele proces
- Kennis over Strong Customer Authentication middelen
- Kennis over de inrichting van de security op devices

  bijv. smartphones bij gebruik van mobile banking! Blackbox / Security container. Opslaan van codes, Fingerprints, koppelen van authenticatie / authorisatie aan betaling (Dynamic Linking requirement)
- Kennis over e-IDAS PSD2 certificaten
- Onderzoeken op basis Richtsnoeren met betrekking tot beveiligingsmaatregelen

Governance	Risk Management
Detection	Protection
Business Continuity Management	Testing Security measures
Situational Awareness	Relation with Payment Users

- Frequent uitvoeren van onderzoeken op deze gebieden

Any other issues I

- **Outsourcing !!**
- **Auditor vereisten:**
  - *Aantoonbare kennis en ervaring IT security*
  - *Aantoonbare kennis en ervaring Betalingsverkeer*

- **Audit reports:**
  - Audit shall present an evaluation and report on the compliance of the payment service provider's security measures with the requirements set out in the regulations.
  - The evaluation and reports shall be made available to competent authorities upon their request

Any other issues II

- **PSD2 vereist uitdrukkelijke toestemming betaaldienstgebruiker!!!**

- **Overlap met GPDR / AVG**

Wat nog niet bekend is ?