Deloitte.
Digital

PSD2 audits

What are they about?

The Directive on payment services in the internal market which has been published in the Official Journal of the European Union on 23 December 2015 and entered into force on 13 January 2016 and also repealed the first directive on payment services in the internal market („**PSD2**") aims to bring about significant improvement in relation to customer protection, security, as well as transparency of payments.

As a result, there are new obligations to be followed by each individual payment service provider („**PSP**"). Among those, as stipulated by the Commission Delegated Regulation 2018/389 concerning strong customer authentication and common and secure open standards of communication („**RTS**"), are audits of specific security measures implemented as well as the methodology, model and reported fraud rates, if the PSP chooses to apply the transaction risk analysis („**TRA**") as an exemption to the strong customer authentication („**SCA**").

The performance of these audits might be optionally preceded by pre-audits to make sure that the PSP remedies all identified gaps before the two mandatory audits are conducted.

Deloitte provides 3 types of audit which are independent of each other:

Audit of security measures
The security measures corresponding to the new obligations listed in Article 1 of the RTS must be audited by each PSP on a yearly basis.

TRA audit - If TRA exemption is applied
TRA as an exemption to the SCA might be applied by a PSP on a voluntary basis. Should the PSP decide to apply the exemption, the minimum yearly audit of the methodology, model and reported fraud rates must be conducted.

Pre-audit - Optional
Deloitte offers its clients the option of performing preliminary audits consisting of both security measures adoption as well as the methodology, model and reported fraud rates relating to the TRA exemption. Despite being fully optional and voluntary, these audits serve as a useful preparation for legally required audits.

Performance of audits - timeframe

When exactly are the audits going to be performed?
Audit reporting should be available to Competent authorities upon their request.

during the first year by making use of the TRA exemption by an independent and qualified external auditor

on a yearly basis by auditors with expertise in IT security and payments

every 3 years by an independent and qualified external auditor

first year and thereafter **annually** by auditors with expertise in IT security and payments — **Audit of security measures**

pre-audit can be prepared **before any of the official audits** — **Pre-audit**

Audit of security measures

What is the scope of the security measures audit?
This audit shall present an evaluation and report on the compliance of the payment service provider's security measures with the requirements described in Article 1 of the RTS.

- **Security measures for the application of SCA**
- **Exemptions from SCA**
- **Confidentiality and integrity of the payment service users personalised security credentials**
- **Common and secure open standards of communication**

TRA audit

What is the scope of the TRA audit?
Banks that have applied the strong customer authentication exemption called TRA, must perform an internal and external audit for the methodology, model, and reported fraud rates.

- **Calculation methodology**
- **Calculation model**
- **Fraud rates**

Pre-audit

What is the scope and purpose of a pre-audit?
Do you want to know if you are fully compliant with the PSD2 / RTS regulation before official audits?

- **Checks of compliance with regulatory requirements before the official audits are commenced.**
- **Identification and rectification of all insufficiencies found.**
- **Assessment, reasoning and recommendations to achieve full compliance.**
- **Detailed report including the points described above.**

Our approach

The audits are based on the materials provided by the client.
Deloitte requires client cooperation.

1. Deloitte PSD2 Scan

Banks that have applied the strong customer authentication exemption called TRA, must perform an internal and external audit for the methodology, model, and reported fraud rates.

2. Price determination

Fixed price determination, depending on several factors, including the number of channels for remote transactions, security methods and SCA exemptions applied.

3. Audit of PSD2/RTS requirements

Compliance audit requires a different approach

4. Your involvement

- Providing answers to the Deloitte PSD2 Scan questions on the PSD2 RTS development, SCA exemptions and security measures
- Providing documentation, source codes, and enabling testing in production

Why Deloitte?

What does Deloitte have to offer?
We have been providing comprehensive technological and legal advisory services in the PSD2/RTS area for major Czech companies, International banks, and other players.

We know the banking industry and know the processes & regulations. You can rely on our unique expertise in the market.

We bring our industry insights and comprehensive knowledge of the IT/ security area and PSD2/RTS regulation gained through our delivered projects.

We have a wide experience helping clients in implementing requirements introduced by PSD2 and RTS SCA legislative to ensure full compliance.

We have a well educated and experienced team in PSD2/RTS analyses.

We bring our previous experience with audit policies and procedures to prove compliance with PSD2 and EBA guidelines.

Contacts

Štěpán Husek
Partner | FSI Technology
shusek@deloittece.com
+420 737 264 352

Radek Musílek
Senior Managing Associate | FSI
rmusilek@deloittece.com
+420 602 888 790

Tomáš Huml
Senior Manager | FSI Technology
thuml@deloittece.com
+420 725 818 378