GRC+ SERVICE SHEET · NOVEMBER 2026

PSD2 SCA Audit

The PSD2 regulatory technical standards require your strong customer authentication measures to be documented, tested, evaluated and audited by auditors who are operationally independent and know IT security and payments. We carry out that audit, and the yearly audit of your transaction risk analysis exemption, and give you a report your competent authority can rely on.

SERVICE
Advisory service

USUALLY TAKES
Weeks, typically, from kick-off to the signed audit report

What It Is

An independent audit of your strong customer authentication and, where you use it, your transaction risk analysis exemption, as the PSD2 RTS require.

WHY IT MATTERS

Your own team cannot audit what it built

The RTS require auditors who are operationally independent and have expertise in IT security and payments.
- Your competent authority can ask for the audit report at any time
- Fraud rates above the reference rates cost you the TRA exemption
- New channels and apps change what has to be tested

THE OUTCOME

A report you can hand to your regulator

You keep your exemptions with confidence and answer your competent authority with an audit that meets the RTS.
- Audit report available on request
- Exemptions backed by evidence
- A clear list of what to improve

What We Audit

Authentication and dynamic linking	The two independent elements, how codes are generated and linked to amount and payee, and what happens after failed attempts.
Sessions, channels and devices	Session time-outs, the security of the devices and apps that carry an element, and the channels where SCA applies.
Exemptions you rely on	Low-value, trusted beneficiaries, recurring payments and, above all, transaction risk analysis: methodology, model and reported fraud rates.
Each finding with a recommendation	Every gap comes with its risk, the RTS article it concerns and a practical recommendation for your teams.

What You Receive

The audit report PDF	Scope, method and a conclusion for each RTS requirement, with the evidence behind it.
The TRA exemption review Section of the report	Methodology, model and fraud-rate calculation checked against Article 18 and the reference rates.
Findings and recommendations Excel finding list	Each gap with its risk, the article concerned and a practical recommendation.
A management summary Presentation and a closing call	The overall result and the decisions management needs to take.

From Scoping to Audit Report

1 **Scoping**
Channels, authentication methods, exemptions and providers in scope, agreed in a short call.

2 **Documents and data**
Security policies, authentication flows, configuration and the fraud data behind your exemptions.

3 **Testing**
Walkthroughs and tests of authentication, dynamic linking and sessions on each channel.

4 **Draft findings**
You see every conclusion before it is final and can add evidence.

5 **Audit report**
The report for your management and your competent authority.

A guide, not a fixed promise: the length of each phase depends on your scope and on how quickly evidence and people are available.

Regulations That Ask for It

PSD2	**PSD2 strong customer authentication audit** The independent review of your security measures that Article 3 of the RTS requires, including the yearly audit of the transaction risk analysis exemption, by an auditor who is not part of the team that runs them.
PSD2 SCA RTS	**The Article 3 audit** An operationally independent audit of your strong customer authentication and, where you use it, the yearly audit of the transaction risk analysis exemption.
PSRs 2017 (United Kingdom)	An independent audit of your strong customer authentication and the transaction risk analysis exemption.
RPAA (Canada)	
PSA (Singapore)	
PSSVFO (Hong Kong)	
RPSCS (UAE)	
Payments Law M/26 (Saudi Arabia)	
QCB PSR (Qatar)	
NPSL (Oman)	
6493 Sayılı Kanun (Türkiye)	
RG 31676 (Türkiye)	

Why Payment Service Providers Choose GRC+

Payments and IT security in one team	The RTS ask for both kinds of expertise; our auditors bring them together on every audit.
Independent of your operations	We do not build or run your authentication, so the audit meets the independence the RTS require.
Fraud data checked, not taken on trust	We recompute your fraud rates from the underlying data and compare them with the reference rates.
Ready for PSD3 and the PSR	We tell you which findings the new payment services requirements affect, so fixes last.

Questions Buyers Ask

How often must the PSD2 SCA security measures be audited?

The RTS leave the audit period to your audit framework, taking into account your accounting and statutory audit cycle. If you use the transaction risk analysis exemption, the methodology, the model and the reported fraud rates must be audited at least once a year.

Who can perform the PSD2 SCA audit?

Internal or external auditors who have expertise in IT security and payments and are operationally independent of the functions they audit.

Who receives the PSD2 SCA audit report?

The report stays with you and must be made available to your competent authority on request. We write it with that reader in mind.

Do we need a separate audit for the transaction risk analysis exemption?

If you use the exemption, Article 18 of the RTS requires the methodology, the model and the reported fraud rates to be audited at least once a year. We can combine it with the audit of your security measures or run it on its own.

Talk to Us

Tell us which channels, authentication methods and exemptions are in scope, and when your report is due. We send a written proposal with scope, dates and a fixed fee.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/psd2-sca-audit

