Payment Services: SCA-RTS ‘audits’

What standard of ‘audit’ suits your firm?

19 July 2024

For the last few months, as in previous years at this time of year, we have been heavily involved in a number of exercises focussed on reviewing firms’ compliance with the Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication (SCA-RTS).

This work has covered both the security measures ‘audit’ requirements and, for those firms using the Transaction Risk Analysis (TRA) Article 18 exemption, ‘audits’ of their methodology, model and reported fraud rates linked to the use of this exemption.

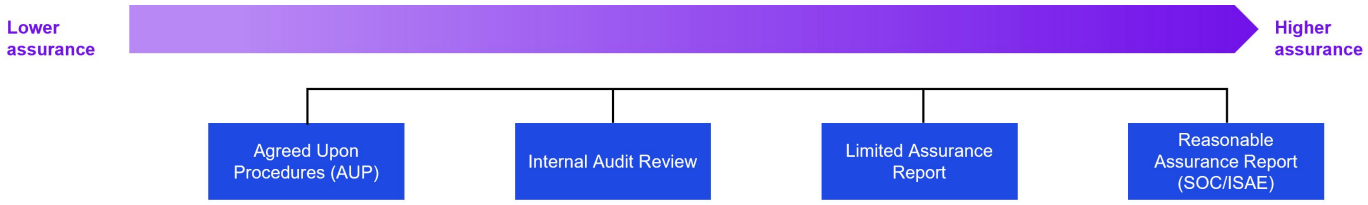
The Financial Conduct Authority (FCA) does not define the meaning of ‘audit’ and so this provides an element of optionality as to what standard firms choose for the execution of these ‘audits’.

Based upon our experience to date, firms often refer to the requirement for an ‘audit’, whilst not fully appreciating the options available.

Here, we explore some of the assurance options available, noting that these are subject to individual firm circumstances:

- Agreed upon procedures (AUP);
- Internal Audit Review;
- Limited Assurance; and
- Reasonable Assurance (SOC/ISAE).

These options are summarised below:



Scope of testing	Implementation	Design and Implementation		Design, Implementation and Operating Effectiveness
Coverage	• Point in time	• Usually point in time	• Point in time	• Point in time (Type I) • Point in time (Type II)
Output	• Factual presentation of results (to internal stakeholders)	• Report to internal stakeholders	• Independent assurance report to management and third parties	• Independent assurance report to management and third parties
Pros	• Relatively inexpensive • Can cover any process/ control	• Relatively inexpensive • Includes feedback on weaknesses	• Formal assurance opinion • Can be shared with third parties	• Formal assurance opinion • Can be shared with third parties • Covers period of time • Widely recognised framework
Cons	• No assurance opinion and only factual results • Generally restricted distribution	• No assurance opinion and only factual results • Not independent • Generally restricted distribution of report	• Lower level of assurance than reasonable assurance • Usually 'point in time'	• Relatively more expensive • More resource intensive

Another option that we have seen a number of firms adopt is a compliance 'review and recommend' style approach, which focusses heavily on whether compliance against the regulatory requirements can be evidenced or not, along with the control framework in place to ensure ongoing compliance.

These reviews have typically been executed by a combined team of specialists across Payments, IT Security and AML/Financial Crime.

So, the key question to ask yourself is ***'What standard of SCA-RTS review will work best for us?'***

How can we help?

In the first instance, we can walk you through the options available to enable you to select the type of review(s) that will work best for you.

KPMG UK has the necessary experience and skills across all necessary disciplines to execute these types of reviews. Depending upon client specific circumstances and requirements, our recent support has included the following models:

- Full execution of the work on behalf of the client concerned, with a KPMG branded report being the end result;
- Specialist support to clients' Internal Audit functions to help in the execution of the work (including payments, IT security and AML specialist support); or
- Specialist support to clients' Internal Audit functions in an advisory capacity rather than hands-on execution.

Please give us a call or send an email if you would like to discuss this matter further. We'll be delighted to hear from you.

This article was co-authored by Michelle Plevey, Stuart Taylor and Andre Mendes.