



Service Organisation Assurance Reporting





September 2020



Summary market and business drivers

As a service provider there are various ways in which you can provide assurance to your customers and other stakeholders over your control environment.

The need for this type of assurance reporting can be driven by the following:

-  **01** The increasingly regulated corporate environment your clients operate in is forcing them to consider how you demonstrate control effectiveness over the operations they have outsourced to you.
-  **02** Slowdown in economic condition has created greater needs for stakeholders to understand fully, and be confident, with the effectiveness of outsourced processes.
-  **03** There is a growing demand in the marketplace for service organisations to provide a recognised controls assurance report to retain and win business.
-  **04** Accountability for demonstrating management of outsourced risk now extends beyond pure financial risk such as Data Security.



Key triggers for you

- You are regularly audited on the same control areas by many or all of the recipients of your service.
- You are required to provide a recognised assurance mechanism when tendering for business.
- You require a mechanism for reporting against increased regulation and specific areas of risk.



Potential benefits and value

KPMG can help you to deliver tangible benefits such as:

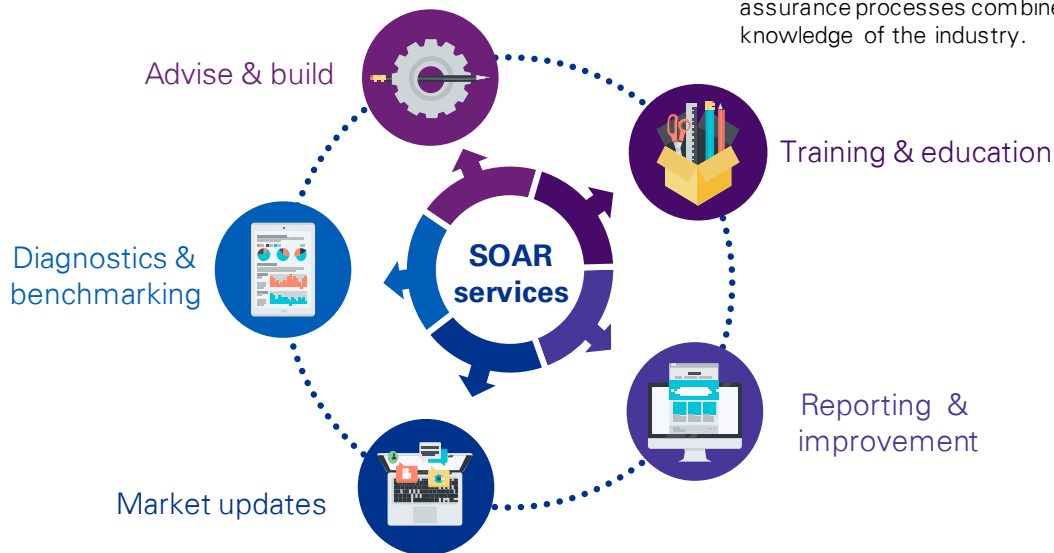
- Independently monitoring service levels.
- Acting as a catalyst to drive change.
- Minimising the number of external audits and reviews.
- Identifying and reporting areas of weakness, over-control and inefficiency.

How we have helped others and what expertise do we have?

- **SOAR:** KPMG issues single and combined reports using recognised risk and control assurance frameworks, ISAE 3000, SOC 1 (ISAE 3402/SSAE 18), AAF 01/06, AAF 02/07, SOC 2, SOC 3, ISO 27001, ISO 20000, ISO 22301, ISO 38500, ITF 01/07 and Agreed Upon Procedures (AUP).
- **Global capability:** KPMG global member firms issue in excess of 2000 SOAR reports world-wide.
- **Sector knowledge: Global:** In the Financial Services arena, KPMG member firms are the SOAR providers for a significant percent of the market.
- **Market coverage: UK:** KPMG in the UK issued in excess of 100 SOAR reports annually.

KPMG in the UK's clients include, amongst others, the following types of service organisations:

- Asset Management, ATM Services, Credit card servicing (authorisation, settlement and clearing), Custody Operations, Depository and Clearing Centre, Facilities Management, Foreign Exchange Services, Fund Accounting, Global Transactions Services, Insurance Processing, Investment Management, IT Data centre, IT Servicing, Mortgage and Payment Processing and Servicing, Pension and Share Based Payment Administration and Solutions, Securities Clearing Services.
- **Capability:** KPMG in the UK has a pool of over 200 SOAR accredited and experienced staff, 160 in the Financial Services sector.
- **Customer experience:** Our methodology and service options are based on rigorous risk, control and assurance processes combined with in-depth knowledge of the industry.



Which SOAR reporting framework?

KPMG can help you to deliver single or combined detailed reports that are designed to satisfy multiple assurance requirements from various stakeholders including your clients and their auditors:

Framework	Applicability
ISAE 3000	An international standard that can cover financial and operational risks and controls specified by a service provider.
AAF 01/06 (to be replaced by 01/20)	UK framework standards designed for the investment management/ pension management and related industries.
AAF 02/07 (to be replaced by 05/20)	UK framework standards for assurance reports on third party operations including internal controls of service organisations delivering specific financial services.
ITF 01/07	A UK framework for reports that covers the outsourced provision of information services and information processing services.
SSAE 18 (SOC 1)	US equivalent standard for ISAE 3402 mostly applicable when service provider performs financial transaction processing or supports transaction processing systems.

Framework	Applicability
ISAE 3402 (SOC 1)	International framework replacing SAS 70 that focuses on financial reporting risks and controls specified by the service organisation.
SOC 2	Reporting standard focused on security, confidentiality, availability, processing integrity and/or privacy and applicable to a broad variety of systems. In the UK, SOC 2 is delivered through the ISAE 3000 standard, and in the US through the SSAE 18 standard.
SOC 3	Same as SOC 2 although a much shorter report with option to issue a web site seal.
ISO 27001	International standard for the certification of an Information Security Management System.
ISO 20000	International standard for the certification of an IT Service Management System.
ISO 22301	International standard for the certification of a Business Continuity Management System.
ISO 38500	International standard for reporting of Corporate Governance of Information Technology.

We are able to work with you and your customers to select a reporting approach (controls/assertion, management system), standard set of principles, criteria and controls – subject matter, report type (diagnostic, Type I/II opinion, certification) and assurance level (reasonable, limited).

Adopting a combined approach is designed to optimise the SOAR experience in terms of time and effort whilst striving to increase the delivery of multiple assurance reports.



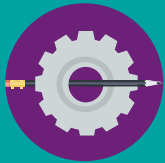
What sets us apart?

KPMG has:



- Significant experience and passion in Service Organisation Assurance Reporting.
- SOAR subject matter experts with a global mindset, methodology and accreditation programme. We are able to deliver a consistent approach to our clients with a national and international perspective on the emerging risk issues which are driving the SOAR agenda.
- A forward thinking approach to sharing good practice, insights and views to service providers and their customers through seminars, workshops and webinars.
- A value adding five stage methodology that advocates the participation of service providers and their customers in scoping and reporting activities – after all the main audience for the reports are the service users.
- A SOAR delivery model that is designed to be innovative and integrated across our advisory and audit practices; KPMG in the UK is an accredited certification body that delivers combined reports (e.g. SOC 2 and ISO 27001 certification) – a leading service capability.

What have we delivered to our clients?



Advise and build:

Scoping of reports with all internal and external stakeholders. Risk assessments and writing control objectives and controls. Legislation and regulatory alignment (e.g. SoX). Roadmap for implementation.



Training and education:

Senior management awareness sessions. Control and process owner training and guidance. Risk and control challenge sessions.



Reporting and improvement:

SOAR reporting under recognised reporting framework standards. Harmonised shield combining assurance reporting and certification services. Insightful improvement recommendations.



Market updates:

Seminars, workshops and webinars that encourage knowledge and experience sharing, with insights on hot topics and the future landscape.



Diagnostics and benchmarking:

Gap analysis and readiness reviews. Benchmarking within and across sectors. COBIT and other standards (e.g. ISO27001, ISO 22301, ISO 20000, ISO 38500).

Contact us



Dr Irene Sellars

Director, FS Regions
National Service Line Leader
IT Risk Management
T: +44 (0) 7827 081835
E: irene.sellars@kpmg.co.uk



Sam Subesinghe

Partner, Head of FS Regions
IT Risk Management
T: +44 (0) 13 15 276836
E: sam.subesinghe@kpmg.co.uk



Suvro Dutta

Partner, Audit
UK Head of Assurance and ESG
T: +44 (0) 2073 111466
E: suvro.dutta@kpmg.co.uk



Allen Eccles

Senior Manager, FS Regions
Deputy Service Line Leader
T: +44 (0) 7785 591704
E: allen.eccles@kpmg.co.uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the United Kingdom. The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Designed by CREATE | September 2019 | CRT107196

www.kpmg.co.uk

