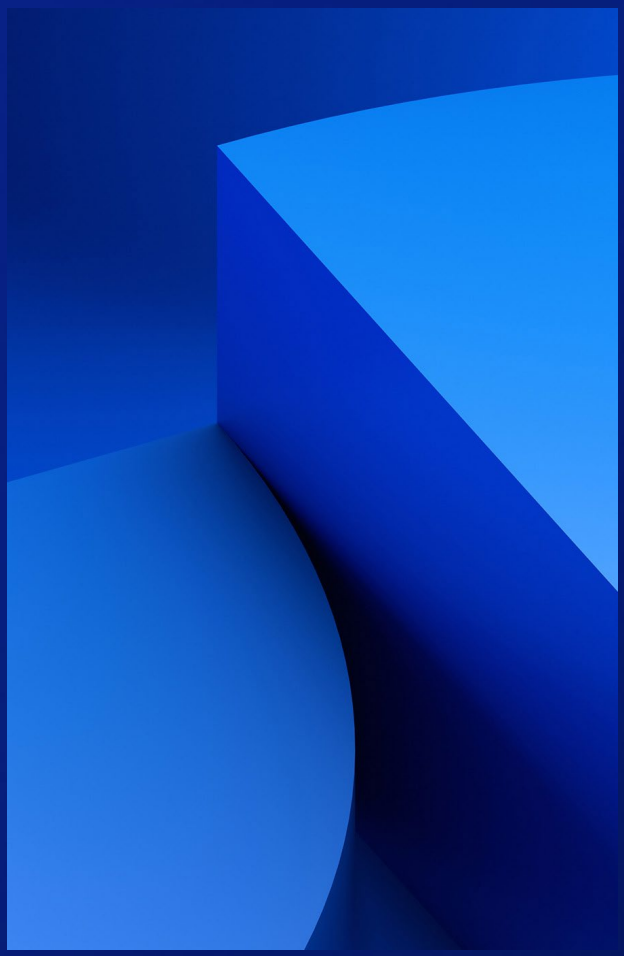
KPMG

Assuring Cloud Services



A KPMG Service for G-Cloud 14

May 2024

kpmg.co.uk

Introduction to Assuring Cloud Services

Service Description:

KPMG works with cloud service providers to build confidence in their control environments by efficiently addressing customers assurance and regulatory requirements.

What are the benefits of KPMG service?

- Helps build confidence in the quality of your cloud service
- Minimises the number of external audits reviews for you
- Independent monitoring of Service Level Agreements and performance
- Drives improvements in control processes
- Aids you in meeting all your regulatory requirements
- Clarifies control roles and responsibilities
- Enables you to demonstrate and maintain robust processes and controls
- Supports in delivering a robust response to known control failures
- Helps you to constantly manage and reduce risk proactively
- Promotes understanding and openness between you and your customers

Our service features

- Follows assurance standards / frameworks / technical releases: ISAE (UK) 3000, ISAE 3402, SSAE 18, SOC2, AAF
- Provides assurance over cloud processes, security, governance, changes
- Delivery of a full independent service auditor's assurance report
- Option to report using Agreed Upon Procedures (AUP) – you determine the areas of focus
- Cloud Security Reference Model used to map the environment
- Control objectives, related controls and tests performed by service auditor
- Multiple assurance reports from one set of control testing
- Provides specific client / auditor requirements including SSAE18 and AAF 01/20

Client Challenges and Our Approach

Our clients face the following internal and external challenges in providing well defined and controlled cloud services to a range of customers.

Our approach

We're one of the largest, and most experienced providers of controls assurance reporting, issuing more than 150 reports in the UK each year, and more than 2,000 globally. Our approach brings that experience to our clients.

A flexible approach. Clients want to get to get to an unqualified Type II report as quickly as possible. We help them to achieve this by tailoring a flexible approach that can start with a diagnostic engagement, before moving into formal Type I and Type II reporting.

Bringing everyone along on the journey. We work closely with key internal stakeholders - providing education, which in turn delivers efficiencies. Assurance reporting can help improve productivity and deliver better client outcomes.

Upskilling control operators. Through educational workshops, briefing sessions and ongoing communication year on year we help businesses to demonstrate robust controls.

A 'no surprises' approach. We encourage frequent two way dialogue, flagging any issues early during regular progress and steering group meetings.

Cloud SOC reporting benefits

Regulatory and contractual

A good night's sleep for Execs

Increasing regulatory and contractual governance demands are driving the third party assurance bar higher. Our in-house subject matter experts and tailored assurance proposition relating to cloud services can help you address these evolving requirements (e.g. GDPR through SOC 2+ with KPMG Privacy Control Framework).

Culture

Changing culture

Enhancing the knowledge and awareness levels of cloud risks and control owners in the service provider as client and regulatory context drives improved understanding, accountability and responsibility.

Driving continuous improvement within the maturity of cloud services in the organisation.

Marketing

Getting on the front foot

A uniquely designed transmittal letter to provide independent evidence of robust cloud controls needed for bids to prospective customers.

Assists in meeting due diligence and supplier questionnaire requirements.

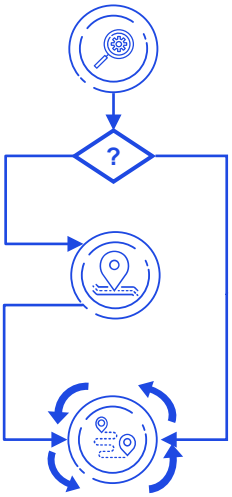
Reduced risk of audit fatigue

Satisfying multiple needs

Third party assurance reports answer many questions and aim to give comfort to your customers, their auditors, the board and internal stakeholders. Our offer involves a scoping workshop and inclusive reporting stages with your clients to help you verify that the scope of your assurance reports meet their requirements.

We've had many successes in the past of being able to help improve confidence over cloud services through an inclusive workshop and reporting stages, which ultimately is aimed to reduce the overhead costs associated with responding to multiple audit requests.

Cloud SOC engagement journey



Stage 1
Diagnostic review

Checkpoint
Complete Stage 2, or proceed directly to Stage 3?
Agree timeline for Stage 2 and 3.

Stage 2
Point in time SOC report issued, for internal and external use, known as ‘Type I’

Stage 3
Period of time SOC report, known as ‘Type II’.
Repeat annually.

Diagnostic review and remediation

We will work with you to:

- Build a strong and balanced control framework. We help to identify areas of over- or under-control, to ensure that the controls included in the SOC report are as effective as they can be. We can leverage your existing control frameworks for this or help you to build the framework from scratch.
- Develop a clear plan of action to remediate any issues before fieldwork for the Type I / Type II reporting begins, reducing the risk of exceptions or a qualified opinion.

Type I & Type II reporting

In both the Type I and Type II planning phase, we will agree a detailed timetable with you and share detailed evidence requests, to help the testing phase run smoothly.

During the testing phase, we will:

- Walk through the design and implementation of controls with your control owners. We’ll also review the evidence you’ve shared to test the design and implementation of the controls.
- Perform testing over the operating effectiveness of your controls based on the evidence you’ve shared (Type II only).

In the reporting phase, we will:

- Review your description of service, management statement, and management representation letters.
- Work with you to compile the draft report, including our opinion letter, test procedures, and test results.
- Finalise our internal quality review processes and review the report together with you prior to signing.

What resources we need from the client

From experience, we’ve found that the assurance fieldwork and reporting process works best with an appointed project manager, who will help to arrange meetings and collect the documentation we need.

It’s also best to appoint specific control owners for each control — someone who knows the control inside-out and can provide the documentation we need.

We will share a detailed list of evidence requests based on the control framework. This is likely to include things like policy documents, service desk tickets, and access request forms. We will set up our secure KCC platform so that these documents can be shared safely.

Throughout each stage, on at least a weekly basis, we hold status update meetings with you to review progress and discuss how to resolve any issues. This is in keeping with our ‘no surprises’ approach.

Why KPMG

01

The best solution for you

Our well-founded methodology will enable us to get it right for you first time, efficiently and reliably. We have an excellent track record in meeting clients' timelines. A key aspect is our partnership with you, and an inclusive approach with your customers, along your assurance journey.

02

Excellent value for money

To demonstrate our commitment to providing you with excellent value for money, we will provide a fixed fee for the Type I / Type II report, once detailed scoping (or the Diagnostic phase) has determined the scale of your control environment.

03

Specialist team

We use our dedicated Controls Assurance team to deliver SOC engagements. This team focuses 100% of their time on delivery of service assurance reports, we don't just use audit or controls generalists for this type of work. This means you will benefit from the insight and challenge they bring.

04

High quality work

Through a combination of using our specialist team and our rigorous review cycle, we provide high quality reports, every time. Each report is reviewed by at least five reviewers: the Engagement Manager, Engagement Senior Manager, Engagement Leader, Technical Reviewer and Engagement Quality Control Reviewer.

05

Access to subject matter experts

We will provide you with at least five meetings per year with our wider specialist network of Cloud and Service Audit professionals to discuss a topic of your choosing

kpmg.com/uk