KPMG

Reimagining Controls Assurance with AI: Latest Insights for Leaders

(SOC 1, SOC 2, ISAE 3402, ISAE (UK) 3000, AAF 01/20, AAF 05/20)

KPMG. Make the Difference.

January 2026

Foreword

Momentum matters. Our **2024 benchmarking study** has resonated strongly with the market and across our global network, prompting follow-up dialogues and unsolicited client commendations on the insights that we are providing.

AI is now central to our client conversations…

In 2025 we have doubled-down on two fronts:

1. **Assurance *with* AI**. We are market-leading in the disciplined use of GenAI and advanced tooling to **accelerate** assurance without compromising rigour – leveraging **KPMG Clara AI ("Clara AI")**, **Microsoft 365 Copilot ("M365 Copilot")**, **DataSnipper®** and **KPMG Clara Collaboration ("KCc")** to reduce disruption for control owners, compress analyst testing cycles, and focus effort on the most judgemental areas that drive stakeholder insight. Recent engagements have evidenced tangible efficiency gains (e.g., testing time reductions of **~18%**) through automating control analysis, evidence extraction and standardised documentation, alongside better transparency of status and findings for sponsors.
2. **Assurance *of* AI**. We are excited to be introducing a **reasonable-assurance opinion** over entities' AI governance and controls through our **SOC 2+** approach – extending trusted SOC principles with **KPMG's Trusted AI** framework to meet growing stakeholder and regulatory expectations. Watch this space.

What the 2025 data says…

Comparing our latest results with last year, overall trends remain consistent, but control frameworks are **improving** in composition: a reduction in highly manual **management review controls** (from 40% to 31%) and a clear increase in **exception reporting** – consistent with greater automation and technology use. Our practical recommendation stays firm: **automate where sensible and strengthen System Access controls**, as these continue to be material drivers of exceptions and report outcomes.

We also highlight the ever-increasing assurance requirements in the **Financial Services (FS) sector,** including evolving needs for **Financial Market Intermediaries** and **Critical Third Parties**, where independent assurance over resilience, governance and third-party dependencies is increasingly a Board-level requirement. The updated corporate governance codes over **material controls**, increasing reliance over **third-party sustainability data** alongside emerging markets such as crypto and digital assets, are now firmly on the Board agenda – driving demand for independent assurance to meet heightened stakeholder and regulatory expectations.

The call to action…

As AI adoption scales and regulatory expectations intensify, organisations that modernise their control mix – automating high-cost activities, reinforcing access management, and evidencing relevance and reliability of information – will see **better assurance outcomes**, **lower disruption**, and **clearer insights** for decision-makers.

I trust you will enjoy reading this publication as much as our team love putting it together, and I look forward to fruitful discussions with many of you.

Irene Sellars

Partner,
Head of Controls Assurance
KPMG in the UK

AI in Assurance

01

KPMG 2025 Global CEO Outlook: AI Findings

CEOs forge ahead with AI investment and adoption while balancing risk

71%

of CEOs consider AI a top investment priority, despite economic uncertainty.

69%

of CEOs plan to allocate 10–20% of their budgets on AI in the next 12 months.

67%

of CEOs anticipate seeing ROI within 1–3 years.

Up from the majority predicting 3–5 years in 2024.

Top CEO Concerns

77%

of CEOs feel AI workforce readiness will impact their organization's prosperity over the next 3 years.

Biggest challenges to implementing AI:

1. Ethical.
2. Data readiness.
3. Lack of regulation.

kpmg.com/CEOoutlook

Assurance with AI

How do we at KPMG use AI to support our work?

KPMG is making multi–billion–pound investments in global technology across our services which include a market leading alliance with Microsoft. Leveraging advanced artificial intelligence (AI) helps us deliver major benefits for service organisations, achieving faster, more accurate and efficient assurance engagements.

The integration of AI–driven tools such as KPMG Clara AI, DataSnipper®, KPMG Clara Collaboration, and Microsoft M365 Copilot supports auditors in reducing manual effort and helps enhance the overall quality and experience of assurance engagements for our clients and us.

KPMG Clara AI: SOC custom agents

Helps reduce number of meetings and time needed from control owners.

Clara AI is KPMG’s in–house AI tool operated in a secure, controlled KPMG environment that can be utilised from planning through to fieldwork/testing and reporting. On Clara AI, we’ve developed a series of custom agents and prompts that allow us to be efficient and productive on assurance engagements.

Whilst some of these help with general project management tasks, others perform specific and technical tasks such as capturing controls and automating the development of a draft test plan for review, for use in walkthroughs and testing. Custom agents provide assistance in many ways:

- Help prepare for walkthrough meetings, and creates meeting agendas.
- Analyse control descriptions against what a good control looks like, including an indicative score! *The score provides us with decision support and not a conclusion.*
- Collate comments on a Description of Service from multiple reviewers and produce a client ready summary of key themes.
- Create flowcharts for better process understanding.

KPMG Clara AI: Control test plan designer

Helps make meetings more efficient.

To make the best use of our clients’ time during walkthroughs, where permitted, we use secure KPMG Clara AI tool to perform a review of the control wording. This then provides a list of the key control attributes and a list of questions to ask in the walkthrough. During the walkthroughs, M365 Copilot is used to transcribe these into useable flowcharts and process maps automatically generating a ‘Test of Design’. This adds value by:

- Breaking the control down into attributes, enabling our clients to better identify and manage risk.
- Thorough identification of all control attributes meaning less follow–up requests for control owners.
- Easing the workload of control operators and providing a detailed agenda ahead of walkthroughs.
- Improving quality of controls and control documentation ultimately contributing to a higher quality report.

Assurance with AI (cont.)

DataSnipper®

Helps improve efficiency during testing by providing traceability, extraction and linkage.

Here are two successful ways in which we have used DataSnipper®, our intelligent audit platform:

Supporting completeness and accuracy details:

- One of our Assured entities population of IT system changes that required testing a high–volume of change tickets. We used DataSnipper® to extract key details from request tickets, saving hours of manual review and efficiently populating our testing tables.

Improving efficiency in controls testing:

- By using DataSnipper®, one engagement team were able to quickly and reliably test controls, address queries and were successful in reducing testing time by ~15%.

KPMG Clara Collaboration

Supports efficient and data driven project management.

KPMG Clara Collaboration (KCc) provides a secure, digital environment for evidence management, progress tracking and engagement communication, improving transparency for clients and audit teams.

Our clients' staff (control owners) are given direct access to KCc to upload their evidence. Requests for evidence are mapped to each control and assigned to control owners providing full visibility of evidence status, audit trail with dates items were uploaded, comments with queries.

We implement risk-based access controls that limit access to certain information to only those who require it. This helps facilitate our 'no surprises' approach with real time stats and findings. It helps keep all engagement documentations in secure KPMG platforms in one place for ease of reference.

M365 Copliot

Boost efficiency by reducing meeting time and follow up questions.

Our partnered AI–powered digital assistant, M365 Copilot, enabled through the KPMG-Microsoft global alliance is utilised throughout engagements. We have found compelling use cases in everyday tasks associated with SOC reporting, including:

- Meeting recaps and actions using the 'transcribe' function reduces the need for follow–up questions. (Transcription occurs within Microsoft 365, and doesn't utilise a separate AI system).
- Data analysis in Excel to efficiently identify trends, anomalies, and insights enhances our testing process.
- Drafting and editing audit workpapers, summarising and extracting information from evidence documents allows our auditors to divert their energy to the most critical and judgemental audit areas (our teams ensure that outputs still reflect auditor judgement).

Assurance of AI

Putting an assurance lens on your AI journey - How KPMG can provide assurance over your AI governance through SOC2+ and Trusted AI

The landscape for AI assurance is evolving rapidly as organisations and regulators place increasing emphasis on transparency, accountability, and trust in AI systems. The latest transformative step change in the world of AI is agentic AI. For organisations that are at the forefront of deploying AI for operations, agents are now a critical part of their AI strategy.

From an assurance perspective, our cross industry and sector experience has allowed us to see organisations that are at different stages of AI adoption and controls over their AI tools and resources. KPMG's approach Assuring AI is to provide reasonable assurance over the governance and controls surrounding AI systems.

Where do you need to start with Assuring your AI landscape?

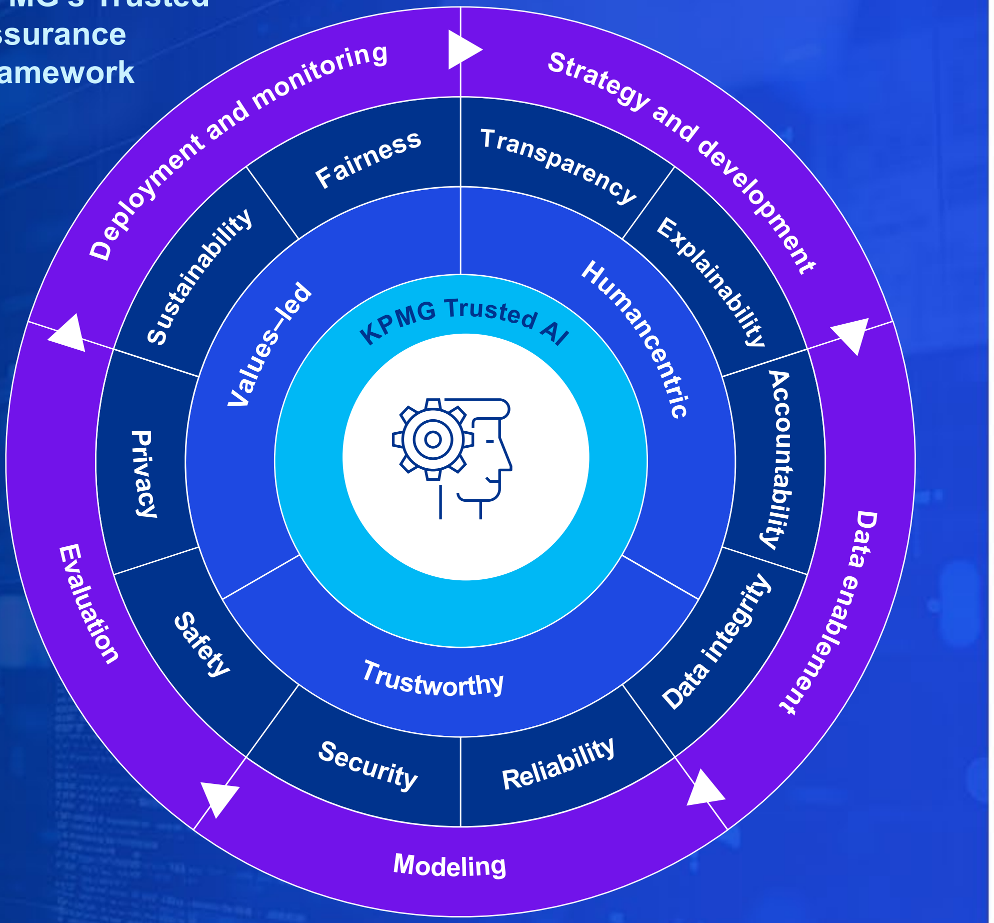
Organisations will need to begin to understand and **map their AI landscape** to assess the risks they are exposed to. Maintaining the AI inventory is key to making sure that AI systems are traceable and continuously monitored for emerging risks or issues.

We strongly recommend that an **AI strategy & governance framework** is implemented to provide a basis for alignment to relevant regulations and ethical standards. A gap analysis can help identify areas of non–compliance with regulatory and internal requirements. Similarly, performing a data privacy and security review and update will help ensure compliance and safeguard against unauthorised access or misuse.

Organisations should continuously **evaluate AI models to monitor** for accuracy, fairness, reliability and bias using automated tools and trigger alerts for deviations. Another critical success factor to getting it right is **training employees** on AI ethics and compliance and educating them on ethical AI use, potential biases, and organisational policies to foster responsible practices.

Once organisations are ready with the above, they can look to engage independent assurance providers to review and attest to the organisation's AI maturity.

KPMG's Trusted Assurance Framework



Assurance of AI (cont.)

Our clients' users are increasingly asking 'How do I know the AI you're using to deliver services to me works properly?'

The UK Government's "Assuring a Responsible Future for AI" (November 2024) forecasts that the UK AI assurance market could exceed £6.5 billion by 2035. This indicates a shift from focusing solely on the benefits of AI to ensuring robust governance and control and to demonstrate trust in AI.

Whilst there is currently no prescriptive regulatory framework mandating external AI assurance, new standards such as ISO/IEC 42001:2023 and regulatory initiatives like the EU AI Act are shaping expectations.

KPMG's approach extends the established SOC 2 framework with additional AI–specific control objectives ("SOC2+"), providing reasonable assurance over the governance and controls surrounding AI systems.

SOC 2, originally designed with technology–focused organisations in mind, already covers core governance, risk management and security topics. The 'plus' part of SOC 2+ builds on this to cover frameworks beyond the Trust Services Categories – in this case specifically using KPMG's Trusted AI framework as a basis.

This approach positions organisations to meet growing stakeholder expectations and regulatory scrutiny, while supporting market growth and innovation in the responsible use of AI.

Our AI Assurance team tests, examines evidence, and reports on management process, controls, and claims regarding responsible use of AI technologies. This includes AI Assurance scoping, AI Assurance Readiness through to providing a formal assurance opinion.

Our 2025 SOC Benchmarking analysis

02

Benchmarking assurance reports

Across 180+ reports spanning a range of frameworks/standards – SOC 1 (ISAE 3402/SSAE 18), SOC 2 (ISAE (UK) 3000), AAF 01/20 and 05/20, we analysed control types, nature of controls and trends in exceptions and reporting outcomes.

The headlines:

Demand for controls assurance reports continues to grow and nearly doubled in the last year (90% over the base year of 2023–24) **with more Technology clients seeking assurance reporting services** (32% of all reports issued in 2024–25)**.**

Fewer qualified reports are being issued compared to past years (15% of all reports issued were qualified compared to 20% in the base year of 2023–24)**.**

Manual controls remain more likely to fail compared to automated controls (90% of all exceptions of operating effectiveness were on manually operated controls)**.**

System Access and Authorisation contribute significantly to control effectiveness failures (39% of all exceptions were on System Access and Authorisation controls)**.**

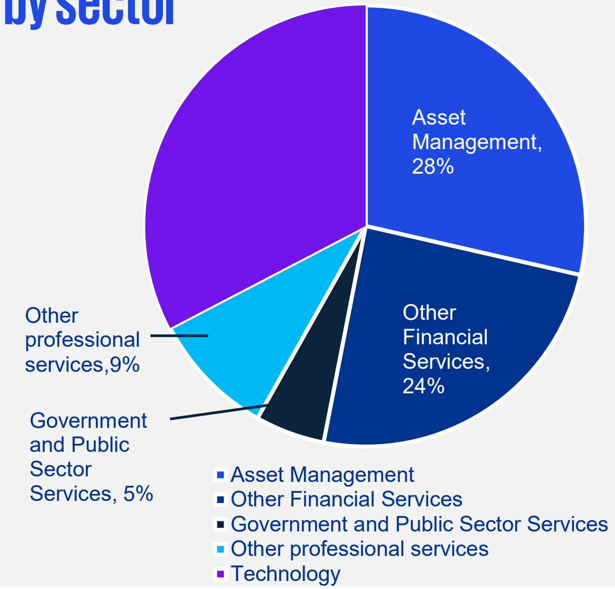
Although Service Organisations have made positive changes to their control frameworks, for instance by increasing the number of automated controls, there isn't an increase in controls over adoption of new technology such as Artificial Intelligence (AI) proportionate to their use across industries.

The control types where exceptions are noted remains consistent with our previous findings, i.e. Management Review controls, System Access and Authorisation controls. Evidencing completeness and accuracy of information continues to be a contributing factor to exceptions.

180+

Reports issued between 2024 and 2025

Reports included in the study, by sector



Control types

Service Organisations have actively rebalanced their control activities to address operational priorities, especially efficiency.

For example, ‘Management Review’ controls which typically carry the highest operational cost have reduced from 40% to 31% of all controls. ‘Exception reporting’ controls have increased from 4% to 13% of overall controls which is consistent with the increased use of technology and automation for detecting and alerting when a potential error has occurred. An increase in segregation of duties controls (from 3% to 5%) further helps efforts to reduce operational costs by helping mitigate fraud and cybersecurity risks.

Overall, these changes signal a proactive approach to control framework design – one that is responsive to regulatory developments, technological advancements, and the complex risk landscape facing organisations today.

How have your operations evolved over the last 12 months? Has your suite of controls evolved to keep pace?

Configuration controls

(automated configurations or mappings, interfaces).

8%
9% ↑

Authorisation controls

15%
18% ↑

Reconciliation controls

(used for verifying completeness, accuracy, and integrity of data and information).

6%
7% ↑

Segregation of duties controls

(and review and escalation).

3%
5% ↑

Exception reporting controls

(and review and escalation).

4%
13% ↑

Independent/management review controls

(used for verifying correctness, completeness, accuracy etc. or monitoring of activities with a view to detect anomalies, includes Key Performance Indicators (KPI) monitoring).

40%
31% ↓

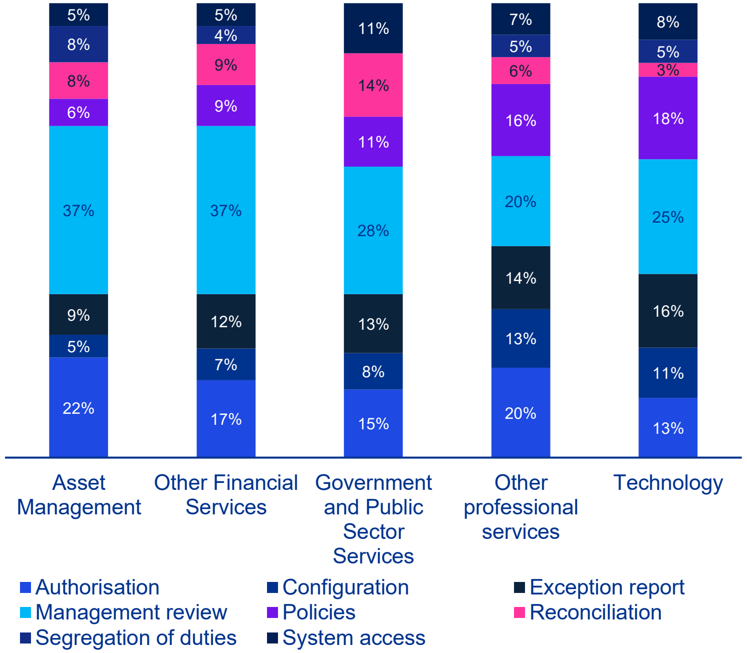
System access controls

(system configurations and reviews of access).

8%
6% ↓

Policies and procedures controls

16%
12% ↓



Trends in exceptions

14% of reports issued in 2024–25 carried exceptions on 10% or more of the overall controls tested.

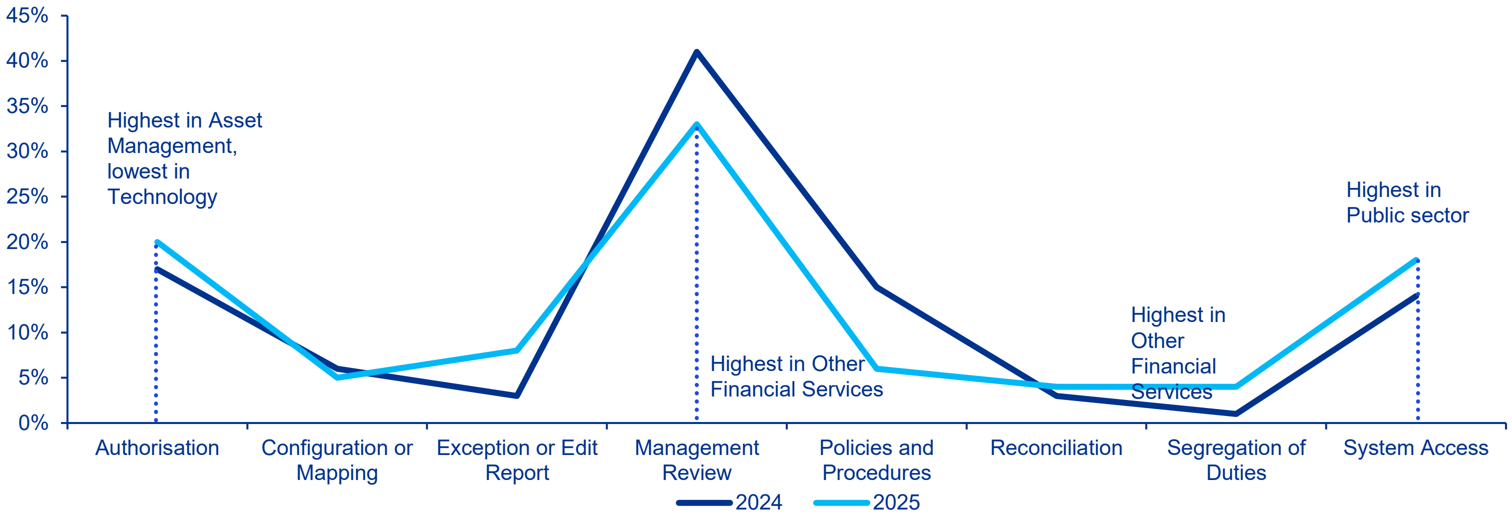
Technology sector tops the exception rate (34% of all exceptions were in reports issued for this sector).

Exceptions on Authorisation controls is on the rise (highest in Asset Management reports where this accounts for 22%).

Automation is key to reducing exceptions as automating validation and reconciliation reduces errors and strengthens control evidence.

How robust are your system access controls? Are you automating operations to minimise exceptions and boost accuracy in your controls?

Trends in exceptions by control types across reports by year



There is a shift towards automated controls. Overall, the volume of manual controls in reports continues to be higher across the board and consequently higher number of exceptions were found in manual controls.

		Automated	Manual
Design/implementation exceptions	2024	17%	83%
	2025	↑ 19%	↓ 81%
Operating effectiveness exceptions	2024	11%	89%
	2025	↓ 10%	↑ 90%

Control exceptions and qualifications – key themes

There has been **reduction in qualified opinions for controls assurance reports in 2025** (number of reports issued with qualified opinions, fell from 20% in previous years to 15% in 2025. These were owing to primarily lack of evidence for authorisation, approval, and reviews.

Organisations should focus on strengthening evidence retention and documentation processes for controls. Proactive engagement with audit teams can further improve overall assurance outcomes. **How do your operations compare?**

System Access Management

Exceptions caused due to delays or failures in revoking system access for leavers, incomplete access removal from in house and third–party systems, and applications and access granted without proper documented approval.

Management reviews

Excess use of Management Review control activities has meant that this was a significant contributor to overall volume of exceptions. Reviews not completed within the expected/required timing, sufficient documentation not maintained for client mandates, internal/external monthly reviews, post event monitoring of IT activities such as backup performance, incident management.

Meetings and communication

Approximately 17% of findings were related to meeting minutes and/or required communication including sign offs and records of review not being maintained.

Completeness and Accuracy

There is an increase in the number of findings reported around lack of completeness and accuracy of information.

Top 10 exceptions

System Access Management	• Access not revoked in a timely manner for leavers. • Incomplete or delayed notifications to disable access. • Access granted without proper authorisation or documentation. • Inadequate review of user access lists and permissions.
Completeness and accuracy	• Lack of completeness and accuracy of the information used by management in the operation of a control. • Lack of completeness and accuracy of populations to select samples from.
Meetings and communication	• Required meetings not occurring, or minutes not retained.
Policies and Procedures	• Missed reviews of policies or other documents.
Other	• Lack of audit trail / documentation for control activities such as approvals, reviews or reconciliations. • Mandatory training not completed.

Making easy improvements such as retaining evidence for meetings or automating reviews where possible can help avoid some common exceptions.

Are your data and controls audit ready?

Insight

Relevance and reliability of information

Following what we shared in 2024, this year there is a notable increase in exceptions reported around the relevance and reliability of information despite Control Activities operating effectively. In recent years, the expectation of auditors, regulators and users of assurance reports have increased in this regard.

What is it and why does it matter?

Completeness and accuracy specifically relates to information used by the Service Organisation in the performance of a control or information used by the service auditor as a population from which to select a sample of control instances to test operating effectiveness. Service auditors are required to perform more in–depth test procedures to confirm the relevance and reliability of the population they select test samples from without which there is a risk that their testing does not detect errors.

Failure to evidence completeness and accuracy can result in reportable exceptions and in some cases, a qualified opinion, reduced confidence from stakeholders and report users and increased requirement (and cost) for additional monitoring controls.

From recent reports, the following patterns have emerged in relation to these findings:

- Incomplete populations: Management unable to confirm that all relevant items were included for review (e.g., leavers, incidents, access requests).
- Missing or unreliable data: Inability to demonstrate that data used for control operation was sourced reliably or was up–to–date.
- System Limitations: Systems not configured to generate complete reports or alerts.
- Manual Processes: Reliance on manually maintained lists or records, increasing the risk of errors and omissions.

Top tips

To avoid exceptions with regards to completeness and accuracy of information, Service Organisations should consider the following:

- For information used in the performance of a control, e.g. an application user list reviewed with a user access review control, evidence of generation and extraction of the user list should be retained as part of the review.
- Where possible, system generated lists should be used to provide information direct from the system.
- Agree an approach for providing complete and accurate information with your service auditors upfront.

The use of advanced Data Analysis tools (using AI) can help reduce the burden of evidencing completeness and accuracy through manual procedures.

Emerging assurance needs

FS Assurance

Financial Services firms operate in an environment of heightened regulatory scrutiny and systemic risk. These increased regulatory scrutiny and requirements demand robust assurance over controls, resilience capabilities, and third party dependencies for market confidence.

Most of the regulations point in the same direction – that assurance is no longer optional. For example, PRA and FCA's Operational Resilience policy require firms to identify important business services, set impact tolerances, and test severe but plausible scenarios. DORA mandates resilience standards for ICT and third party providers across the EU for the Financial Services sector. The Critical Third Party (CTP) regime introduces direct regulatory oversight of service providers, with expectations for assurance over governance, resilience, and risk management. The UK Corporate Governance code calls for assurance over non financial reporting and material controls, reinforcing transparency and accountability.

Our clients face three key challenges – Complexity as a result of multi jurisdiction operations, layered outsourcing, and critical technology dependencies; growing intensity of regulatory scrutiny where the regulators demand evidence of resilience and effective control environments; and increasing stakeholder expectations around confidence in governance and risk management. Without credible independent assurance, firms risk regulatory intervention, competitive disadvantage, and erosion of trust. Assurance can also serve as an effective tool for organisations in the crypto and digital asset markets due to the complexity of technology and the significant security risks inherent with this sector.

KPMG delivers end to end FS Assurance solutions that combine deep sector expertise, regulatory insight, and proven methodologies. Through our assurance solutions we assess governance, resilience, and control design across critical services and third party ecosystems using proprietary tools and benchmarking data for pragmatic and actionable insights.

Emerging assurance needs (cont.)

Material Controls Assurance

Following the FRC's Corporate Governance Code (“the Code”), Boards are seeking confidence that their declaration to the market and the public can be trusted. This means verifying that their most critical controls are operating effectively. Boards will be required to make a declaration on the effectiveness of material controls annual report. This was a key change in the FRC's update to the Code in 2024 (effective 2026 onwards)

At KPMG, we are working on the appropriate route to providing a reasonable assurance report over the material controls. Whilst KPMG's opinion would not extend to the identification or suitability of which controls are material, this matter is for the Directors to decide, we expect the Board will be able to make a public reference to the fact that the company has commissioned a reasonable assurance report on material controls.

A dry run of the approach to the declaration, including assurance is recommended for Boards to make this declaration with confidence.

Emerging assurance needs (cont.)

Third party sustainability data

Organisations increasingly rely on third-party sustainability data to meet growing reporting and regulatory demands. As scrutiny intensifies, the quality and control of this data has become critical for credible disclosures and informed decision-making.

Regulators and stakeholders expect transparent, well-governed non-financial information. New sustainability reporting rules, tax regimes, and the incoming regulation of ESG ratings providers in the UK and EU increase expectations for robust, defendable data. Additional requirements — including the CSRD assurance mandate and emerging supply-chain due-diligence legislation — further heighten the consequences of inaccurate or incomplete third-party data. Financial penalties, contractual breaches, and reputational harm remain significant risks where methodologies or controls are weak.

Organisations face three main challenges: complex and fragmented third-party data sources; rising expectations for high-quality, consistent sustainability information; and increasing exposure when external data is unreliable. Without independent assurance, firms risk compliance failures, operational inefficiencies, and loss of trust. Third-party assurance provides confidence over the design and operation of sustainability data processes.

KPMG’s ISAE (UK) 3000-based approach offers phased readiness, limited, and reasonable assurance to strengthen governance, improve data reliability, and support consistent reporting. A single assurance report can also streamline oversight for multiple users, reducing duplication and improving audit efficiency. As sustainability requirements grow, assured third-party data is essential for transparency, resilience, and stakeholder confidence.

Where are you on your assurance journey?

03

How can we help you?

At KPMG, we have extensive experience of assurance reporting services and have been issuing these reports for several years over a wide range of topics including business operations and IT, Cybersecurity, supply chain or other specific subject matter that organisations have wanted to report on. We have used our expertise to help many businesses new to Controls Assurance to navigate the challenges of successfully implementing and operating formal assurance engagements.

We do not believe in a one–size–fits–all approach to assurance reporting, because it is a valuable tool to instill trust in a Service organisation's customers. To this end, we have helped organisations to better translate their assurance requirements into best fit and optimised assurance approaches over the years.

We can provide assurance using one or more of the available assurance standards and frameworks:

SOC 1 report (either reported through the ISAE 3402 standard, or combination with the AT–C 320 requirements); 1

SOC 2 report (reported through the ISAE (UK) 3000 standard), based on the Trust Services Principles and Categories (TSP 100): Security, Availability, Confidentiality, Processing Integrity and Privacy; 2

AAF 01/20 report, especially for pension management, investment management and related industries; and 3

ISAE (UK) 3000 for a wide range of operational or other subject matters. 4

If you are new to Controls Assurance, we are often able to help you undertake a Diagnostic/Readiness Assessment prior to embarking on a formal review cycle.

Where should you start

For Service Organisations that are new to assurance, starting with a readiness assessment is the right place to start.

A typical assurance journey for a Service Organisation starts with a simple diagnostic or readiness assessment. This is followed by formal reviews of your documented internal controls and ultimately into a mature cyclical assurance engagement process.

Readiness

Including documentation, assessment of internal control readiness and remediation plan.

Remediation

The time you need for remediating gaps and completing actions identified during the readiness stage.

Formal assurance engagement

Assurance through an independent service provider, either as at a specified date or over a period of time.

It's important to identify your principal risk areas and prioritise them in order for you to be able to get started. This can be done via scoping sessions and a series of workshops with relevant personnel to determine the material areas in scope for the services delivered to customers, as well as key operational, compliance and reporting risks.

Using these you will then need to bring together a formal control framework by identifying and documenting your key controls that mitigate those principal risks. It is advised that you use available guidance as a starting point. For instance, the COSO13 guidance can be used as a basis.

If there are controls that are not documented, performing a readiness assessment is a suitable course of action to get these documented. The key output of a readiness stage is a controls matrix – your documented internal controls with all the necessary information required to assess their design and operating effectiveness. Readiness assessments provide an indication of whether you have any material weaknesses and bring to light any gaps and improvements and the level of effort and resources that are required to remediate these.

Designing a SOC review

There are a number of factors involved in the design of a SOC engagement, controls are only one aspect of this! We have provided here the drivers and factors for the selection of the standard and the type and extent of the review that allows a Service Organisation to design a best fit approach to an assurance engagement.

Drivers for SOC review

Cost drivers

- Shared or Common Controls.
- Degree of customisations/homogeneity.
- Complexity of underlying technologies.
- Complexity of underlying service delivery.
- Changes in processes, services, technology and locations.
- Type of exceptions in prior years.

Control framework factors

- Testing/field work strategy and preparation needed.
- Degree of Standardisation of processes, technology and controls.
- Degree of process and control documentation.
- Control Design, Ownership and Monitoring.
- Control framework maturity and stability.

+

Assurance standard

User Entity Factors

- Reporting Period.
- Products/Services.
- Geography and Industry.
- Criticality to Financial Statements.
- Vendor Risk Management Programs.
- Controls sophistication/needs.
- Contractual Requirements.
- Complementary User Entity Controls (CUEC).

User Auditor Factors

- Audit Requirements.
- Reporting Period.
- CUEC.
- Financial Statement.
- Risk Assessment.
- Regulatory focus on ICOFR.
- Exception Evaluation.

=

The assurance report

SOC report

- Report Scope.
- Process and controls description.
- Control coverage.
- Exceptions and Management Response.
- Management assertion process.
- Other report linkage.
- Subservice organisations.

SOC Portfolio

- Types of Reports.
- Report Timing and Frequency.
- Report Consolidation.
- Platform Consolidation.
- Reporting Objectives and Priorities.

Assurance of AI

Our services are designed to help organisations build confidence in AI by providing a structured approach to responsible AI adoption and oversight, building trust with stakeholders and regulators through transparency and assurance.

SOC Reporting

- Independent attestation of control environment.
- Validates AI security, privacy, and system integrity.
- Builds trust through compliance.

Cyber Attestation

- Provides assurance over cybersecurity risk management.
- Demonstrates robust internal controls and transparency in managing cyber threats.
- Promotes transparency and trust.

Emerging Regulations & Technology

- Helps organisations comply with new AI–related security, privacy, and transparency regulations.
- Provides third–party assurance for trust .
- Simplifies complex regulatory requirements.

Digital Transformation – Assurance

- Real–time system assessments during transformation initiatives.
- Enables early identification and mitigation of risks.
- Supports smooth and secure organisational change processes.

Glossary

SOC Report: A System and Organisation Controls report is a third–party audit report that evaluates the internal controls of a Service Organisation.

FRC: The Financial Reporting Council is the United Kingdom's regulator responsible for promoting high–quality corporate governance and reporting to foster investment.

FCA: The Financial Conduct Authority is a financial regulatory body in the United Kingdom, operating independently of the UK Government, responsible for regulating financial firms and maintaining the integrity of the UK's financial markets.

PRA: The Prudential Regulation Authority is a part of the Bank of England responsible for the prudential regulation and supervision of banks, building societies, credit unions, insurers, and major investment firms in the United Kingdom. Its primary aim is to promote the safety and soundness of these firms, ensuring the stability of the UK financial system and protecting policyholders. The PRA sets standards and supervises financial institutions to reduce risks to the financial system and maintain public confidence.

ISAE (UK) 3000: The International Standard on Assurance Engagements (UK) 3000 is a standard for assurance engagements other than audits or reviews of historical financial information. It is issued by the FRC.

ISAE 3402: The International Standard on Assurance Engagements 3402 is a standard for reporting on controls at a Service Organisation, issued by the International Auditing and Assurance Standards Board (IAASB).

SSAE 18: The Statement on Standards for Attestation Engagements 18 is an attestation standard established by the American Institute of Certified Public Accountants (AICPA) that governs the performance of a variety of attestation engagements, including SOC reports.

AT-C Section 320: A specific section in SSAE 18 that sets out requirements and guidance for performing and reporting on engagements to examine and report on the effectiveness of a service organisation's internal controls, particularly those relevant to user entities' financial reporting. It is commonly referenced in SOC 1 reports alongside ISAE 3402.

AAF 01/20: The Assurance Framework 01/20 is a technical guidance issued by the Institute of Chartered Accountants in England and Wales (ICAEW) for Assurance engagements in relation to internal controls at Service Organisations.

AAF 05/20: The Assurance Framework 05/20 is a standard issued by the Institute of Chartered Accountants in England and Wales (ICAEW) for assurance engagements in relation to Master Trusts.

SOC 1: A System and Organisation Controls 1 report is an audit report that focuses on the internal controls over financial reporting at a Service Organisation, typically relevant to user entities' auditors in performing their audits of financial statements.

SOC 2: A System and Organisation Controls 2 report is an audit report that focuses on the internal controls related to security, availability, processing integrity, confidentiality, and privacy at a Service Organisation, relevant to user entities and stakeholders for Assurance purposes.

DORA: DORA is a regulatory framework established by the European Union aimed at ensuring that financial institutions within the EU can withstand, respond to, and recover from all types of Information and Communication Technology (ICT)–related disruptions and threats.

GDPR: A Regulation of the European Parliament and of the Council regarding the processing of personal data and on the free movement of such data, known as the General Data Protection Regulation.

EU AI Act: The EU AI Act is a regulatory framework for AI, emphasising risk–based classification and strict requirements for high–risk AI systems developed, deployed, or whose outputs are used in the EU.

Contacts:

Irene Sellars

Partner
UK Head of Controls Assurance
irene.sellars@kpmg.co.uk

Thomas Collins

Partner
Controls Assurance
thomas.collins@kpmg.co.uk

Allen Eccles

Director
Controls Assurance
allen.eccles@kpmg.co.uk

Willie McCabe

Director
Controls Assurance
william.mccabe@kpmg.co.uk

Binu George

Senior Manager
Controls Assurance
binu.george@kpmg.co.uk

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/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.

Document Classification: KPMG Public

Create | CRT164405A | January 2026