



SOC Reporting Benchmarking: Insights for your assurance journey

KPMG Controls Assurance Benchmarking Report 2024
(SOC 1 / 2, ISAE 3402 / SSAE18, ISAE (UK) 3000, AAF 01/20, AAF 05/20)

October 2024



Foreword

I am delighted to share with you the key trends and insights from our latest benchmarking study. This is one of the most comprehensive exercises we've undertaken in the UK for SOC Reporting, where we've analysed over 400 Controls Assurance reports issued in the past three years across multiple industries.

During this period, the number of SOC reports we issue has nearly doubled, increasing by more than 80%. This surge in demand for assurance is driven by a combination of regulation, a better understanding of supply chain risks, and businesses wanting to demonstrate a competitive edge.

Staying ahead of the regulatory compliance curve is a significant pressure for organisations. Examples include ISA 315 (revised), the SEC requirement on cybersecurity disclosure, the FRC's revised corporate governance code, DORA, and the FCA/PRA's critical third-party regime, among others.

The diversity of these regulations reflects the range of sectors demanding SOC reports within the last three years. While Financial Services still represent the largest proportion of our reports, we are now seeing increasing demand in other areas such as Technology, Professional Services, and Logistics.

From our benchmarking study, we found that control frameworks remain relatively static over the years. Entities should look to review their control frameworks every three years or so to ensure they align with the ever-changing risk landscapes.

It is also interesting to observe the mix of control types, with an extremely high degree of management review controls (40%) and conversely very low segregation of duties controls (3%).

Given the scrutiny of audit regulators over management review controls and the importance of effective segregation of duties controls, management should review the mix of their controls and diversify accordingly.

Our study finds that System Access exceptions represent 17% of all exceptions (one of the highest exceptions based on control types), while only 8% of this type of control is identified across all reports. Investing in strengthening System Access controls will significantly improve overall assurance results.

Another interesting trend is the growing uptake of SOC 2 for Technology and Professional Services clients, as well as emerging SOC reporting requirements to address ESG regulations (e.g., ESG value chain reporting) and the rapid proliferation of AI and GenAI.

Our 'Technology Story' is one we continue to evolve to deliver efficiencies and ultimately achieve higher quality audits. In this report, we share some examples of how we use AI in assurance, through Large Language Modelling (LLM) and intelligent automation platforms.

At KPMG, we're continually strengthening our Controls Assurance practice and our people to deliver consistent, high-quality reporting services to support organisations on their assurance journeys.

We trust this report will provide insights to inspire change in your journey too.



Irene Sellars

Partner,
Head of Controls Assurance
KPMG in the UK



The purpose of this Benchmarking Analysis

was to examine trends and patterns related to important aspects of Controls Assurance reporting and provide insight for organisations to consider in their own assurance reporting journey.

01

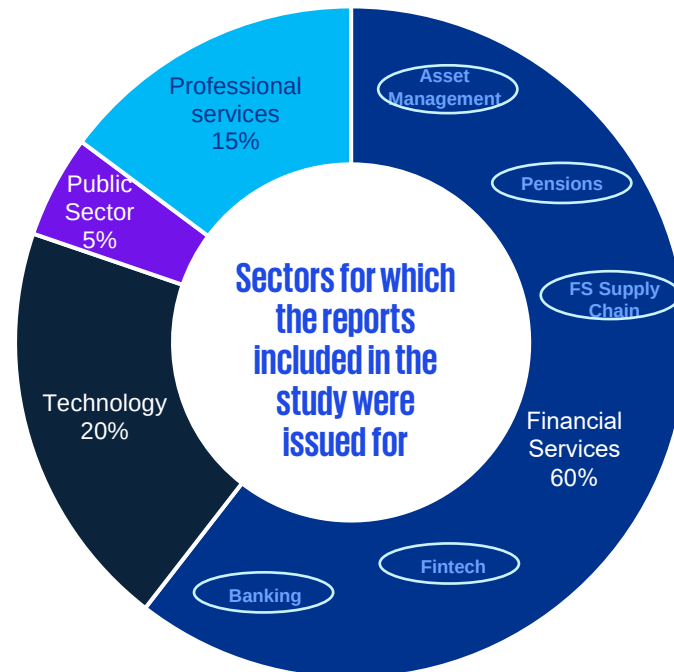
Benchmarking Analysis



At a glance: what did we find?

We performed an analysis of over 400 controls assurance reports issued between 2021 and 2023. These were specifically Controls Assurance reviews performed by KPMG LLP under the following frameworks / standards: SOC 1 (ISAE 3402 / SSAE 18), SOC 2 (ISAE (UK) 3000), AAF 01/20 and 05/20, and reports of other subject matters also reported under ISAE (UK) 3000.

The reports were issued for Financial Services, Professional Services (incl. Consultancy, Payroll, B2C, Business Process Outsourcing and Logistics), Technology and Public Sector.



@ **400+** Reports issued between 2021 and 2023



Insufficient change in control frameworks has been made to reflect modern risk landscape – such as cybersecurity threats, increased levels of adoption of new technology such as Artificial Intelligence (AI), or regulatory trends such as Operational Resilience.



The control types where exceptions are noted are consistently the same across the three years, especially Management Review, System Access and Authorisation controls.



Insight

Increased scrutiny from Users and their Auditors

In the last couple of years, we have seen a marked increase in scrutiny from user auditors as a consequence of control exceptions identified in Controls Assurance reports. This is particularly true when exceptions pertain to logical access and change management controls.

There are proactive steps that management can take to increase confidence and minimise additional questions and follow-on audits from user auditors or user organisations.

Key to this is for management to perform a robust impact assessment over:

1. The pervasiveness of the relevant exception to the full population (e.g. if a leaver account has been identified as an audit finding, then management should look to review whether there had been other similar occurrence of leavers over the full population);
2. Other compensating controls which operated effectively during the same period (e.g. user access reviews);
3. Whether risk has materialised due to the control failure (e.g. if a leaver account hasn't been revoked in a timely manner, has that account been used for unauthorised activities?); and
4. What remediation is needed, by whom and by when.

Management should then articulate the above impact assessment in their management responses. If appropriate, further explanation of remediation plans can also be provided in the 'Other Information' section of the Controls Assurance report.

For one of our Service Organisations, what was considered by them to be a low-risk exception for a logical access control led to multiple follow-up requests from their users and their auditors. This required the Service Organisation to provide additional evidence and perform further investigations into the exceptions and root causes. Management now perform a detailed impact assessment for exceptions noted.

This is strong evidence of the importance of management responses when preparing Controls Assurance reports, and the need for management to consider how their users might interpret exceptions and provide clear evidence of their impact assessment.

Volume and nature of controls

The number of controls increases with the complexity of the subject matter, period covered, and the number of control objectives / criteria to be met.

Reports related to Asset management and Technology sectors had the highest number of controls:

- Similarly, most of the reports issued for the Technology sector are under SOC 2, which again, prescribes a list of predefined criteria, and therefore require more controls to cover those.

55% of all reports had fewer than 100 controls. This is owing to the following reasons:

- AAF 05/20 reports (for Pensions Master Trusts) have smaller control frameworks (below 100 controls) compared to other reports.
- The UK entity for some sectors like Banking, is usually a sub-set of a Global provider, so the UK controls report would just be one of the component reports that feeds into a large global report. This has artificially skewed the proportion of reports with less than 100 controls.
- In some sectors such as Payroll processing, it is common to see lower number of controls (e.g. 50 - 70 controls), and a high number of reports in the same portfolio.

There are benefits and drawbacks to issuing a report under pre-defined criteria such as those under AAF 01/20 in the UK or the SOC 2 framework.

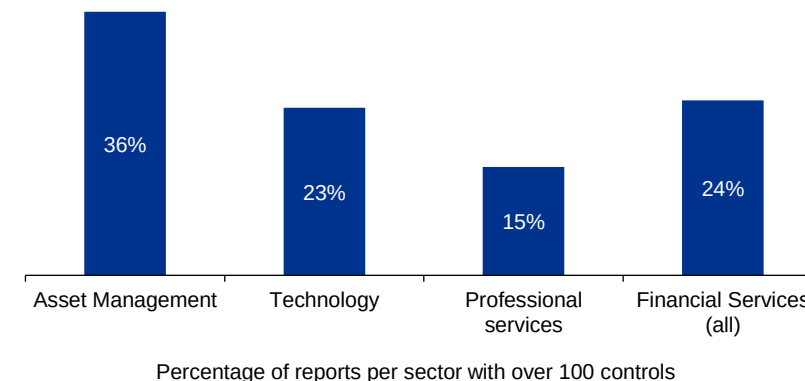
Having pre-defined criteria helps the Service Organisation to be objectively benchmarked against similar reports. For the Service Organisation, there is an industry wide standard to build their assurance framework around. Having more controls will likely mean a more robust control environment and potentially reduced likelihood of qualification.

The drawbacks of using a framework with pre-defined criteria are:

- An increase in the overall volume of controls means higher assurance cost overall.
- Predefined criteria like SOC 2 require a higher number of governance and policy type controls, which in turn means a larger volume of manual control activities (e.g.: Management Review) that are more likely to have exceptions. (See more on this in the section “Trends in exceptions”).



Percentage of reports with over 100 controls, by Sector



Percentage of reports with over 200 controls

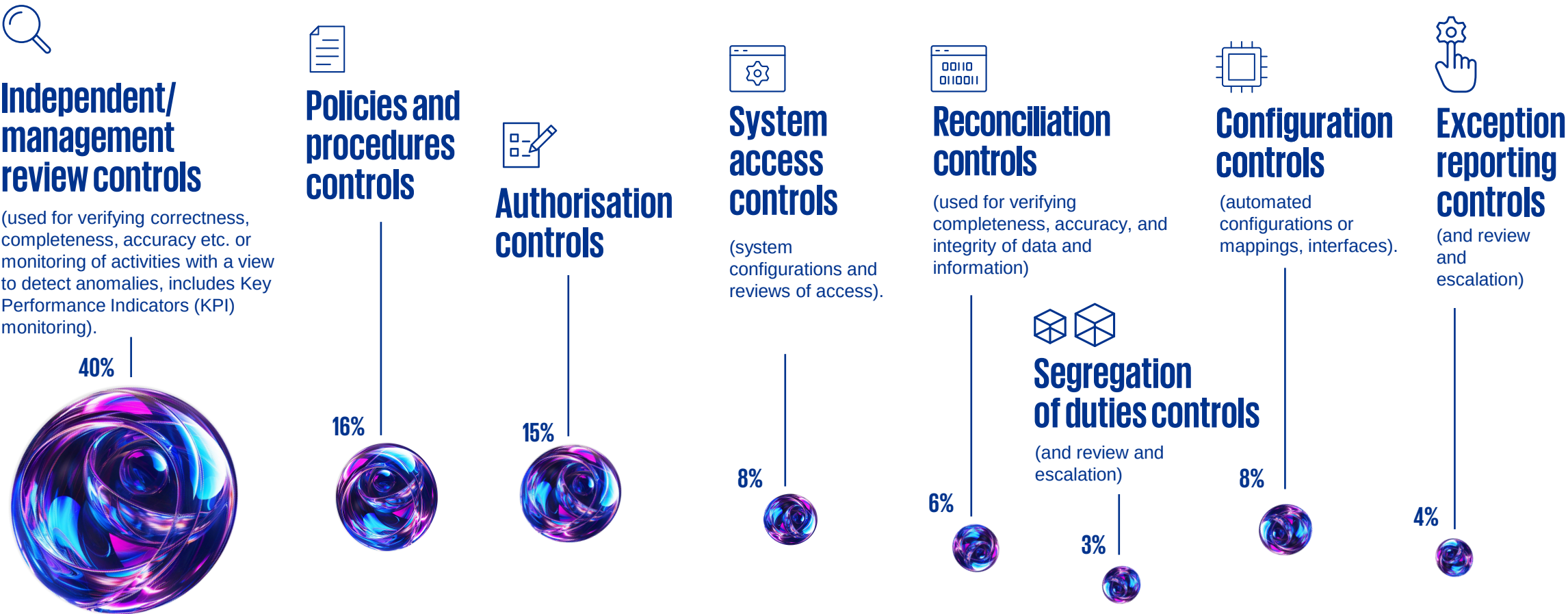
15% Avg. of 290 controls per report

Percentage of reports with 100-200 controls

30% Avg. of 140 controls per report

Control types

Controls assurance reports include several types of control activities defined by the Service Organisation and are based on the type of activity that is performed in the control. The Benchmarking analysis looked at the distribution of eight types of control activities that are typically found in control frameworks. These are shown below, ordered by the volume of each type found across all reports analysed. (There were also controls that did not fall into these categories, these have been included in an “Other” category in this analysis).



Control types (cont.)

Authorisation controls follow the same pattern as Management Review controls and were noted to be prevalent in AAF 01/20 reports than those issued under different standards / frameworks. In general, these controls are used more in Asset Management, Investment Management, Pensions and Financial Services reports.

Policies and procedures controls feature highly across sectors and reporting standards, with around 15% of all controls being of this type. For SOC 2 reports policies and procedures controls form 44% and 34% respectively for public sector and technology reports. For SOC 2, this is owing to there being predefined SOC 2 criteria that require controls over policies and procedures to be in place for a number of subject areas at the Service Organisation.

On average, **segregation of duties (SOD) controls together account for only 1 - 5 % of all controls** across all types of reports. In our professional experience, we believe that SOD controls are key in the prevention of fraud (e.g. payment authorisation) and expect these to represent at least 10% (most sectors) and up to 20% (specific sectors such as Asset Management, Payment, Treasury, etc.).

Only 35% of system access controls are automated, with the rest manually operated (e.g. periodic reviews of access to in-scope systems are manual controls, these account for 22% of all manual system access controls).

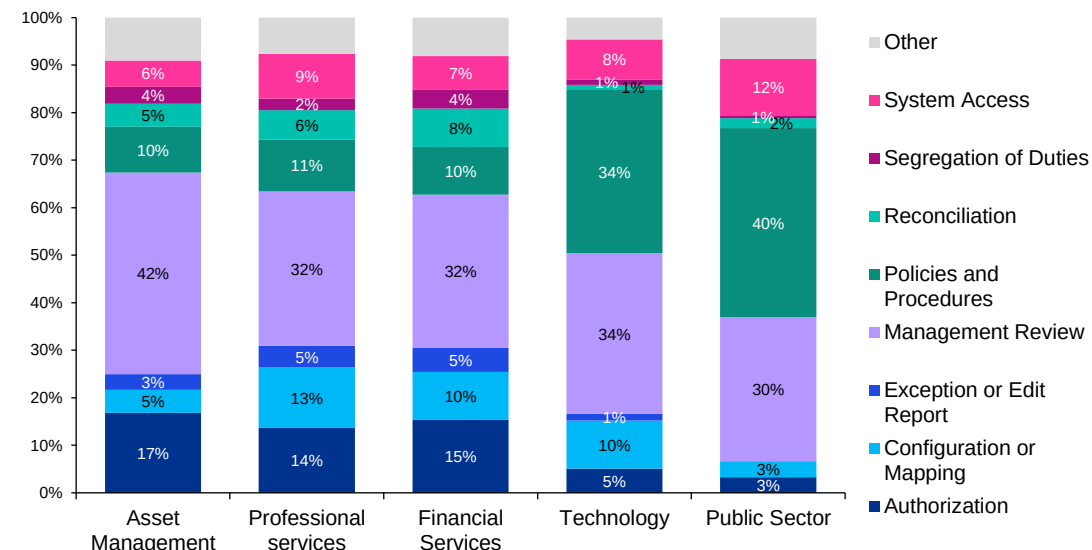
In the last few years, the FRC and PCAOB have focused their attention on the effectiveness of Management Review controls and the audit of these controls. When designing and implementing Management Review controls, management should take care to consider:

1. The nature and extent of outliers that the control is designed to identify.
2. The knowledge, experience and skills of the person performing the control.
3. Whether there are any automated components (and reliance on those automated components).

It is prudent to consider whether there are sufficient controls of other types of controls in the control framework (for instance Reconciliations, Authorisations / Approval, Segregation of Duties).



Types of controls across reports by sector



Preventative vs. Detective for manual and automated controls (all reports)

We expect to see an even split of preventative and detective / corrective controls in a typical framework. **Over the years, there has been a welcome increase in the overall number of preventative controls (46% in 2021 vs 61% in 2023), and a small increase of automated controls (12% in 2021 vs 15% in 2023).**

94% Of **detective** controls are **manual**

20% Of **preventative** controls are **automated**

02

A closer look

Findings analysis and
observations



Control exceptions

Controls reports conclude on the Service Auditor's opinion based on the results of the tests performed. Typically, control exceptions are higher in tests of operating effectiveness when compared to tests of design and/or implementation.

Where these results lead us to conclude that the exceptions are material and that they impact the achievement of a control objective / criteria, the opinion will carry a qualification.

Type I reports are usually issued at the beginning of the Service Organisation's assurance journey. Given the audit requirements only pertains factual accuracy and design / implementation of controls as at a point in time, there is less challenge to meet these, hence these reports carry fewer exceptions. It is rare to have Type II reports without exceptions. In fact, the first Type II reports typically have a high number of exceptions and may even be qualified. Type II reports typically see fewer exceptions and qualifications from Year 2 onwards.

Exceptions occur for a variety of reasons due to limitation of testing or unavailability of evidence or owing to more sophisticated audit procedures including lack of evidence for completeness and accuracy of populations used for testing controls.

Manual controls have a higher risk of failure and conversely, automated controls have a lower likelihood of failure.

Overall, the higher volume of manual controls in reports across the board has also meant significantly higher proportion of exceptions were found in manual controls.

Percentage of reports issued with no exceptions



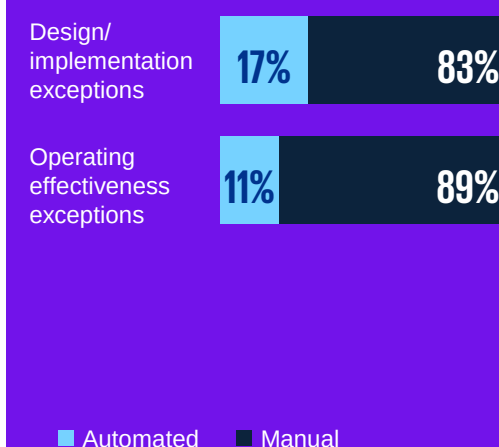
A large number of Type I reports being issued without exceptions does not mean these are better reports. Type I reports without exceptions are typically owing to controls only tested as at a point in time and typically tested for one instance of the control.

Percentage of overall reports that were "Qualified"



Around 20% of the reports that we benchmarked have been qualified across sectors. Typically, matters resulting in qualifications are associated with exceptions in General IT Controls (particularly logical access controls and change management) and third party management.

Percentage of manual / automated controls with exceptions



Trends in exceptions

The control types with the highest number of exceptions noted on tests of operating effectiveness in Type II reports, have remained consistent. Exceptions noted on Management Review controls, System Access controls and Authorisation controls continue to be the highest contributors to overall control exceptions noted across the period. Since timeliness and lack of evidence are key contributors to findings on System Access controls, automating the processes around Access Management such as access revocations and User Access Reviews may help reduce findings in this area.

Percentage of exceptions by control types

30%

Of exceptions on Management Review controls

17%

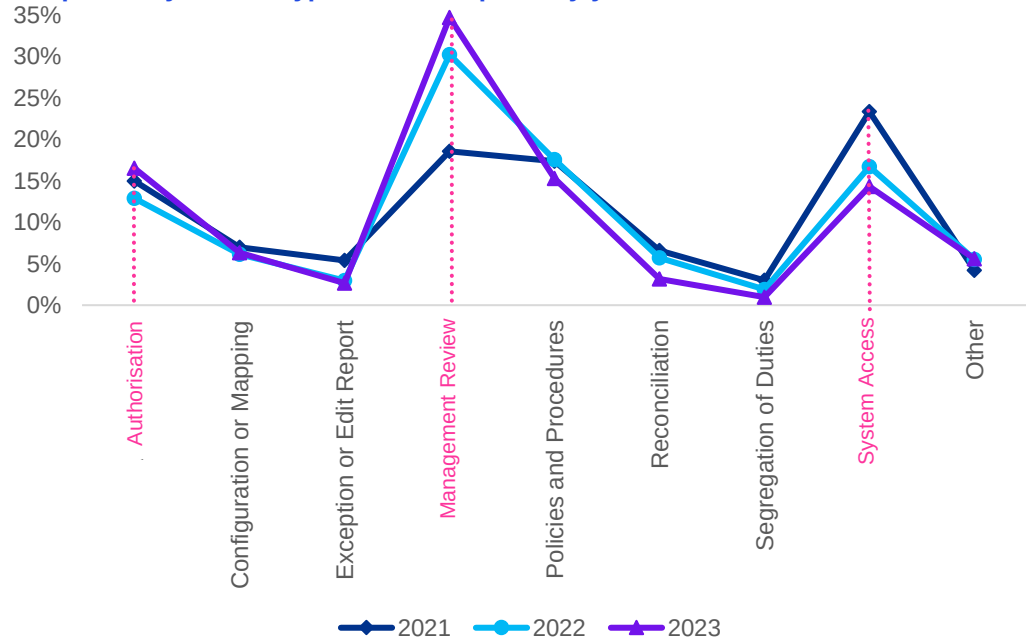
Of exceptions on System Access controls

15%

Of exceptions on Authorisation controls

Management Review controls make up for 40% and Authorisation controls make up 15% of all controls. Whilst System Access only makes up 8% of controls across reports, therefore improvements made in System Access controls will have a more far reaching impact in improving the overall control framework.

Exceptions by control types across reports by year



These results are for reports issued across multiple sectors and for this reason, they provide an indication of which areas organisations need to focus on first when they look to improving and strengthening their control environment.

Exceptions across sectors

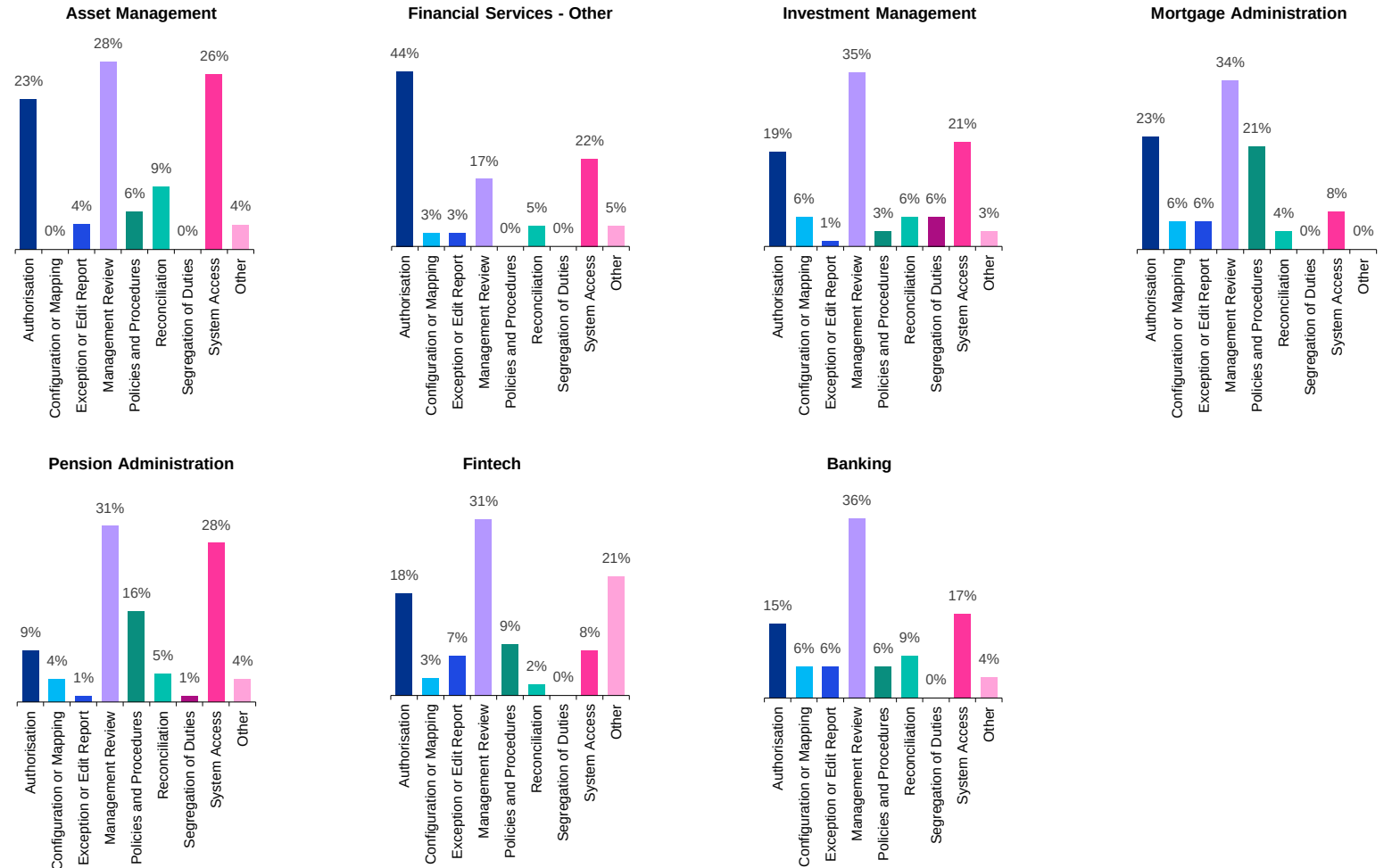
The in-depth analysis of exceptions revealed that reports related to Financial Services exhibit a different pattern of exceptions compared to non financial services reports. The primary factor is the higher level of standardisation across the Financial Services sector, largely in consideration of the illustrative control objectives outlined in Appendix 1 of AAF 01/20 (issued by the ICAEW).

System Access-related findings were consistently noted across reports for all Financial Services sectors. These findings were most prevalent in the Asset Management and Pension Administration sectors. Other significant contributors to control exceptions included Management Review controls and Authorisation controls.

Automating authorisations, as well as exception reporting and reviews against pre-defined criteria, may provide an effective mechanism for reducing findings in Management Review controls. This approach would also help ensure timeliness and enhance the quality of evidence for retrospective reviews and audits.

Across all reports, the overall volume of controls has seen little change over the past three years, and the percentage of controls with findings has followed a similar trend.

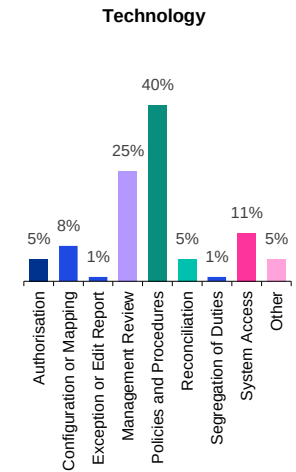
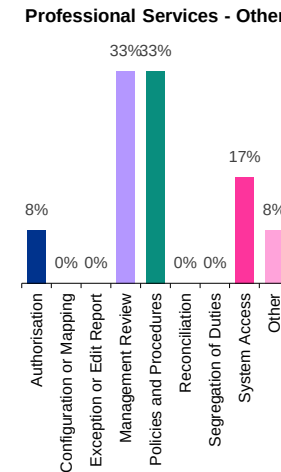
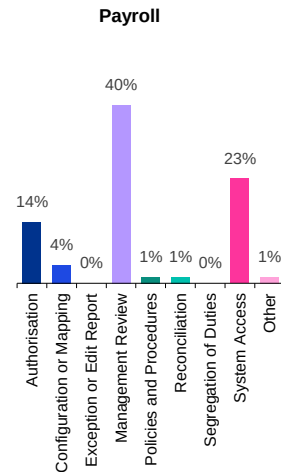
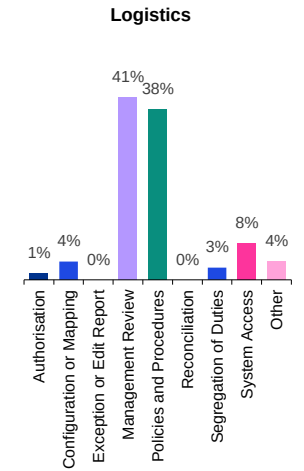
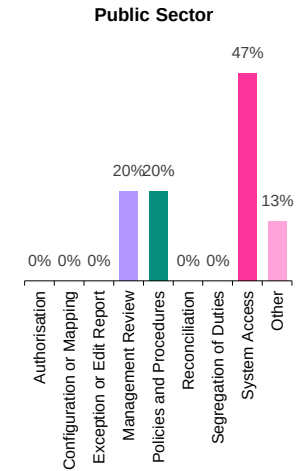
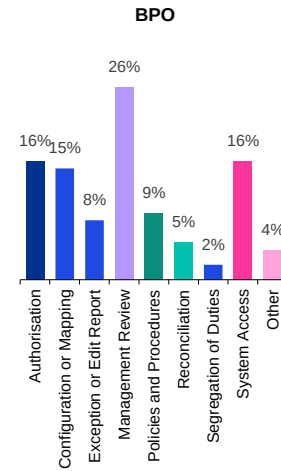
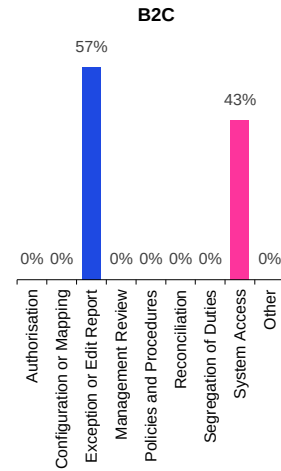
Financial Services sector: Exceptions across reports by subsector and by type of control



Exceptions across sectors (cont.)

For non financial sector reports, exceptions follow a less defined pattern. Although we still see challenges with System Access controls, we also see exceptions in other type of controls such as Exception / Edit Report (in B2C), Configuration and Reconciliation controls (in BPO).

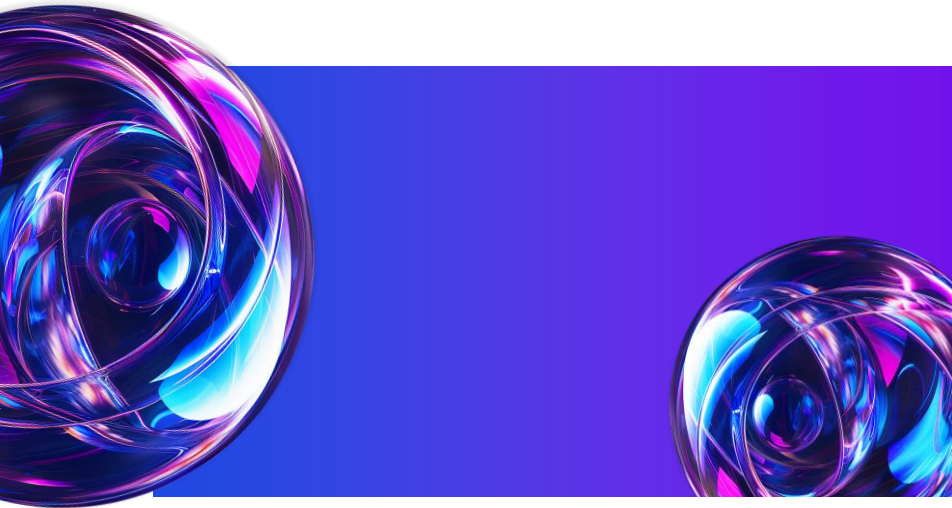
Non-Financial Services sector: Exceptions across reports by subsector and by type of control



Reality of internal controls

Areas of concern

- **Lack of control evolution:** little change in control types / coverage over the three year period examined.
- **Exceptions occur in the same areas.** Control types with exceptions remained consistent across the three year period.
- **Fixing the gaps:** exceptions identified were often not remediated, and continued to appear in subsequent years.
- **Covering emerging risks:** low or no coverage of hot topics.



Call to action:

- **Align risks and controls**, in particular by reviewing the strategic / emerging risk register and assessing whether controls adequately address both the risk, and stakeholder expectations.
- **Follow-through on remediation commitments** so that gaps reported are fixed, and to prevent repeat exceptions in the same risk areas.
- **Communicate with customers / report users** so that they're aware of progress being made to address issues, and don't have to wait 12 months until the next controls assurance report is issued.



Case study: 1

Completeness and Accuracy

As audit and regulatory pressures are increasing, auditors now have higher expectations with regards to completeness and accuracy of information relevant to the controls assurance report. Specifically:

1. Information used by the service organisation in the performance of a control.
2. Information used by the service auditor as a population from which to select a sample of control instances to test operating effectiveness.

Consequently, service auditors are now required to perform more in-depth analysis and test procedures to gain comfort over completeness and accuracy of information.

Completeness

Service auditors will need to obtain evidence to show that information provided by the service organisation contain all relevant items and have not been filtered to exclude any articles that should form part of their testing.

Accuracy

Service auditors will need to obtain evidence to show that information provided by the service organisation contains data that is both relevant and comes from a reliable source.

Inability to evidence completeness and accuracy of information may be determined as an exception.

Top tips

To avoid exceptions with regards completeness and accuracy of information, service organisations should consider the following:

1. 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.
2. Where possible, system generated lists should be used to provide information direct from the system.
3. 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. (See also Case study 2 where we talk about the use of Large Language Modelling in this context).

03

Emerging trends to watch out for

Actions for Service Organisations



Regulatory drivers insight

UK Corporate Governance, DORA



UK Corporate Governance code requirements



In January 2024, the FRC updated the UK Corporate Governance Code in relation to internal controls. This is another driver of stakeholder demand for trust and transparency.

The updates made the Board responsible not only for establishing, but also for maintaining the effectiveness of the risk management and internal control framework. The board should monitor the company's risk management and internal control framework and, at least annually, carry out a review of its effectiveness.

New for the 2024 Code, the FRC is now asking Boards to explain through a declaration in their Annual Reports how they have done this in relation to 'material controls', and their conclusions.

These material controls are expected to cover financial, operating, reporting, and compliance controls, i.e. going significantly further than financial reporting controls alone.

We have seen examples of Boards going beyond the Code by seeking independent assurance over the operating effectiveness of their material controls, through ISAE (UK) 3000 reporting.

Management identify material risks before designing, implementing and operating their corresponding material controls to address those risks.

Auditors like KPMG then provide assurance over those controls as at the balance sheet date. Note that this is an emerging area, and we anticipate issuing the first of these reports in early 2026.

The Code is a further driver for Boards and management to stand back and critically evaluate their risk, control, and assurance strategy.

Digital Operational Resilience Act (DORA)



Regulatory changes like the review of critical supplier risk in financial services, the SEC's new cybersecurity disclosure requirements, and the EU's Digital Operational Resilience Act (DORA), are increasing the pressure on business, and in turn, their suppliers, to demonstrate a robust control environment.

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.

DORA sets out requirements for risk management, incident reporting, digital operational resilience testing, and third-party risk management. The primary goal is to enhance the operational resilience of financial entities and safeguard the stability of the financial system.

DORA, in particular, will increase the focus on the technology sector as these services will often underpin many of those provided by financial entities.

We have observed a significant increase in requirements by our technology clients for them to provide assurance to their financial services clients to satisfy the DORA requirements.

As there is a significant overlap between DORA and the SOC 2 framework, we have analysed and mapped both requirements to offer a tailored SOC 2 assurance aligned with DORA.

If you need help with your DORA requirements, do get in touch.

Regulatory drivers insight

SEC's Cybersecurity disclosure



SEC's Cybersecurity disclosure requirement – A snapshot



In 2023, the SEC introduced new rules for cybersecurity disclosures aimed at enhancing transparency and consistency for investors. Key requirements:

Incident Disclosure:

- Public companies are required to report material cybersecurity within four business days of determining the incident's materiality.

Annual Reporting:

- Companies are required to describe their cybersecurity risk management, strategy, and governance in their annual reports.
- Annual reporting requires describing detailed processes for assessing and managing cybersecurity risks, the impact of previous incidents, as well as the role of the Board and management in overseeing management of these risks.

Governance:

- Companies need to disclose how their Board perform oversight of cybersecurity risks and the expertise of management in handling these risks.

Foreign Private Issuers:

- Disclosures are also required for foreign private issuers for incidents, risk management and governance. (Form 6-K) for incidents and Form 20-F for risk management)

How can a SOC 2 help organisations ?



SOC 2 reports are critical for material service providers of an organisation in ensuring cybersecurity and assisting with SEC disclosures:

- **Demonstrates Compliance:** SOC 2 reports demonstrate that the service provider complies with established standards for managing customer data based on trust services categories (security / availability / processing integrity / confidentiality / privacy). This compliance is essential for SEC disclosures as it shows the organisation's proactive steps to secure data.
- **Risk Management:** SOC 2 reports provide detailed insights into the cybersecurity controls and practices of the service provider. This information is vital for organisations to assess and manage risks associated with third-party vendors, which is a key aspect of SEC cybersecurity disclosures.
- **Transparency and Accountability:** By obtaining a SOC 2 report, a service provider demonstrates transparency and accountability. This transparency aligns with SEC requirements for clear and detailed disclosure of cybersecurity practices, incidents, and risk management strategies.
- **Incident Response:** SOC 2 reports often include information on how the service provider handles and responds to security incidents. This data is crucial for SEC disclosures as it helps outline the steps taken to mitigate and manage cybersecurity threats and breaches.
- **Continuous Monitoring and Improvement:** Regular SOC 2 audits indicate that the service provider is continuously monitoring and improving their cybersecurity measures. This ongoing commitment can be highlighted in SEC disclosures to show that the organisation is not only compliant but also dedicated to enhancing their cybersecurity posture.

Insight

How can SOC for Cybersecurity help you for your SEC's Cybersecurity disclosure?

SOC for Cybersecurity is a reporting framework issued by the AICPA, which is designed to provide assurance about the organisation's overall cybersecurity posture. It focuses on the organisation's cybersecurity risk management program and the effectiveness of controls related to cybersecurity.

Similar to SOC 2, SOC for Cybersecurity is also based on the Trust Services Principles and Categories (TSP 100): Security, Availability, Confidentiality, Processing Integrity and Privacy.

A SOC for Cybersecurity report provides a robust and credible foundation for an entity to support its SEC cybersecurity disclosures. Here are some reasons why a SOC for Cybersecurity report can support SEC Cybersecurity disclosures:

Comprehensive Evaluation: The SOC for Cybersecurity report includes a thorough evaluation of the organisation's cybersecurity risk management programme, covering all critical aspects such as security, availability, processing integrity, confidentiality, and privacy.

Independent Assurance: The report is prepared by an independent Chartered Accountants or qualified practitioner, such as KPMG, providing an unbiased opinion on the effectiveness of the organisation's cybersecurity controls. This adds credibility and trust to the disclosed information.

Structured Framework: Based on the AICPA's TSP Section 100 criteria, the report follows a structured and standardised approach, ensuring consistency and comprehensiveness in the evaluation of cybersecurity controls.

Detailed Information: The report includes management's description of the cybersecurity risk management programme, management's assertion about the effectiveness of controls, and the practitioner's report. This detailed information can be used to support the entity's disclosures about its cybersecurity practices and risk management efforts.

Alignment with Regulatory Requirements: The SOC for Cybersecurity report aligns with the expectations of regulatory bodies like the SEC, which emphasise the importance of effective cybersecurity risk management and transparent communication of cybersecurity risks and incidents.

Emerging trends to watch closely

When looking to strengthen the control framework by reassessing risks, objectives and controls, there are a few emerging trends that Service Organisations must pay attention to in the context of their own services as well as those of their own outsourcing partners.



Cybersecurity

Cybersecurity is a growing concern priority and is now part of the risk landscape for an increasing number of organisations. Benefits of technology that improves cybersecurity are being seen as outweighing the costs of deploying them. With large scale cybersecurity failures becoming more frequent, customers want to see Service Organisations demonstrate their resilience and secure service delivery. KPMG International's report on AI in financial reporting and audit, 2024, found that cybersecurity was one of the biggest concerns that firms have about the use of traditional AI in financial reporting processes.

Assurance reports function as a proven way to help build trust and demonstrate strong, resilient control environments to protect against cybersecurity incidents. Increasingly service organisations are using SOC 2 framework to provide assurance to their users on Cybersecurity.

In parallel with SOC 2, another suitable framework for non service providers is the SOC for Cybersecurity, which is used to provide assurance about the organisation's overall cybersecurity posture. It focuses on the organisation's cybersecurity risk management program and the effectiveness of controls related to cybersecurity.

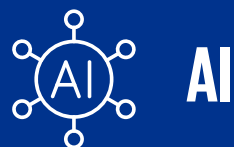


Digital transformation

With growing economic and political uncertainty, the importance of having the right priorities is increasingly important for any organisation. Embracing new technology is what gives organisations an edge over competition. For instance, the KPMG global tech report 2023, where over 2000 executives were interviewed across 16 countries, found that despite the tighter budgets and resource constraints, there is an increased interest and buy in from leadership for emerging technology. This survey reported that most organisations surveyed were already using digital transformations to improve performance.

Given this context, the possibility of making service delivery more efficient and profitable for customers is an exciting prospect for Service Organisations, this also means a significant investment in risk management and compliance. Controls assurance reviews, specifically diagnostic and readiness assessments, are extremely useful tools for initiating change in this area.

Emerging trends to watch closely (cont.)



AI

Artificial Intelligence (AI) is transforming operations and reporting structures of organisations, and it is here to stay. The **EU AI Act** introduces a comprehensive 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.

The **UK's AI White Paper** directs UK regulators to develop sector-specific rules ensuring AI systems are "safe, secure, and robust," with transparent, explainable decisions. With 86%* of companies testing or using AI, it's critical to establish robust governance and controls to comply with new and upcoming regulations. Companies must address risks such as biases and data protection while meeting legal mandates.

Ensuring and assurance compliance builds trust and confidence among stakeholders.

Organisations should be prepared for regulatory attestation requirements related to their AI governance frameworks. Review of AI governance, policies and procedures, AI controls assurance and AI assurance readiness are options available to organisations as they are navigating fast developing AI regulatory landscape and respond to risks associated with AI. This is a new and emerging area for KPMG, and we are maturing our approach and methodology to deliver AI assurance in the UK.

*Introduction to AI assurance - GOV.UK (www.gov.uk)



ESG value chain assurance

We believe that pre-assured ESG data & methodologies will give competitive advantage for ESG data providers in the market. It could deliver significant cost advantages to their customers too who are legally required to seek assurance over their sustainability reporting.

Assurance is now legally mandated within EU's Corporate Sustainability Reporting Directive (CSRD) and is likely to be included under the US SEC rule (for GHG metrics), California rule and is a very likely within UK's ISSB implementation plan too.

Throughout our ESG Assurance practice, we have been raising audit findings over the difficulty of assuring 3rd party ESG data in all our ESG Assurance Reports in the last year.

We continue to see this as one of the biggest challenges in assuring clients who use ESG data from third party providers. There is no doubt that this will be a key competitive driver in the ESG data market, their customers will start to expect it as a part of your service and not simply as a value add.

If you are an ESG data providers who requires assurance, do get in touch as we'd love to help you!

Case study: 2

Audit with AI

At KPMG, we are at the forefront of leveraging AI and other advanced technologies to deliver high-quality audits. One of our innovative approaches involves the use of Large Language Modelling (LLM). Language models can analyse vast amounts of textual data, helping to identify relevant information, patterns, and insights. For instance, tools such as RelativityOne© enable us to significantly speed up the review process while increasing its accuracy.

Another AI tool we utilise is DataSnipper©, which automates, simplifies, and accelerates the audit process by extracting, cross-referencing, and verifying data. This tool enhances our ability to perform thorough and efficient audits.

The following case studies illustrate how we use each of these tools to transform our audits and ultimately deliver high-quality assurance.

Case 1:

At one of our assurance entities, we had concerns regarding the completeness and accuracy of the populations provided by management for the assured controls. To address this, we conducted a Large Language Modelling (LLM) exercise using RelativityOne© to validate these populations against source documents.

We enlisted our Forensics Technology team to automatically interrogate over 600GB of email data, which contained requests sent by user organisations to our entity. This allowed us to recreate each of the populations in question.

Our efforts resulted in matching the populations generated by management for more than 80% of the controls. This significantly increased our confidence in the completeness and accuracy of these populations, ultimately leading to a higher quality audit.

Case 2:

At another assurance entity, we aimed to test the sufficiency of property insurance coverage. However, we lacked confidence in the completeness and accuracy of the property listing provided by management.

To address this, we utilised DataSnipper© to review hundreds of transaction documents, thereby gaining assurance over the property listing and the related insurance coverage.

This tool enabled us to create and review the listing efficiently and effectively, while ensuring the completeness and accuracy of the population.

04

What can you do to stay ahead of the curve?

Actions for Service Organisations



Immediate actions for service organisations

Service Organisations face several challenges with market, customers and other stakeholders. From a controls assurance perspective, having a robust controls framework that is based on updated business and external risks provides a firm foundation for reducing their impact. For Service Organisations that are already issuing controls reports, there are some immediate actions to consider in the short term.

Diagnostic assessments are a good method of getting it right with assessing risks and controls. These can be performed ahead of readiness for a specific standard/framework or even as a controls refresh project to cover wider base of controls over and above the scope of any externally issued reports.

01

Are your risks up to date?

Assess your existing control objectives and risks to identify changes that may be required. This may sound obvious but a comprehensive review performed enterprise-wide could take anything from six to nine months.

Start with mapping your existing risks and controls, including those that may not be covered in your existing controls reports. Identify gaps and involvement management and control operators to plan appropriate remediation for the identified gaps.

We recommend this activity is performed every three years or so.

02

Are your controls sufficient?

Understand whether the existing controls are sufficient to mitigate existing and new risks, paying special attention to areas where previous controls reviews have identified weaknesses, both material and non-material.

For example, System Access has been one of the areas with the highest number of findings. Management should consider improving these processes through automation or adding preventative controls. Similarly, there is a high reliance on manual controls such as management review controls. Automating some processes and implementing other types of controls such as Segregation of Duties controls and automated preventive controls can help audit outcomes significantly.

03

What is your state of change?

You may be growing/expanding with more customers or service offerings. Or, there may be an IT or business transformation project in progress. Consider any changes to the way you operate and the impact of these on your risks and controls.

Not all change would be relevant to the services you provide your customers. However, you may have to include controls that mitigate risks related to ongoing projects if these are material to the service you provide to your customers.

Immediate actions for service organisations (cont.)



If you manage large volumes of sensitive / personal / confidential / transactional data for your clients or provide material financial processing for (for example - payments, payroll, claims, loans, deposits) your clients, you may want to consider SOC 2 assurance reporting.

This is especially relevant if are an IT cloud outsourcing company (with services such as cloud hosting, cloud email, SaaS-based HR services) where security, availability and privacy key focus points.

04

Are you fully aware of your clients' assurance needs?

Your customers' risks change and with it their assurance requirements will also change. Further to this, their Auditors may also require more information than what they may have needed previously.

Take steps to have an open dialogue with your customers to identify how their assurance needs can be met in an efficient and effective manner. Consider available compliance work that you have (e.g. Internal Audit, etc. etc.), that can be shared with clients to meet additional assurance needs. If the scope of their current external assurance report needs amending, then look to plan and agree an objective and commercially effective way to incorporate the change.

05

What technologies are you introducing into your operations?

A significant proportion of our clients are introducing new and improved ways of delivering their services, including cloud computing, robotic process automation and use of AI.

We have already shown that the proportion of automated controls in control frameworks is on an increasing trend. With the introduction of automation and AI, you may need to revisit your assurance reporting approach. For example, will you need SOC 2 to cover the increased risks on managing data securely.

Where should you start

For Service Organisations that are new to assurance, the most immediate action for you is to start planning for it right away.

A typical assurance journey 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 review 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 reviews

Assurance (internal/external), 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.

Where should you start (cont.)

Once you have completed the actions identified during the readiness stage to fix all the issues and gaps, you can look for either internal or external assurance. Internal assurance typically is carried out by a second or third line team. Some companies outsource their internal assurance provision in this area. External assurance is done with the assistance of an independent assurance provider and follows an established standard.

Below is an example of what a simplified controls matrix may look like. This is only an excerpt from a control framework and therefore will not show a full set of controls required to meet the control objective shown:

Control area – area within which the activity falls	Control objectives are statements of intent of what an organisation looks to achieve, based on the risks being managed (sometimes also called “criteria”)		Control descriptions are internal control activities that help the organisation manage risks within the relevant business processes	Evidence that you will be required to provide	Actions for remediation phase		Indicative view of whether the control objective is achieved
Control Area	Control objective per AAF 01/20 standard	Control ref.	Indicative control	Evidence	Gaps/issues	Control finding	Achievement of control objective
AUP: Authorising and processing transactions	Investment transactions are authorised, executed and allocated accurately within agree timescales	AUP 1	Each fund has a documented Prospectus which defines how the fund operates. On an annual basis, each Prospectus is reviewed by Risk and Compliance. The CEO signs off the annual reviews.	Inspected: - Prospectus for a selected fund. - Annual review checklist completed by Risk and Compliance for a selected fund.	There is no formal process for documenting the CEO sign off of the annual Prospectus reviews.	Poorly documented controls or deficient controls.	Criteria achieved – improvement areas identified
		AUP 2	On a weekly basis, the Investment Strategy Committee (ISC) meeting is held to discuss investment strategy, portfolio positioning, and transactions. This is attended by the CIO, Heads of Investment, and Risk and Operations. Actions are documented in the ISC action log and owner allocated. These are then investigated and discussed at the next ISC meeting.	Inspected: - ISC meeting minutes for a selected week. - ISC action log spreadsheet.	There is no versioning of the ISC action log spreadsheet, therefore we were unable to evidence that actions had been investigated and discussed at the next ISC meeting.	Poorly documented controls or deficient controls.	

Designing a SOC review

There are a number of factors involved in the design of a SOC review, 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 review.



Drivers for SOC review



Assurance standard



The assurance report

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

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

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



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 reviews.

We do not believe in a one-size-fits-all approach to assurance reporting, because it is a valuable tool to instil 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 SSAE 18 standard);
- 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;
- SOC for Cybersecurity report, also based on TSP100;
- AAF 01/20 report, especially for pension management, investment management and related industries; and
- ISAE (UK) 3000 for a wide range of operational or other subject matter.

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

Glossary

SOC Report: A Service organisation Control report is a third-party audit report that evaluates the internal controls of a service organisation.

ISA 315 (revised): The International Standard on Auditing 315 (Revised) is a standard issued by the International Auditing and Assurance Standards Board (IAASB) which focuses on identifying and assessing the risks of material misstatement in financial statements.

SEC: The Securities and Exchange Commission is a U.S. government agency responsible for regulating the securities industry, enforcing federal securities laws, and overseeing securities exchanges and other entities.

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

PCAOB: The Public Company Accounting Oversight Board is a non-profit corporation established by the U.S. Congress to oversee the audits of public companies and broker-dealers to protect investors and the public interest by promoting informative, accurate, and independent audit reports.

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 around 1,500 banks, building societies, credit unions, insurers, and major investment firms in the UK.

ESG: Environmental, Social, and Governance criteria are a set of standards for a company's operations that socially conscious investors use to screen potential investments.

Glossary (cont.)

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: This is a mirror standard of ISAE 3402, applicable in the US. 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.

AAF 01/20: The Assurance Framework 01/20 is a standard 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 Service Organisation Control 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 Service Organisation Control 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.

SOC for Cybersecurity: A System and Organisation Controls (SOC) for Cybersecurity is an audit report that focuses on the organisation's cybersecurity risk management programs.

Similar to SOC 2, the SOC for Cybersecurity report is also based on the AICPA's TSP Section 100 (Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy).



Authors:



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

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

Your Swiss contacts:

KPMG AG

Badenerstrasse 172
PO Box
8036 Zurich
Switzerland



Stefan Wälti

Partner
Head of Assurance Technology
swaelti@kpmg.com
+41 58 249 68 94



François El Assad

Director
Assurance Technology
felassad@kpmg.com
+41 58 249 66 51

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.

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Document Classification: KPMG Public

CREATE: CRT157109A | August 2024