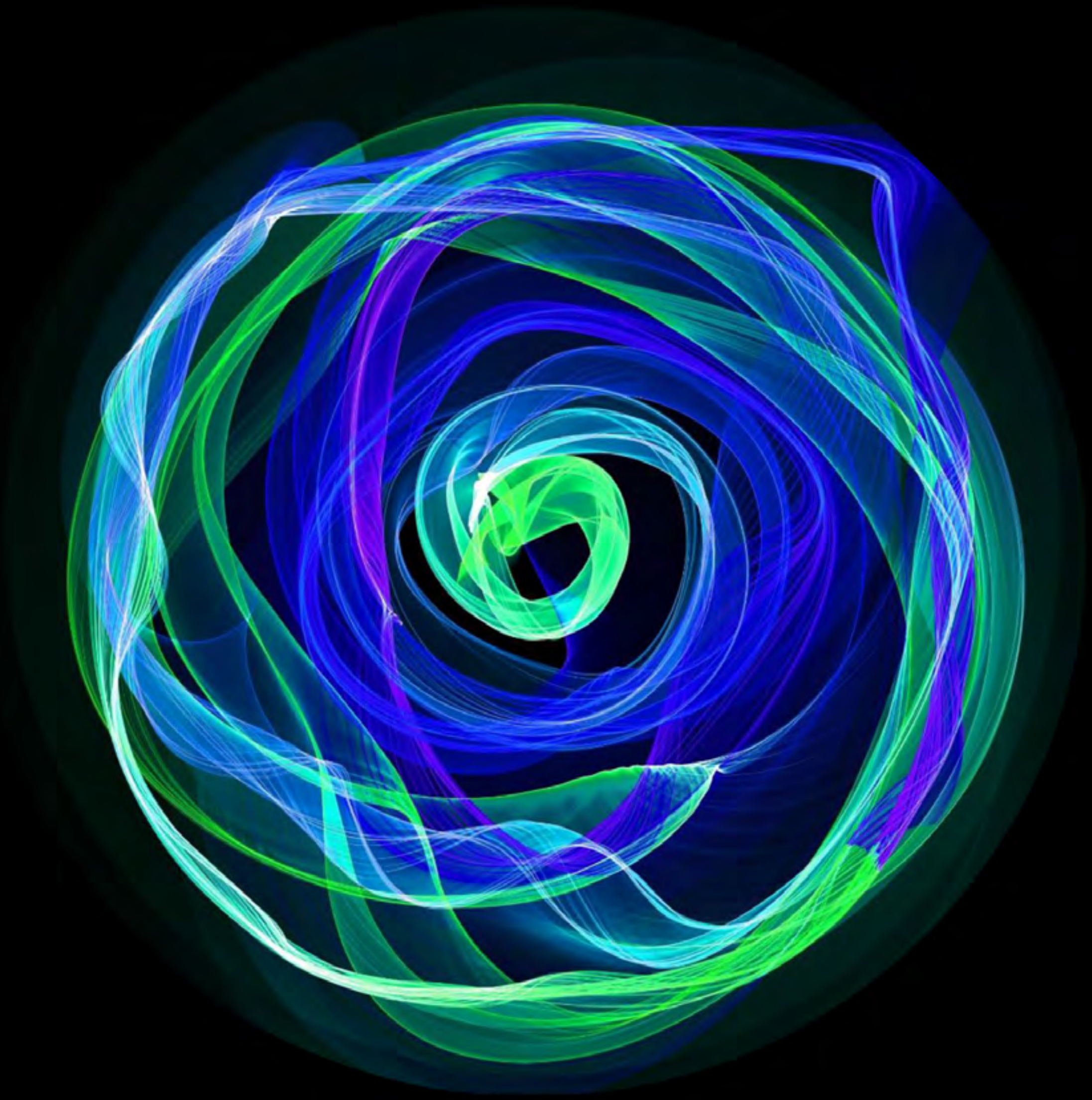
Deloitte.



Third Party Assurance

Providing Assurance through System and Organisation Controls (SOC) Reports

MAKING AN IMPACT THAT MATTERS since 1845

Many companies rely on ISAE 3402, SOC 1 and SOC 2 reports to address outsourcing risk, Sarbanes-Oxley (SOX) and other compliance requirements.

Service organisations often find themselves serving many industries across multiple geographies, which expands the range of compliance and regulatory requirements they must meet.

Under increasing compliance pressures, companies are asking their service organisations to demonstrate the efficacy of their controls to higher degrees. In some cases, SOC reports have become a prerequisite for service organisations to win new business with established companies.

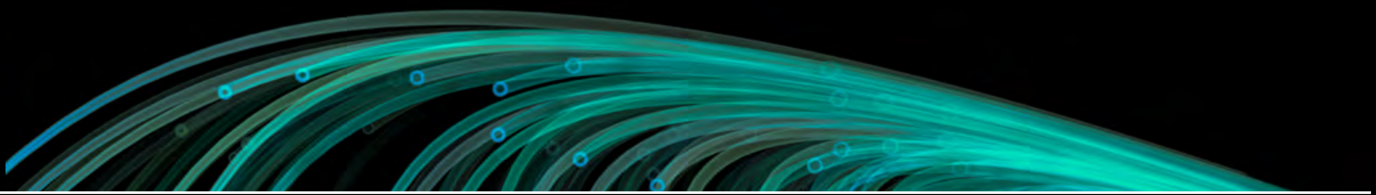
According to the American Institute of Certified Public Accountants (AICPA)[1] & Chartered Institute of Management Accountants (CIMA)[2] 2020 SOC Survey, there is a growing market for SOC services with a 49% increase in demand for SOC 2 engagements between 2018 and 2020.

The Deloitte Global Third Party Assurance (TPA) Survey from 2022 further indicates a growing volume and intensity of risk domains and emerging areas of cybersecurity, privacy and ESG where organisations are looking to SOC reports (including SOC 2+) to bring the wide range of assurance requirements together.

Let us take you through what you need to know about providing assurance to customers, business partners, regulators, and auditors through SOC reports.

- How a SOC report works
- Benefits of a SOC report
- SOC 1 and SOC 2 comparisons
- SOC 2 trust services categories
- SOC 2 additional options
- Components of a SOC report
- Typical path for a new SOC report
- SOC readiness assessment
- Selecting your service auditor

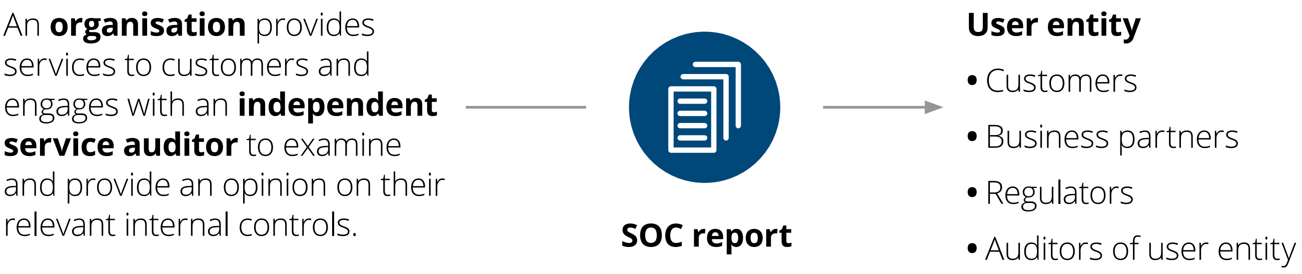
Click here to get more insights from our Global TPA Survey.



[1] The American Institute of Certified Public Accountants
[2] Chartered Institute of Management Accountants

How a SOC report works

The SOC report framework enables an independent auditor to perform procedures and issue and opinion on the internal controls at a service organisation.



An **organisation** provides services to customers and engages with an **independent service auditor** to examine and provide an opinion on their relevant internal controls.

SOC report

User entity

- Customers
- Business partners
- Regulators
- Auditors of user entity

Benefits of a SOC report

- **Audit and Regulatory**
  May be used by user entities in support of regulatory and legal requirements, including SOX
- **Responding to Requests**
  May be leveraged to respond to internal control and audit requests from suppliers, customers, and their auditors
- **Control Environment**
  Brings focus on internal controls and control environment in accordance with COSO framework
- **Contracting**
  Assists in meeting contractual requirements for existing and prospective customers
- **Risk Management**
  Provides an opportunity to further enhance enterprise and third party risk management and monitoring
- **Compliance**
  May be leveraged to provide assurance related to compliance with certain requirements specified by customers and government agencies

SOC Report Comparisons

The most common third party assurance reports are SOC 1 and SOC 2 reports.

SOC 1

- Examination of controls relevant to internal control over financial reporting , intended to meet the needs of user entities evaluating for their use entity financial statements
- Customised control objectives and controls with consideration to services provided and related financial statement assertions
- Scope can be business and/or IT controls
- Report issued in accordance with ISAE 3402 or AICPA's SSAE 18 standard

SOC 2

- Examination of controls related to specific trust categories (security, availability, processing integrity, confidentiality, or privacy), service commitments, system requirements, and potentially compliance (SOC 2+)
- Standard trust services criteria (TSC) in which controls are identified and mapped to
- Scope is IT controls for specified products or services
- Issued in accordance with ISAE 3000 or AICPA's SSAE 18 standard and AICPA 2017 Trust Services Criteria

Type 1 and Type 2 Reports

Type 1

- Reports on an organisation's description of controls, whether such controls were suitably designed and whether they had been placed in operation as of a specified date as of a point in time (e.g. as of 30 June 202X)
- Most often performed only in the first year of a SOC report

Type 2

- Includes everything in the Type I report plus testing the operating effectiveness of controls over a specified time period (e.g. 1 January to 31 December 202X)
- Includes a description of the testing procedures performed by the service auditor and the results of testing performed

SOC 2 Trust Services Categories

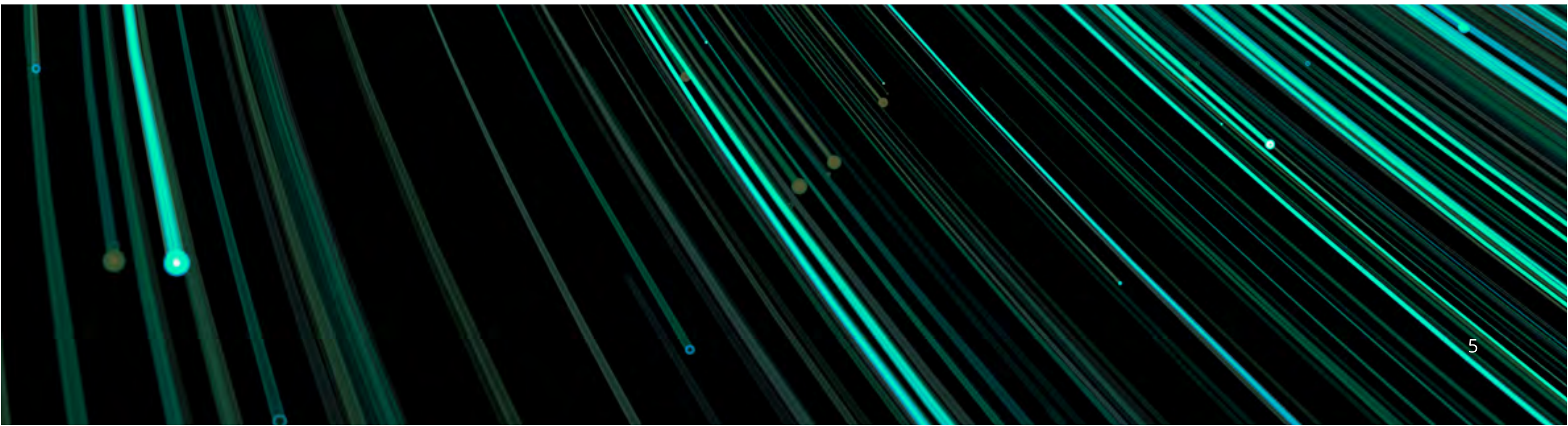
SOC 2 represents an examination on controls relevant to the following trust services categories, which are mapped to TSC.

Trust Services Categories

Category	No. of TSC
Security* against unauthorised access or appropriation, either logical or physical	33
Availability**, addressing continuity of operations	3
Processing Integrity**, including complete, accurate, and timely processing	5
Confidentiality** of information	2
Privacy** in keeping with AICPA's trust principles and the organisation's privacy policy (e.g. Personally Identifiable Information (PII) and confidential data) or other regulations	18

*Mandatory
**Optional

Security Category	No. of TSC	
Control Environment	5	*Aligned with the 17 principles in the COSO framework*
Information and Communication	3	
Risk Assessment	4	
Monitoring	2	
Control Activities	3	
Logical and Physical Access Controls	8	*Other Required Common Criteria*
System Operations	5	
Change Management	1	
Risk Mitigation	2	
Total	**33**	

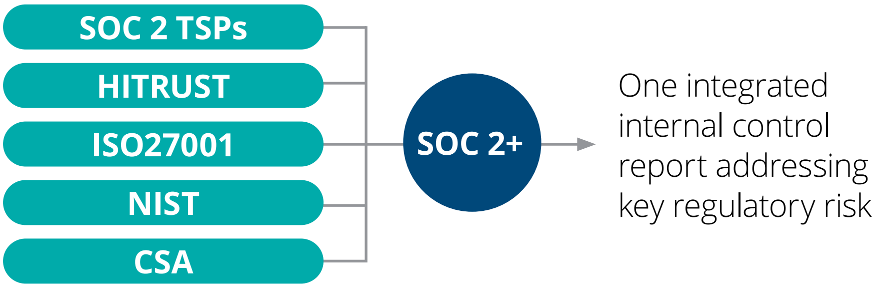


SOC 2 Additional Options

Adding Other Criteria (SOC 2+)

The AICPA has provided a great deal of flexibility regarding inclusion of other control criteria in a SOC 2 report, creating the concept of a SOC 2+ report. Such a report can be used to demonstrate assurance in areas that go beyond the Trust Service categories and address industry specific regulations and requirements.

Additional "suitable criteria" added to a SOC 2 report must be objective, measurable, complete, relevant, and available.

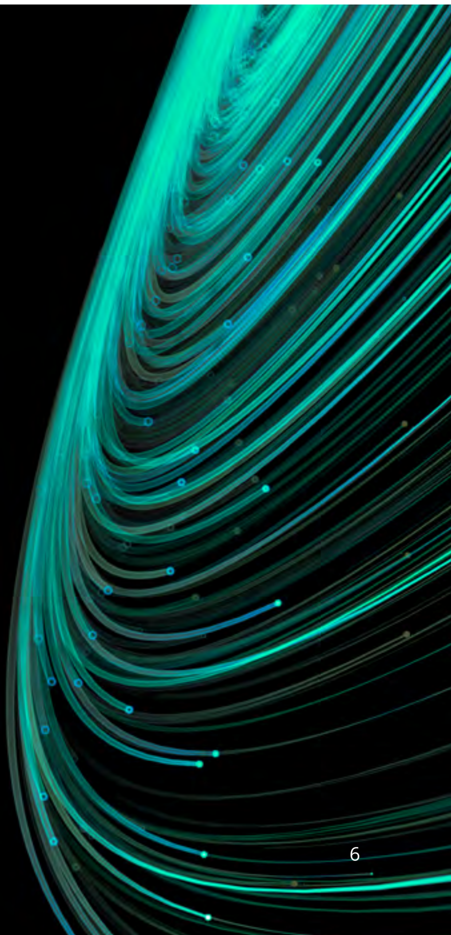


One integrated internal control report addressing key regulatory risk

SOC 3

- An examination with same underlying scope as a SOC 2, however with the issuance of a "slimmed down" report that is available for general use
- Publicly available for anyone to view
- May be utilised for marketing material
- Includes the independent service auditor opinion, management assertion, and boundaries of the system (no detailed testing matrix)

Framework	SOC 2+ Example
Health Information Trust Alliance (HITRUST)	A claims processor must have access to HIPAA data in order to execute its responsibilities. To demonstrate that it is adequately safeguarding personal health information, it maps controls in their SOC 2 to the HITRUST framework.
National Institute of Standards and Technology (NIST)	A company that maintains governmental contracts for building roads and bridges has contractual obligations to demonstrate how it meets the latest revision of NIST. To demonstrate adherence to the NIST framework, it maps controls in their SOC 2 to NIST 800 53.



Components of a SOC Report

Report Section No.	Section Name for SOC 1 Report	Section Name for SOC 2 Report
Section 1	**Independent Service Auditor’s Report** Independent auditor attestation that expresses an opinion on related subject matter. The possible opinion outcomes are unqualified opinion, qualified opinion, adverse opinion, or disclaimer of opinion.	
Section 2	**Management’s Assertion** Written assertion from management that describes the criteria and informs user entities about how the controls are designed and intended to operate to achieve the applicable control objectives or trust services criteria. In addition to being a component of the SOC report, management’s assertion is also included as in appendix within the Management Representation Letter, which is signed by Company executive management and provided to the service auditor.	
Section 3	**Description of the System** Management’s description of the system, which incorporates a narrative description of key elements such as an overview of business operations, control environment, systems, controls that achieve control objectives, complementary user entity controls, and complementary subservice organisation controls.	**Description of the System** Management’s description of the system, which incorporates a narrative description of key elements such as an overview of business operations, control environment, systems, controls that achieve the service commitments and system requirements, based on the trust services criteria, system boundaries, complementary user entity controls, and complementary subservice organisation controls.
Section	**Information Provided by Independent Service Auditor Except for Control Objectives and Control Activities** Testing matrix with control objectives, control activities, tests of operating effectiveness, and exceptions.	**Information Provided by Independent Service Auditor Except for Trust Services Criteria and Control Activities** Mapping of trust services criteria to controls, along with a testing matrix that includes control activities, tests of operating effectiveness, and exceptions.
Section 5 (optional)	**Other information provided by the service organisation** This optional section is presented by management to provide additional information not subject to the examination. For example, management’s response to identified exceptions could be added to this section.	

Typical Path for New SOC report

SOC Readiness

We have developed a structured approach designed to prepare for your initial attestation.

	1. Define Report Scope	2. Assess Current State	3. Draft Description	4. Remediation	5. SOC Attestation
Objectives	**Define the scope relevant to SOC**	**Understand current state of controls**	**Draft initial description**	**Remediate gaps**	**Plan and perform SOC attestation**
Key activities	Define the following: • Products and services • Business processes* • Control objectives* • System boundaries** • Systems • Locations • Subservice organisations • User entities	• Perform walkthroughs • Map controls to control objectives or TSC • Assess design and implementation of controls • Identify gaps in achieving control objectives or TSC	Prepare initial draft of the description, including: • Principal service commitments and system requirements** • System boundaries** • Control objectives* • Control descriptions • Complementary user entity controls (CUECs) • Complementary subservice organisation controls (CSOCs)	Remediate gaps in achieving control objectives or TSC, which may include: • Designing and implementing new controls • Enhancing execution of existing controls • Enhancing documentation as evidence of controls	• Plan attestation considering readiness and remediation status • Determine report type, reporting period, and target issue date • Perform necessary actions for attest service (independence, background checks, etc.) • Develop test plan and perform tests of controls

Legend

Key activities are typically applicable to all types of SOC reports, unless otherwise noted.

*Applicable to SOC 1

**Applicable to SOC 2

Note: The service auditor performing the examination can assist and advise the company in readiness activities, however it cannot assume any management roles including remediation.

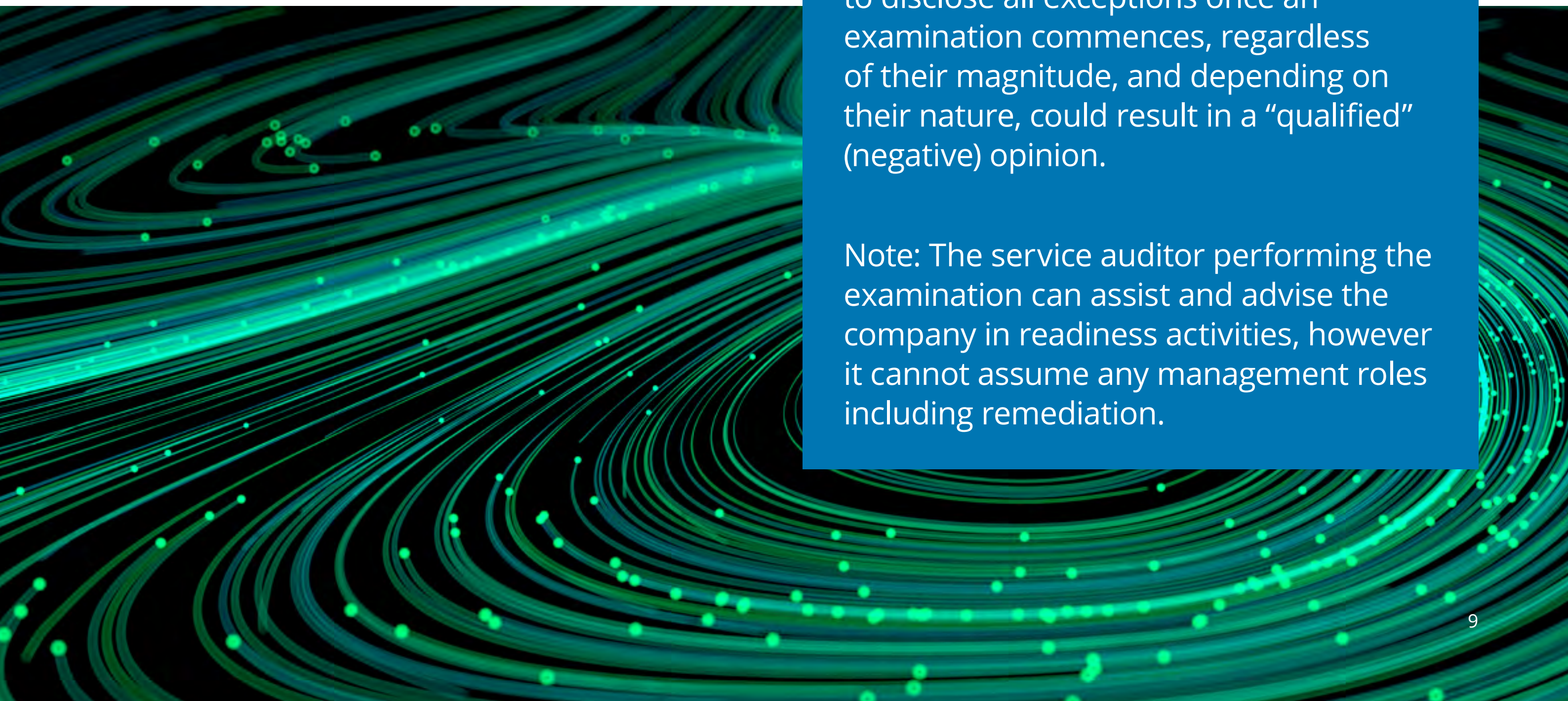
SOC Readiness Assessment

A readiness assessment is a "pre-audit" that provides a basis for understanding control gaps and remediation efforts in preparation for a future SOC attestation. As part of a readiness engagement, Deloitte may assist management in the following areas.

- Assist in defining report scope that may be useful to address the needs of user entities
- Advise on potential control objectives that may be useful to user entities for inclusion in a SOC 1 report
- Conduct interviews with control owners and review available documentation to assist management with drafting the control activities. Provide feedback on the coverage of control activities to achieve the control objectives or the service commitments and system requirements, based on the trust services criteria
- Advise on the identification of design or implementation control gaps and potential enhancements (new controls, enhanced documentary evidence, modified existing controls, etc.)
- Assist management with drafting portions of the description, such as:
  - Narrative description of control activities that support control objectives or trust services criteria
  - Potential user entity control considerations (i.e., controls that user entities would be expected to have in place)
  - Potential complementary subservice organisation controls (i.e., types of controls that subservice organisations would be expected to have in place)

An additional thought
Identifying and remediating any control gaps prior to embarking upon a formal SOC examination is critical, as the audit standards require the service auditor to disclose all exceptions once an examination commences, regardless of their magnitude, and depending on their nature, could result in a "qualified" (negative) opinion.

Note: The service auditor performing the examination can assist and advise the company in readiness activities, however it cannot assume any management roles including remediation.



Your SOC Service Auditor Makes A Difference

Why Deloitte?

SOC Leader

Deloitte is a leading provider of SOC services, issuing thousands of SOC reports annually. Representative clients range from emerging companies embarking on their first SOC report to listed multinational companies with many SOC reports.

Brand Reputation

Deloitte has stood the test of time for more than 175 years. Our reputation is a testament to our commitment to quality and our core values of integrity, objectivity, and technical excellence. Deloitte provides highly effective solutions and brand recognition that promotes trust and confidence.

AICPA Collaboration

In the US, Deloitte has served as an advisor to the AICPA for the past 25+ years. Deloitte participates in AICPA working groups responsible for developing authoritative guidance for emerging areas of assurance. Deloitte recently presented at the 2022 AICPA & CIMA SOC & Third Party Risk Management Conference.

Our Practice

We have an extensive team of professionals who specialise in internal controls, risk management, cyber security, ICFR/SOX, and information systems. With 1,050 Risk Advisory professionals in Africa alone, we have the breadth and depth of qualified resources.

Our team is connected globally, with specialised delivery capability in all major geographies.

Audit Quality Leader

Deloitte is a market leader in audit quality, which is backed by a rigorous quality focus and results in leading class assurance. We have demonstrated superior inspection results, with the lowest number of deficiencies in the PCAOB's Part 1 when compared to the other firms.[1]

Within South Africa we have received 100% good or acceptable quality outcomes on the engagement files selected for review by the IRBA and no reportable findings on our system of quality control in 2022 and 2023.

[1] https://pcaobus.org/oversight/inspections/firm-inspection-reports

Let’s talk

Africa TPA Leaders

Trevor Wright
Risk Advisory Africa
Associate Director
Mobile: +27 11 209 8244
trewright@deloitte.co.za

Jan Herbst
Risk Advisory Africa
Senior Associate Director
Mobile: +27 11 202 7571
jherbst@deloitte.co.za

Risk Advisory Africa Leaders

Southern Africa

Greg Rammego
Risk Advisory Africa
Managing Director
Mobile: +27 11 806 5255
grammego@deloitte.co.za

Michele Townsend
Risk Advisory Africa
IT and Specialised Assurance
LeaderDirect: +27 11 806 5992
mntownsend@deloitte.co.za

East Africa

Urvi Patel
Risk Advisory East Africa Leader
Mobile: +254 71 405 6887
ubpatel@deloitte.co.ke

West Africa

Temitope Aladenusi
Risk Advisory West Africa Leader
Mobile: +234 19 041 730
taladenusi@deloitte.com.ng

Central Africa

Tricha Simon
Risk Advisory Regional Leader
Mobile: +263 867 700 0261
tsimon@deloitte.co.zm

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s approximately 415 000 people worldwide make an impact that matters at www.deloitte.com

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.