Service Auditor Reporting
Provide assurance to your customers and win in the marketplace
Organisations are:

- Increasingly focusing on their core competencies, and
- Strategically outsourcing non-core activities to service providers to reduce costs and increase margins

To establish trust and win in the marketplace, service providers must demonstrate strong governance and internal controls over the services they provide.

Organisations face increasing demands from their end customers and regulators, and these demands are passed onto the service provider. The service provider needs to be able to provide assurance – often through a service auditor report that best suits the needs of its stakeholders.

What is a service auditor report?

A service auditor report provides assurance around the control environment and key controls designed by the service provider to govern its critical systems. Service auditor reports include Service Organisation Control (SOC) reports (SOC 1, SOC 2, and SOC 3) as well as other assurance reports.

Service auditor reports can be used by management to assess their internal control environment – but more importantly, they can be used by clients, regulators, and depending on the type of report, the public at large to gain assurance over key risks such as information security, availability of systems, integrity of data processing, confidentiality and privacy.

Why would a service auditor report benefit you?

A service auditor report allows you to demonstrate a strong internal control environment. A service auditor report can be shared with numerous clients and stakeholders, avoiding the need for multiple audits to be conducted by each of your customers. This will limit the operational disruptions and time and cost impacts to the organisation.
## Types of Reports

<table>
<thead>
<tr>
<th>Professional standards</th>
<th>SOC 1 reports</th>
<th>SOC 2 / SOC 3 reports</th>
<th>Other assurance reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISAE 3402</td>
<td>ISAE 3000</td>
<td>Agreed upon procedures</td>
<td></td>
</tr>
<tr>
<td>SSAE 18</td>
<td>SSAE 18</td>
<td>Others in various</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>jurisdiction</td>
<td></td>
</tr>
</tbody>
</table>

### Subject matter
- Controls relevant to control over financial reporting
- Controls relevant to security, availability, processing integrity, confidentiality or privacy
- Controls relevant to a specific purpose or agreed upon procedures required by the stakeholder

### Purpose
- Financial reporting controls
- Operational controls
- To address a specific compliance requirement or agreement between two parties

### Intended users
- Management of service organisation, management of user organisations, user organisation auditors
- SOC 2 reports are intended for parties knowledgeable about the services, interactions, internal control and criteria (including clients, management, regulators, etc.). SOC 3 reports can be shared with the public at large.
- Specific stakeholders (e.g. specific client, management, regulators, etc.)

---

### Why Deloitte?****

- We have a global team of information technology security, audit and controls specialists
- We have extensive SOC 1, 2 and 3 audit experience with small, medium and large organizations
- We follow a proven approach/methodology that is scalable to organizations of all sizes
- We are thought-leaders demonstrated through our involvement in associations such as ISACA and AICPA.
- We have a unique approach and experience in start-up SOC 1, 2 and 3 audit situations
- We are recognised for our independence and objectivity

---

The service provider needs to be able to provide assurance – often through a service auditor report that best suits the needs of its stakeholders.

---

### How can you prepare for a service auditor report?****

Deloitte recommends leveraging a proven roadmap strategy to get to the desired end state over time.

---

#### Timeline

1. Understand customer needs and expectations
2. Define scope
3. Perform readiness assessment ("pre-audit")
4. Remediate identified gaps
5. Type I audit
6. Control deficiency remediation, if any
7. Type II audit (first time, may have some control deficiencies noted)
8. Control operating effectiveness deficiency remediation, if any
9. Type II audit (fewer or no deficiencies noted)
For more information on the best way to provide assurance to your clients and other stakeholders, please contact:

**Navin Sing**  
Managing Director: Risk Advisory Africa  
Mobile: +27 83 304 4225  
Email: navising@deloitte.co.za

**Shahil Kanjee**  
Risk Advisory Africa Leader: Cyber & Technology Risk  
Mobile: +27 83 634 4445  
Email: skanjee@deloitte.co.za

**Sisa Ntlango**  
Director: Risk Advisory Southern Africa  
Mobile: +27 82 920 3677  
Email: snlandgo@deloitte.co.za

**Mark Victor**  
Director: Risk Advisory Southern Africa  
Mobile: +27 82 772 3003  
Email: mvictor@deloitte.co.za

**Chris Lotter**  
Director: Risk Advisory Southern Africa  
Mobile: +27 82 572 7413  
Email: clotter@deloitte.co.za

**Vonani Chauke**  
Director: Risk Advisory Southern Africa  
Mobile: +27 83 486 0415  
Email: vchauke@deloitte.co.za

**James Alt**  
Associate Director: Risk Advisory Southern Africa  
Mobile: +27 72 163 9356  
Email: jamalt@deloitte.co.za

**Trevor Wright**  
Senior Manager: Risk Advisory Southern Africa  
Mobile: +27 83 675 7997  
Email: trewright@deloitte.co.za

**Anthony Olukoju**  
Risk Advisory Regional Leader: West Africa  
Mobile: +234 805 209 0501  
Email: aolukoju@deloitte.com.ng

**Ibukun Beecroft**  
Director: Risk Advisory West Africa  
Mobile: +234 805 901 6634  
Email: ibeecroft@deloitte.com.ng

**West Africa**

**Julie Nyangaya**  
Risk Advisory Regional Leader: East Africa  
Mobile: +254 720 111 888  
Email: jnyangaya@deloitte.co.ke

**Urvi Patel**  
Director: Risk Advisory East Africa  
Mobile: +254 714 056 887  
Email: upatel@deloitte.co.ke

**Central Africa**

**Tricha Simon**  
Risk Advisory Regional Leader: Central Africa  
Mobile: +260 973 224 715  
Email: tsimon@deloitte.co.zm

**Rodney Dean**  
Director: Risk Advisory Central Africa  
Mobile: +263 867 700 0261  
Email: rdean@deloitte.co.zw
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte Legal means the legal practices of Deloitte Touche Tohmatsu Limited member firms or their affiliates that provide legal services. For legal, regulatory or other reasons not all member firms provide legal services.

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) 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 entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2018. For information, contact Deloitte Touche Tohmatsu Limited.