Assurance through Attestation

Key points for understanding and enabling Attestation in your organization.

Select the right professional services firm – one with the industry depth, knowledge, and insight to help clients address their most pressing issues.

2016

kpmg.com
With increased global competition and cost pressures, companies are outsourcing more of their key business functions to service organizations. What can they do to gain confidence over their business processes? KPMG has a solution to help companies meet their control assurance needs.
# Table of Contents

The Increasing Need for Attestation for Service Organizations/Outsourcers ........................................... 4

Solutions to Fit your Attestation Needs ........................................... 5

Applicability of SOC Reports ........................................... 7

Overview of SOC Reporting ........................................... 8

Reporting Types and Structure ........................................... 12

SOC Report Structure ........................................... 13

Phases for Preparing for and Issuing a SOC Report ........................................... 14

KPMG’s Attestation Services ........................................... 15

Conclusion ........................................... 16
The Increasing Need for Attestation for Service Organizations/Outsourcers

Companies are increasingly outsourcing non-core business functions. Nonetheless, companies are ultimately responsible for their control environment. This has led to increased demand for control assurance for activities performed by third parties. KPMG understands the risks and challenges associated with outsourcing and can help companies meet the growing demand for control assurance.

Increased global competition
Global economic competition and cost pressures have driven companies to increase outsourcing to service organizations. Outsourcing is no longer confined to routine back-office tasks. It now frequently deals with initiating, recording, processing, and reporting an organization’s transactions, which can have a direct impact on an organization’s financial statements and key business processes.

Emerging threats
The increase in the outsourcing information brings increased risks and security concerns. Companies could suffer operational, reputational, and financial damage from the security deficiencies of outside service organizations that result in real or perceived breaches of customer information.

Consumers are also becoming increasingly sensitive to the measures taken to protect their personally identifiable information (PII) and protected health information (PHI).

Risks to companies increase when the outside service organization processes and stores customers’ private and/or confidential information, performs transaction processing for multiple clients, and is audited by their clients or regulators. An independent examination of the critical IT and business operations that have been outsourced can help companies identify and control these risks.

Regulatory requirements
Increased regulatory requirements (e.g. the Sarbanes-Oxley Act) are putting pressure on organizations to obtain and provide assurance that their controls are effective. As with responding to increased global competition, ensuring compliance with regulatory standards also requires assurance that outsourced IT systems and processes have the proper controls.

Bottom line benefits
Both service organizations and user entities can find noticeable benefits with Service Organization Control reporting. User entities gain comfort over the outsourced aspects of their business while service organizations can see immediate gains, such as the following:

- Reduction in interruption to business operations by multiple user organization audits
- Strengthening and refinement of internal control environment resulting from independent assurance examinations
- Gaining efficiency in audit and compliance activities by combining assurance and audit suppliers
- Confidence in the market due to transparency of control environment
The most common attestation services include Service Organization Control (SOC) 1 and 2 reports, which are performed under ISAE 3402 and ISAE 3000 standards, respectively. A SOC examination is a widely recognized representation that a service organization has been through an independent and in-depth examination of its internal controls.

**SOC reports**

**Overview**

In 2009, the International Auditing and Assurance Standards Board (IAASB) issued International Standard on Assurance Engagements (ISAE) 3402, which has become an internationally recognized standard for service organization assurance. This report is also known as a SOC1 report and in the United States is performed under the SSAE 18 standard issued by the American Institute of Certified Public Accountants (AICPA).

An ISAE 3402 report is intended to assist service organizations’ customers and their auditors in a financial statement audit and covers services that are likely to be relevant to those user entities’ Internal Controls Over Financial Reporting (ICOFR). Since ISAE 3402 reports are not intended to cover controls unrelated to financial reporting, the ISAE 3000 (or SOC2) reporting option was developed to help service organizations meet a broader set of specific user needs – such as addressing concerns over privacy, confidentiality, and availability.

**ISAE 3402**

The ISAE 3402 report provides guidance to enable an independent auditor (service auditor) to issue an opinion on a service organization’s description of its system and the suitability of the design and operating effectiveness of its controls through a Service Auditor’s Report. Companies are required to define their own control objectives and activities that meet the needs of their customers. The report typically covers general IT controls (e.g., security management, physical and logical security, change control, network and systems monitoring, and systems development) as well as transaction processing, application, and other service-specific controls.

**ISAE 3000**

SOC2 reports issued under the ISAE 3000 standard use the Trust Services Principles and Criteria, a set of specific requirements developed by the AICPA and Canadian Institute of Chartered Accountants (CICA) to provide assurance. Principles and criteria are specifically defined for security, availability, confidentiality, processing integrity, and privacy. This has been done in a modular way so that a SOC2 (hereafter referred to as a ISAE 3000) report can cover one or more of the principles, depending on the needs of the service organization and its users.

By contrast, ISAE 3402 reports require the service organization to define control objectives that are likely to be relevant to their customers’ (user entities’) Internal control over financial reporting (ICOFR).
ISAE 3000 reports typically cover a subject matter that provide more value to customers than just ICOFR. For example, Industry surveys consistently rate security and availability as top concerns when considering cloud adoption. ISAE 3000 provides a strong mechanism for providing third-party assurance in these areas.

**SOC3**
The SOC3 report is used where there is a need to communicate overall results from an ISAE 3000 engagement to a broad base of users without having to disclose detailed controls and test results. A SOC3 report may be publicly shared via the service organization’s website with the SOC3 seal of authenticity.

**ISAE 3402 financial reporting controls**
- Financial services – Custodial services
- Healthcare claims processing
- Payroll processing
- Payment processing

**ISAE 3000 operational controls**
- Cloud ERP service
- Data center colocation
- IT systems management
- Enterprise cloud e-mail
- Cloud collaboration
- Software-as-a-service (SaaS)-based HR services
- SaaS enterprise system housing third-party data
- Any service where topics such as security, availability and privacy are areas of concern
Applicability of SOC Reports

**Applicability to different types of outsourced services**

Using the table on page 6 will help to determine what type of SOC report is most applicable regarding certain controls and services. Starting at the top of the table, there are services that are clearly financial reporting oriented, and where it is likely ISAE 3402 reports will be requested, and provided. These include financial services as well as processing for healthcare claims, payroll, payment and financial transaction processing.

In addition, there may be some cases where users require more detail on security or availability. In these cases, the service provider might provide a ISAE 3402 report for ICOFR purposes, and a ISAE 3000 report to address security/availability assurance needs if the demand for such reports or the burden of accommodating users’ security audits is great enough.

In the middle of the table are services that do not neatly fit into one category or the other. Depending on the specific nature of services provided, and user needs, ISAE 3402, and/or ISAE 3000 may be most applicable. For example:

- For IT systems management, which can include general IT services provided to a portfolio of users as well as customized services provided to specific users, ISAE 3402 or ISAE 3000 reporting could be applicable, depending on whether users’ assurance needs are more focused on ICOFR or security/availability.

- A cloud-based ERP service provides a core financial reporting service to users. It is likely that it would provide an ISAE 3402 report for that same reason.

However, it may also have a need to provide a ISAE 3000 security, and availability report to address user assurance needs specific to cloud services.

- Many data center colocation providers have historically completed ISAE 3402 examinations limited to physical and environmental security controls. However, most data center providers host much more than just customers’ financial systems. As a result, leading providers are moving toward ISAE 3000 security reporting. Some service providers incorporate supporting environmental security controls within their ISAE 3000 security report, whereas others also address the Availability Criteria depending on the nature of their services.

At the other end of the spectrum, there are services that are operational, and technology focused with very little, if any, direct connection to users' ICOFR.

For example, these types of outsourced services are unlikely to be included within a public company’s financial reporting scope. Users of these services are typically most concerned about the security of their data, and availability of these systems. This would typically be addressed by a ISAE 3000 report covering Security, and Availability. Where applicable, ISAE 3000 reports can also cover Confidentiality, Processing Integrity, and/or Privacy. ISAE 3000 is also potentially applicable for any organization that is storing, and processing sensitive third-party data. Where there is a need to demonstrate to third parties that effective Security, and Confidentiality controls are in place to protect information, ISAE 3000 reports provide a mechanism for providing this assurance.
SOC refers to Service Organization Control reports in general, but specific reports include ISAE 3402/SOC1 and ISAE 3000/SOC2. This table compares and contrasts the focus, scope and control domains covered by the two reports.
<table>
<thead>
<tr>
<th>Intended User Base</th>
<th>ISAE 3402/SOC1*</th>
<th>ISAE 3000/SOC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Internal Control Over Financial Reporting (ICOFR)</td>
<td>• Operational controls</td>
<td>• Detailed report for user entities, their auditors**, and specified parties</td>
</tr>
<tr>
<td>• Detailed report for user entities and their auditors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purpose</td>
<td>Focused on financial reporting risks and controls specified by the service provider. Most applicable when the service provider performs financial transaction processing or supports transaction processing systems.</td>
<td>Focused on: • Security • Availability • Confidentiality • Processing Integrity and/or • Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Applicable to a broad variety of systems</td>
</tr>
<tr>
<td>Defined scope of system</td>
<td>• Classes of transactions</td>
<td>• Infrastructure</td>
</tr>
<tr>
<td></td>
<td>• Procedures for processing and reporting transactions</td>
<td>• Software</td>
</tr>
<tr>
<td></td>
<td>• Accounting records of the system</td>
<td>• Procedures</td>
</tr>
<tr>
<td></td>
<td>• Handling of significant events and conditions other than transactions</td>
<td>• People</td>
</tr>
<tr>
<td></td>
<td>• Report preparation for users</td>
<td>• Data</td>
</tr>
<tr>
<td></td>
<td>• Other aspects relevant to processing and reporting user transactions</td>
<td></td>
</tr>
<tr>
<td>Control Domains Covered</td>
<td>• Transaction processing controls***</td>
<td>• Security</td>
</tr>
<tr>
<td></td>
<td>• Supporting IT general controls</td>
<td>• Availability</td>
</tr>
<tr>
<td>Level of Standardization</td>
<td>• Control objectives are defined by the service provider and may vary depending on the type of service provided.</td>
<td>• Confidentiality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Processing Integrity and/or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Privacy</td>
</tr>
<tr>
<td>Applicability****</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Accounting and tax services, custodial services, debt collections, ERP general ledger software provided under hosted/ASP model, health plans, loan processing companies, lock box processing, payroll processors, property and casualty (P&amp;C) insurance claims processing, retirement plans and trust operations.</td>
<td>• Business process outsourcing (BPO), Cloud computing IaaS, credit card data processors, data analytics, data center collocation facilities, disaster recovery services, electronic medical records (EMR) service providers, e-marketing service companies, telephony, managed security service providers, PaaS and SaaS providers without financial reporting impact, records management companies, technology support, telephony, web hosting service providers etc.</td>
</tr>
<tr>
<td>Benefits</td>
<td>• Can address customer’s requirements for testing the operating effectiveness of the service organization’s controls.</td>
<td>• The audit is performed against a standard set of specific controls (the Trust Services Principles and Criteria).</td>
</tr>
<tr>
<td></td>
<td>• Provides details and comfort regarding the effectiveness of the service organization’s controls.</td>
<td>• Useful to service organization’s customers, regulators, business partners, and due diligence by acquirer companies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The report can play an important role in oversight of the third-party service organization, vendor management programs, internal corporate governance, and risk management process.</td>
</tr>
</tbody>
</table>
ISAE 3000/SOC2 Trusted Service Principles

ISAE 3000 reports use the globally recognized Trust Services Principles and Criteria, a set of specific requirements developed by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) to provide assurance beyond internal controls over financial processes. Principles and Criteria are specifically defined for Security, Availability, Confidentiality, Processing Integrity and Privacy. In contrast to ISAE 3000, ISAE 3402 reports require a service organization to describe its system and define its control objectives and controls that are relevant to users’ internal control over financial reporting. An ISAE 3402 report generally should not cover services or control domains that are not relevant to users from a financial audit (ICOFR) perspective and it specifically cannot cover topics such as disaster recovery and privacy.

<table>
<thead>
<tr>
<th>Trust Services Principle</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td>• Most commonly requested area of coverage.</td>
</tr>
<tr>
<td></td>
<td>• Security criteria are also incorporated into the other principles because security controls provide a foundation for the other domains.</td>
</tr>
<tr>
<td></td>
<td>• Applicable to all outsourced environments, particularly where enterprise users require assurance regarding the service provider’s security controls for any system, non-financial or financial.</td>
</tr>
<tr>
<td></td>
<td>• The system is protected against unauthorized access (both physical and logical).</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>• Second most commonly requested area of coverage, particularly where disaster recovery is provided as part of the standard service offering.</td>
</tr>
<tr>
<td></td>
<td>• Most applicable where enterprise users require assurance regarding processes to achieve system availability SLAs as well as disaster recovery which cannot be covered as part of ISAE 3402/SOC1 reports*.</td>
</tr>
<tr>
<td></td>
<td>• The system is available for operation and use as committed or agreed.</td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
<td>• Most applicable where the user requires additional assurance regarding the service providers practices for protecting sensitive business information.</td>
</tr>
<tr>
<td></td>
<td>• Information designated as confidential is protected as committed or agreed.</td>
</tr>
<tr>
<td><strong>Processing Integrity</strong></td>
<td>• Potentially applicable for a wide variety of non-financial and financial scenarios wherever assurance is required as to the completeness, accuracy, timeliness and authorization of system processing.</td>
</tr>
<tr>
<td></td>
<td>• System processing is complete, accurate, timely, and authorized.</td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td>• Most applicable where the service provider interacts directly with end users and gathers their personal information.</td>
</tr>
<tr>
<td></td>
<td>• Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity’s privacy notice and with criteria set forth in globally recognized privacy.</td>
</tr>
</tbody>
</table>

* Depending on national financial audit regulations back up and recovery controls can be in scope of an ISAE 3402/SOC1 report under local regulations.
Assurance through Attestation
**Reporting Types and Structure**

**SOC report types**
SOC reports most commonly cover the design and effectiveness of controls for a 12-month period of activity with continuous coverage from year to year to meet user requirements from a financial reporting or governance perspective. In some cases, a SOC report may cover a shorter period of time, such as 6 months, if the system/service has not been in operation for a full year or if annual reporting is insufficient to meet user needs. A SOC report may also cover only the design of controls at a specified point in time for a new system/service or for the initial examination (audit) of a system/service.

Period of time reports covering design and operating effectiveness are generally referred to as “Type 2” reports whereas point in time reports covering design are generally referred to as “Type 1” reports. For example, if a user organization required a period of time report covering Security and Availability for a particular system, the user organization would request a ISAE 3000 Type 2 Security and Availability report from the service provider. If the user organization required a period of time report covering financial reporting (ICOFIR) related controls for a particular system, the user organization would request an ISAE 3402 Type 2 report of that system from the service provider.
The following table gives an illustration of the output of the report and the entity responsible for preparing it. The report can cover a point in time (design – Type 1) or period of time (design and operating effectiveness – Type 2).

<table>
<thead>
<tr>
<th>ISAE 3402</th>
<th>Responsible Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor’s Opinion</td>
<td>Service Auditor</td>
</tr>
<tr>
<td>Management Assertion</td>
<td>Service Organization</td>
</tr>
<tr>
<td>System Description (including controls)</td>
<td>Service Organization</td>
</tr>
<tr>
<td>Control objectives</td>
<td>Service Auditor &amp; Service Organization</td>
</tr>
<tr>
<td>Control activities</td>
<td>Service Auditor &amp; Service Organization</td>
</tr>
<tr>
<td>Tests of operating effectiveness*</td>
<td>Service Auditor</td>
</tr>
<tr>
<td>Results of tests*</td>
<td>Service Auditor</td>
</tr>
<tr>
<td>Other Information (if applicable) (i.e. Management’s response to identified deficiencies in the testing)</td>
<td>Service Organization</td>
</tr>
</tbody>
</table>

* Applicable for Type 2 reports
Phases for Preparing for and Issuing a SOC Report

For service providers that have not previously completed an attestation engagement, there is typically a two phase process to prepare for and complete the SOC examination.

The following points summarize our phased approach for first time attestations. We start with an Attestation Preparation phase where we collaborate with the service provider and provide guidance to set the stage for a successful engagement. The Execution phase then builds upon the understanding of the service provider’s architecture and controls that was established in the Attestation Preparation phase.

**Attestation Preparation**
- Define audit scope, and overall project time line
- Identify existing or required controls through discussions with management, and review of available documentation
- Perform readiness review to identify gaps requiring management attention
- Communicate prioritized recommendations to address any identified gaps
- Hold working sessions to discuss alternatives, and remediation plans
- Verify that gaps have been closed before beginning the formal execution phase
- Determine the most effective audit, and reporting approach to address the service provider’s external requirements

**Execution**
- Provide overall project plan
- Complete advance data collection before on-site work to accelerate the audit process
- Conduct on-site meetings, and testing
- Complete off-site analysis of collected information
- Conduct weekly reporting of project status, and any identified issues
- Provide a draft report for management review, and electronic, and hard copies of the final report
- Provide an internal report for management containing any overall observations, and recommendations for consideration
There are several key factors in the success of KPMG’s attestation practice:

**A qualified professional in delivering IT attestation services**
KPMG has competent and experienced resources who have a background in providing SOC and other IT attestation services. We establish long-term relationships with clients and strive to develop and maintain those relationships.

**We understand your business**
KPMG’s professionals have extensive knowledge and experience in numerous business processes in a variety of industries, including IT services, banking, energy, healthcare, insurance, logistics and manufacturing.

**A well-established approach**
KPMG has carefully constructed thorough methodologies and approaches in its delivery of attestation services.

**A leading methodology**
We have developed a repository of control objectives and activities to guide you through the process of identifying the control objectives and activities that meet your customers’ and regulators’ expectations.

In addition to reports, KPMG can provide observations recommendations for improving your organization’s environment. Our recommendations are tailored to your business and consider relevant industry and regulator standards and leading practices.

**Our project management tools**
KPMG works closely with you to plan all attestation activities and to help reduce interruptions to your normal business operations. We involve key stakeholders at the beginning of a project to promote a clear understanding of the audit process and its objectives. Project status, issues, and their impact are communicated throughout the engagement.
Contacts

Gunnar Sotnakk  
Partner, Audit  
T: +47 4063 9279  
E: gunnar.sotnakk@kpmg.no

Roland Fredriksen  
Partner, Audit  
T: +47 4063 9317  
E: roland.fredriksen@kpmg.no

Sanna Suvanto  
Director, Information Risk Management  
T: +47 9526 0768  
E: sanna.suvanto@kpmg.no