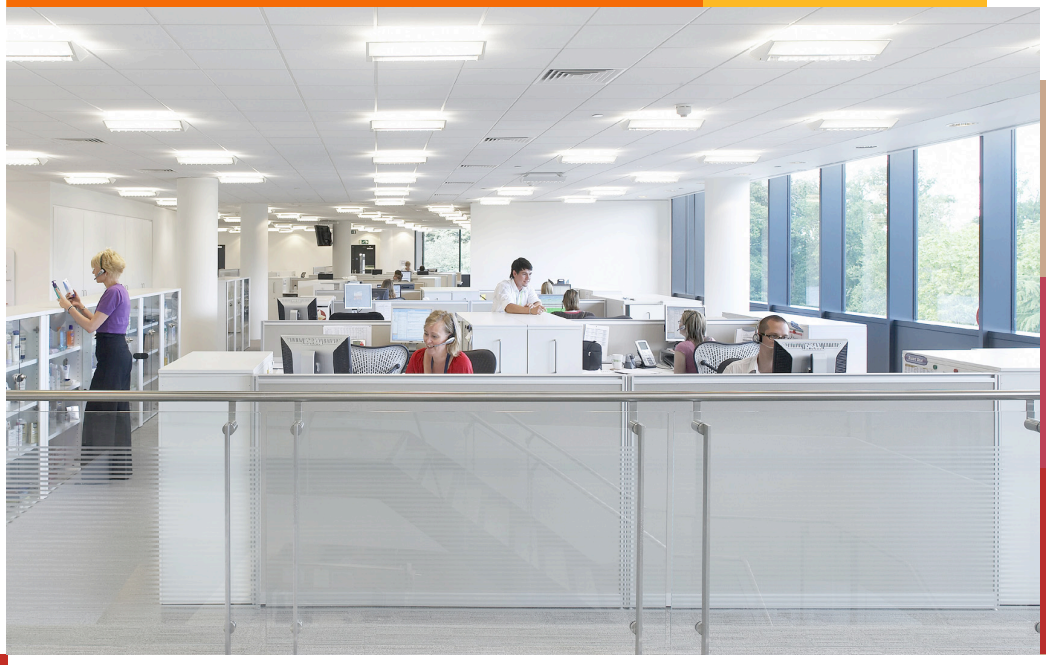
www.pwc.com

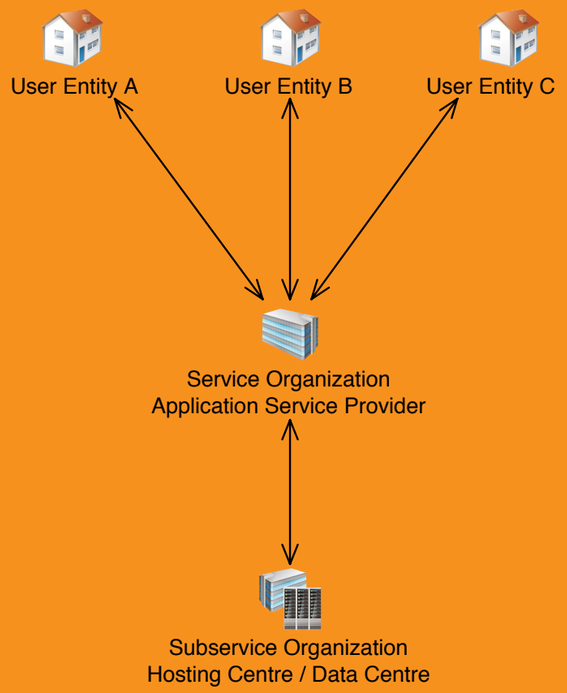
Making trust evident

Reporting on controls at Service Organizations



pwc

Does this picture look familiar to you?



Introduction and background

Many entities outsource aspects of their business activities to organizations that provide services. Outsourcing can range from performing a specific task (e.g. payroll calculations) to replacing entire business units of functions of the entity (e.g. IT/IS function).

Organizations that provide services to their customers are often subject to independent assessments of the services which they execute on behalf of their customers. International Standard on Assurance Engagements ISAE 3402 provides the service organization with a mechanism for sharing comfort (via an independent assurance report).

International Standard on Attest Engagement ISAE 3402 uses the term ***service organization*** to refer to an entity to which services are outsourced.

The entities that use the services of a service organization are termed as ***user entities***. Look at the picture we made for your illustration.

Where is the added value for you?

Independent Assurance Report is focused on reporting for the benefit of external users about internal controls at service organizations. The attestation report ***provides assurance*** that the service organization´s controls are suitably designed and operating effectively.

How many various „audits" is your organization subject to in a year? Are you looking for ***cost-effective solution***?

What is you ***differentiation*** from the competition?

Building of trust, contributed to service organization to get clients.

Read more to found out how you can obtain comfort as to the adequacy of design of controls and operating effectiveness regardless you are user of the services or provider of the services.

Interaction between a user entity and a service organization

Interaction between a service organization and a user entity relates to the extent to which a user entity is able to monitor and control the activities of the service organization. For example, when a user entity initiates transactions and the service organization executes, processes, and records those transactions, a high degree of interaction exists between the activities at a user entity and those at a service organization.

Controls at the Service Organizations

Service organizations can implement controls that can help user entities obtain assurance on service(s) provided and as such minimize the risk of a misstatement. For example, the service organization can implement controls to make sure:

- that errors in transaction processing are identified and resolved on a timely basis;
- that correct inputs are used for data processing, for example foreign exchange rates and tax rates, or
- that data is appropriately backed up and recoverable.

It is important for the user entity to obtain an understanding of the services provided and the service organization's controls over those services such as user manuals, system overviews, the service contract, written process descriptions, and reports by service auditors and/or internal auditors on the service organization's controls.

Reporting on controls at Service Organizations
Get cost efficiencies

There are several ways to obtain an understanding of controls implemented at the service organization(s):

- By visiting the service organization and performing necessary testing of controls at the service organization.
- By asking for a service auditor's report on controls at the service organization
- By using another auditor to perform procedures that will provide the necessary information about the relevant controls at the service organization, for example tests of controls at the service organization or substantive procedures on transactions and balances maintained by a service organization

When does a user entity have to perform a visit of a service organization or ask for a service auditor's report?

When a user entity has no information about the service organization's controls to ensure the reliability of the processing of transactions . A user entity can ask a service auditor to be engaged to perform procedures to supply the information.

According to the ***International Standard of Auditing*** (ISA 402), an auditor of a user entity has an obligation to obtain evidence about the financial statement assertions affected by the service organization. As the result, a user auditor can ask that a service auditor be engaged to perform procedures to supply the information.

Generally, a service organization will want to minimize the number of user auditors or other auditors performing their tests of controls. Therefore, the service auditor's report is an efficient option for a service organization to assess and report on their control environment.

What information would the user entities and their auditors be looking for?

- How the entity uses service organizations and/or subservice organizations in the entity's operations.
- The nature of the services provided by the service organization and the significance of those services to the entity.
- The nature and materiality of the transactions, accounts and / or financial reporting processes.
- What are the complementary user controls that users entities are expected to perform? For example, the controls for completeness and accuracy of input submitted to/ received from the service organization.

When the service organization decides to deliver a service auditor report what is the service organization responsible for?

Management of the service organization is responsible for preparing its description of service organization's systems ("the system") that includes:

- Services covered
- Description of classes of transactions processed;
- Control objectives, related controls and consideration of risks to achieve control objectives (even if management does not have a formal Risk Management Process);
- Period covered by the report;
- Type of the Report (type 1 or type 2);
- Complementary user entity controls;
- Controls performed by sub-service organization(s);
- The process used to prepare reports provided to customers;
- Preparing management's written assertion (a letter).

Scope is important Define just the controls that may be key to your customers

This is the ***key*** to success of any third-party assessment. It involves working with the key stakeholders' management to plan the details of the engagement including the establishment and agreement of report and engagement scope as well as the establishment of an engagement timeline that depicts each stage by date.

The service organization and/or its customers must formally define the scope that will be covered in the report: business units, business processes, classes of transactions performed, or applications to be covered. The scope will be focused on controls likely to be ***relevant*** to user entities' internal control over financial reporting.

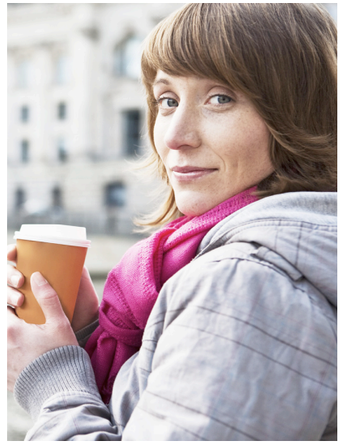
The service auditor should also obtain an understanding of the components of the financial statements of user entities. For example, review a set of financial statements and the contract between a user entity and a service organization.

Description of the service organization's system

There is no particular requirement on how the description should be documented. It can vary depending on size and complexity of the service organization and it's monitoring activities. What the description should provide is ***sufficient information*** for user auditors to understand how the service organization's processing affects user entities financial statements and ***enable user auditors to assess the risks*** of material misstatements in the user entities' financial statements.

Management is responsible for the accuracy and completeness of the description which may not include all aspects of the service organization's system, such as services or certain aspects of the processing not ***relevant*** to user entities internal controls or ***beyond*** the scope of the engagement. As a requirement, the description of the service organization system should include the following:

- Specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls. The service auditor is required to determine whether the control objectives are reasonable under the circumstances. In other words, the controls that are likely to be relevant to user entities internal controls over financial reporting.
- How the system captures and addresses significant events and conditions other than transactions (such as changes to standing data, program calculations or other program procedures).
- The related accounting records, whether electronic or manual, and supporting information involved in initiating, authorising, recording, processing, and reporting transactions, including the correction of incorrect information and how information is transferred to the reports and other information prepared by user entities.
- The process used to prepare reports and other information for user entities.



Control objectives and controls
What should be included?

When we talk about the scope of the service auditor report, it is important to focus on ***controls likely to be relevant*** to user entities' internal control over financial reporting. The same focus should apply to the control objectives. The management of the service organization should think of the controls that relate to the assertions embodied in their user entities' financial statements.

For example, financial statement assertions about existence and accuracy are affected by controls that prevent, or detect and correct, unauthorized access to the system. Below is the sample of an ***illustrative control objectives*** for the Information Security.

> " controls provide reasonable assurance that logical access to programs, data and computer resources is restricted to authorized and appropriate users"
>
> "physical access to computer is restricted to authorized and appropriate personnel"

General Computer Controls can be used alone or in combination with the business process controls depending on the nature of the outsourced service.

Control objectives have to also be stated ***objectively*** so that individuals having competence in and using the same or similar measurement criteria arrive at similar conclusions.

The role of the service auditor is to determine if the control objectives are reasonable, including whether the control objectives relate to the user entities financial statements. On the other hand, the user auditor and user entity are responsible for determining whether the control objective are complete.

Type of the work
Difference between type 1 and type 2 report

There are two types of the Service Auditor Report

A ***Type 1*** report covers the period ***"as of"*** the date of the report. Type 1 does not provide assurance that the controls have been operating throughout the entire period (for example a year). A Type 1 Report ensures that the controls are designed effectively to make sure the control objectives are achieved "as of" the issue report date. To issue only a Type 1 Report is useful when a service organization engages a service auditor for the first time. It helps a user auditor to plan an audit of a user entity.

A ***Type 2*** report provides evidence that the described system and determined control objectives operate ***throughout the period*** of time (e.g. a year). A Type 2 report has more practical use.
The aim of the service auditor should be to provide a report that is useful to user entities and their auditors. Type 2 reports are predominant in practice.

The time period covered by the Report

Any report that covers less than 6 months is unlikely to be useful to user entities and their auditors. As a service organization, you can decide on the period covered. In some circumstances you can issue the report for the shorter period:

- When the report is issued for the first time, or
- The service auditor is engaged close to the date by which the report is needed as the evidence on the controls cannot be obtained retrospectively.

Does the service organization use another organization to provide services?

If the answer is yes, what are the services this organization provides and may such services affect the user entities internal control over financial reporting? The following is a description of such a service:

- Application service provider hosts its System at Computer Outsourcing Organization, which provides the computer processing infrastructure. This organization maintains responsibility for computer processing infustructure, backup and recovery procedures. The service organization maintains responsibility for user management and changes. This organization is called ***sub-service organization***.

A service organization that uses a sub-service organization has two options to present information about the services provided by the sub-service organization in its description of the system:

- Include the sub-service organization description of controls (inclusive method).
- Exclude the sub-service organization description of controls (carve-out method).

The inclusive method provides more information for user auditors. If the carve-out method is used, the description of the system should include the nature of the services provided by the sub-service organization, but not describe the detailed processing or controls at the sub-service organization. Certain control objectives of the service organization (for example physical security of the applications) may only be achieved if controls are implemented and operating effectively at the sub-service organization.

To decide which approach to use depends on the nature and extent of the information about the subservice organization that user auditors may need and on the challenges in implementing the inclusive method. Service auditor, service organization and sub-service organizations have to carefully plan, communicate and agree on the inclusive approach ***before it is adopted***.

Complementary user entity controls

The service organization may design its services with the assumptions that certain controls will be implemented by the user entities, complementary user entity controls. If such controls are necessary to achieve certain control objectives, the Standard requires a service auditor to evaluate whether the service organization's description of its system adequately describes complementary user entity controls.

Some examples of typical complementary user entity controls are:

- User entities have controls in place to provide reasonable assurance that:
  - Access to system resources and applications are restricted to appropriate user entity personnel.
  - Input submitted to the service organization is complete and accurate.
  - Output received by the user entity is complete, accurate, and authorised (for example, reconciling input reports to output reports).

In order to evaluate that complementary user entity controls included in the description are adequate, the service auditor reads contracts with user entities to gain an understanding of the user entities responsibilities and whether those responsibilities are appropriately described in management's description of the service organization's system.

What is management written assertion?

Management is required to provide a written assertion (a letter) with respect to the service organisations responsibilities for systems and controls. In the letter the service organization has to acknowledge its responsibilities through a written assertion, which will state that the controls are fairly presented, suitably designed and operating effectively to achieve the specified control objectives.
Managements assertions would be expected to address:

- ***Fairness*** of presentation of the service organization's system,
- ***Suitability*** of the design of controls to achieve control objectives, and
- ***Operating effectiveness*** of controls throughout the specified period.

Management uses certain ***criteria, reasonable basis*** (standards or benchmarks) in preparing the description of the service organization's system. The service auditor is required to assess the suitability of the criteria and the Standard determines the minimal requirements on what the criteria should include.
An example of criteria used is that the description does not omit or distort information relevant to the service organization's system.

The written assertion must be included in, or attached to, management's description of the service organization's system. It is a responsibility of a service auditor to determine if the management assertions are appropriate. A service auditor is precluded from issuing a report if management does not provide a written assertion.

"Increased readiness for Third Party Assurance reporting via the identification of control design gaps and operating effectiveness issues".

For the first time
From Readiness to Engagement

Phase 1

Development of the report structure

The service organization and/or its customers must formally ***define the scope*** that will be covered in the report. Our extensive experience with third party assurance reports allows us to help you and your customers develop control objectives and procedures to finalize the scope of the report.

Phase 2

Assessment of the business environment

The second phase is the most critical portion of the assignment. As part of this service, we identify ***areas that must be improved*** before your organization's processes are subjected to a formal audit. Similarly, we will also identify existing procedures that are currently adequate but nonetheless could be improved for the benefit of your organization.

Phase 3

Correction of identified deficiencies

In this phase, the organization will determine its action plan to ***address weaknesses*** identified in the first and second phases of this assignment. Our professionals can provide guidance on the fixes being implemented to ensure they meet audit readiness requirements.

Phase 4

Attestation

The fourth phase is the ***attestation and reporting of results*** and findings. Although we can test at a point-in-time or for a period of time, first-time attestations are most commonly completed at a point-in-time (type 1 report) to assess the adequacy of design prior to testing the operating effectiveness of the selected processes.

About us

Our Systems & Process Assurance (SPA) practice provides services to you that relates to controls around the financial reporting process, including financial business process and IT management controls.

How we can help you?

- Financial and operation applications/business process controls reviews and design
- Database security controls reviews
- IT general controls reviews
- Third party assurance and opinion services
- Compliance with other regulatory standards
- Due diligence on systems and controls
- Pre- and post-implementation systems reviews
- Data services (e.g., data analysis, data quality reviews)
- Computer security reviews

Just a little can make a difference. Let´s start today.

Jón Sigurðsson
Partner, Löggiltur endurskoðandi
sími: +354 550 5387
gsm: +354 840 5387
jon.sigurdsson@is.pwc.com

Jana Flieglová, *CISA, ACCA*
Manager
sími: +354 550 5364
gsm: +354 840 5364
jana.flieglova@is.pwc.com

www.pwc.com