EuroCloud
TRUSTED DIGITAL COMPETENCE PLATFORM

pwc



CLOUD AND ANNUAL ACCOUNTS

Guideline for Accountants, Auditors, and Staff in Finance, IT and Revision of Companies Subject to Statutory Audit

PROVIDED BY EUROCLOUD
CLOUD KNOW HOW
knowhow.eurocloud.org
TRUSTED DIGITAL COMPETENCE PLATFORM

14

PRINTING SPONSORED BY

SOURCING INTERNATIONAL
Digital Transformation Advisors

IMPRINT
EuroCloud.Austria
Verein zur Förderung von Cloud Computing
Museumstraße 5/14
1070 Vienna, Austria

E-Mail: info@eurocloud.at
Web: http://www.eurocloud.at
Seat of the Association: Vienna
Copyright: EuroCloud.Austria 2017



TABLE OF CONTENTS

1 PREFACE 5

2 CLOUD COMPUTING 6
- 2.1 WHAT IS CLOUD COMPUTING? 6
- 2.2 CLOUD COMPUTING SERVICE MODELS 7
- 2.3 CLOUD COMPUTING REQUIREMENTS RELEVANT TO ANNUAL ACCOUNTS 8

3 THE ANNUAL ACCOUNT AUDIT 10
- 3.1 GOALS OF THE ANNUAL ACCOUNT AUDIT 10
- 3.2 PRINCIPLES OF ANNUAL ACCOUNT AUDITING 12
  - 3.2.1 EFFICIENCY AND MATERIALITY 12
  - 3.2.2 PROCEDURE OF THE RISK-ORIENTED AUDIT APPROACH 12
  - 3.2.3 CONCLUSION 16
- 3.3 FUNCTION TEST OF THE ICS IN THE AREA OF IT 17
  - 3.3.1 IT SYSTEM TEST 18
  - 3.3.2 COMPONENT “IT CONTROL ENVIRONMENT” 19
  - 3.3.3 COMPONENT “GENERAL IT CONTROLS” 20
  - 3.3.4 COMPONENT “APPLICATION CONTROLS” 22

4 CHALLENGES AND RECOMMENDATIONS 24
- 4.1 RELEVANCE FOR THE ANNUAL ACCOUNT AUDIT (CLOUD SERVICE) 24
- 4.2 ERROR AND CONTROL RISK (CLOUD CUSTOMER) 28
- 4.3 ERROR AND CONTROL RISK (CLOUD PROVIDER) 30
- 4.4 EFFECTIVENESS OF THE ICS (CLOUD PROVIDER) 36

5 SUMMARY 38

6 APPENDIX 39
- 6.1 LEGAL INFORMATION 39
- 6.2 AUTHORS 42



1 PREFACE



This guideline is intended for accountants and auditors as well for staff in the Accounting/Finance, IT and Internal Revision departments (CFOs, CIOs, IT Managers, Heads of Internal Revision) of companies subject to statutory audit.

The point of departure for this guideline is the irrefutable fact that companies are increasingly using cloud services. As soon as such services have a certain influence on the accounting processes and numbers, and can therefore affect annual accounts, they also need to be taken into consideration during auditing of the annual accounts by an auditor.

This represents a significant challenge for all involved persons — for the cloud customer, i.e. the company whose annual accounts the auditor is reviewing, as well as for the auditor.

The aim of this document is to describe the framework conditions for the use of cloud services in regard to annual accounts and the resulting requirements, and present possible solution approaches.

This guideline was created over the course of more than one year in a cooperative process between EuroCloud and the authors Markus Ramoser, Jörg Asma and Manfred Scholz, whom I wish to thank for their efforts. Special thanks go out to Markus Ramoser of PwC Austria, who assumed the leading role in terms of content and elaborated every detail in many sessions with me and with great personal commitment.

I hope that you enjoy reading this guideline and can benefit from it in your day-to-day work.

Vienna, June 2017



Dr. Tobias Höllwarth

2 CLOUD COMPUTING

2.1 WHAT IS CLOUD COMPUTING?

Cloud computing is frequently described as a special form of IT outsourcing[1] with the following fundamental characteristics[2]:

- On-demand self-service: The service is provided in a demand-oriented fashion without the need for human interaction.
- Broad network access: The service is not location-based and is provided via standard web technologies.
- Resource pooling: Required IT resources are provided from a pool of available IT resources. These resources can be distributed across several users/customers as needed.
- Rapid elasticity: The provided service capacity is automatically adjusted upwards as well as downwards.
- Measured service: The provided resources are charged according to their usage.

Significant differences between traditional IT outsourcing and cloud computing become apparent as early as during the phase of demand determination by the outsourcing company. While classic outsourcing is often characterised by a call for tenders and contract negotiations featuring a definition of the required services, employed technologies, data centre standards, personnel and geographical attributes, cloud computing makes use of vastly more "industrialised" IT services where the performance specifications to be delivered are communicated, but there is generally much less information about how the services are rendered.

While classic outsourcing often still features a call for tenders and contract negotiations, cloud computing offers vastly more "industrialised" IT services with much less information about how the services are rendered.

1 - Cf. IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud Computing (IDW RS FAIT 5)
2 - Cf. National Institute of Standards and Technology: The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology, Version 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, last accessed on 20/02/2016.



Many businesses have begun to realise that cloud services are very attractive in terms of their commercial framework conditions and their scope of services. They are also coming to recognise, however, that the evaluation of the scope of services and the quality of cloud services, as well as their integration into the existing IT environment and legally compliant operation (especially concerning compliance with data privacy regulations) represent a significant challenge.

2.2 CLOUD COMPUTING SERVICE MODELS

The following service models[3] can be distinguished:

- Infrastructure as a Service (IaaS): Exclusive provision of IT resources like data centre(s), network or storage.
- Platform as a Service (PaaS): Provision of development and runtime environments. This includes databases as well as operating systems.
- Software as a Service (SaaS): Provision of services directly at the user. A heavily standardised service model offers benefits in terms of cost, but disadvantages in terms of flexibility. The user generally only requires network access and a device.

This simplified classification of cloud services is slowly becoming obsolete, since many services increasingly consist of mixtures or compounds of these service models. It is noticeable, however, that pure infrastructure services, i.e. the provision of hardware for operation of proprietary servers by the customer, have by now developed into commodity services that are becoming ever more affordable on the market due to heavy price competition.

The primary development focus for cloud services lies on the area of Software as a Service, where ever more comprehensive applications for companies' core service areas (purchasing, sales, personnel, production, ERP) are increasingly being offered as services.

These types of services necessarily need to integrate with existing applications so as to exchange data with on-premise software. This means that the availability and quality of purchased cloud applications are highly relevant to the performance capability of the purchasing company.

3 - Cf. National Institute of Standards and Technology: The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology, Version 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, last accessed on 20/02/2016.

The primary development focus for cloud services lies on the area of Software as a Service, where ever more comprehensive applications for companies' core service areas (purchasing, sales, personnel, production, ERP) are increasingly being offered as services.

2.3 CLOUD COMPUTING REQUIREMENTS RELEVANT TO ANNUAL ACCOUNTS

If accounting-relevant services and data are outsourced using cloud services, the responsibility for compliance with legal and regulatory requirements that the outsourcing company is subject to remains with that company's legal representatives. This applies in particular to the observance of security and compliance requirements. Among other things, the representatives are obligated to consider the risks and possible consequences for the outsourcing company's internal control system (ICS) resulting from the use of cloud services.[4]

If accounting-relevant services and data are outsourced using cloud services, the responsibility for compliance with legal and regulatory requirements remains with the outsourcing company's legal representatives.

Determining what constitutes accounting-relevant data or services is not always easy in practice, as this category may include services that do not directly process accounting-relevant data but have significant influence on accounting processes as upstream systems, and must therefore likewise be taken into consideration (e.g. web shops). For Germany, the Institut der Wirtschaftsprüfer (Institute of Auditors) has established the following definition: Outsourced services are relevant for accounting if they serve to store or process data on business transactions, events or business activities that are either entered directly into accounts (e.g. other expenses in accounting) or are made available to the accounting system as the basis for accounting transactions.[5]

4 - Vgl IDW RS FAIT 5 Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Prozessen und Funktionen einschließlich Cloud Computing (Institut der Wirtschaftsprüfer, 2015), TZ 7
5 - Vgl IDW RS FAIT 5 Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Prozessen und Funktionen einschließlich Cloud Computing (Institut der Wirtschaftsprüfer, 2015), TZ 5



Outsourced services are relevant for accounting if they serve to store or process data on business transactions, events or business activities that are either entered directly into accounts (e.g. other expenses in accounting) or are made available to the accounting system as the basis for accounting transactions.

For Austria, the Chamber of Commercial Fiduciaries has published an expert opinion on annual accounts including the use of IT (KFS/DV2[6]). This document also deals with the topic of "Outsourcing" and defines the following requirements for the annual account auditor:

"If a company outsources significant systems of information technology and information-technology-supported business functions to another company (an independent service provider or an incorporated company), then the annual account auditor of the outsourcing company is obliged to evaluate how this process affects the effectiveness of the internal control system of the outsourcing company."

It should also be noted that all applicable legal and regulatory requirements in the areas of accounting and finance must be observed during the use of cloud services. In certain limited cases, outsourcing to other countries may be forbidden, or allowed only with the approval of the competent financial authority.

This means that if a cloud service is employed that provides essential business functions, the auditor is required to evaluate what effects the use of the cloud service has on the ICS of the outsourcing company, and in many cases will have to assess whether the ICS at the outsourcing company as well as that of the cloud service provider are effective.

6 - Vgl. KFS/DV2 Fachgutachten über Abschlussprüfung bei Einsatz von Informationstechnik (Kammer der Wirtschaftstreuhänder, 2004)

3 THE ANNUAL ACCOUNT AUDIT

To help to determine whether and how the use of cloud services affects the annual account audit, the following section explains what an annual account audit is and which important criteria apply to it.

3.1 GOALS OF THE ANNUAL ACCOUNT AUDIT

The goal of an annual account audit is to confirm with reasonable certainty that the audited annual accounts conform to the applicable accounting laws and regulations under consideration of the generally accepted accounting principles (GAAP) and are free of material errors, thus providing a faithful portrayal of the assets, finances and profitability of the company.[7]

It should be noted that, in simplified terms, it is not the auditor's task to pass judgment on the audited company's business decisions, nor is the auditor obliged to make an explicit statement on GAAP compliance at the audited company.

As a further aside, the generally accepted accounting principles (GAAP) themselves should also be mentioned here:

The accounting of a company must be proper.[8] This means that business transactions are recorded comprehensibly, unmodifiably, completely, correctly, and in a timely and orderly fashion in the company's accounting. Furthermore, the principles also include clarity, circumspection and individual assessment. Some of these principles are required by law, while some are simply considered mandatory standards to be upheld. These generally accepted accounting principles are very similar in Austria, Germany and Switzerland, i.e. they are roughly the same. They are defined in more detail in corresponding expert opinions and standard documents by auditor associations:

Comprehensibility: All business transactions must be recorded in such a way that a competent third party can understand them in a reasonable amount of time. This means

The generally accepted accounting principles are comprehensibility, unmodifiability, completeness, correctness, timeliness and orderliness.

7 - Vgl. KFS/PG3 Fachgutachten über die Erteilung von Bestätigungsvermerken nach den Vorschriften des UGB bei Abschlussprüfungen von Jahres- und Konzernabschlüssen (Kammer der Wirtschaftstreuhänder 2008, überarbeitet 2015)
8 - Vgl § 190 (1) UGB



that there must also be a suitable means of documentation describing the IT accounting system's application, operation and technology.

Unmodifiability: The original content of every accounting transaction must remain determinable. After it has been entered, an accounting transaction may never be erased, only cancelled.

Completeness: All accounting-relevant business transactions must be recorded once and only once.

Correctness: All business transactions must be recorded with their actual values, with the correct time and in the correct accounts.

Timeliness: Entry into the accounts must occur promptly after recording of the respective business transaction.

Orderliness: All entries must be made in chronological order and with certain specifications that describe the business transaction (e.g. amount, date, posting text). It must be ensured that all business transactions can be reproduced unmodified, completely and in an orderly fashion until the end of the legally required retention period.

The GAAP must also be observed without restrictions in the context of the use of accounting-relevant cloud services. However, the use of accounting-relevant cloud services entails additional risks in regard to compliance with the GAAP as well as in terms of errors in the annual accounts when compared to the use of traditional IT outsourcing services. These additional risks must be taken into account in the evaluation of the ICS by the auditor. More on this topic in a later section.

Last but not least, the above explanations illustrate not only the goals of the annual account audit, but also its limited focus: Besides many other areas of activity within a company, the annual account audit serves to assess the correctness and completeness of the annual accounts, i.e. the data from which the numbers in the financial statements and income statements are calculated. Any areas and activities that have no influence on these data are not relevant.

The goal of an annual account audit is to confirm with reasonable certainty that the audited annual accounts conform to the applicable accounting laws and regulations under consideration of the generally accepted accounting principles (GAAP) and are free of material errors.

3.2 PRINCIPLES OF ANNUAL ACCOUNT AUDITING

3.2.1 EFFICIENCY AND MATERIALITY

Two important principles of annual account auditing are efficiency and materiality.

Any audit of annual accounts should be performed with consideration for efficiency, as an audit of all (100 %) relevant areas of a company would entail unjustifiably high costs.

Principle of efficiency: A complete audit of all areas of a company is uneconomical.

The purpose of an annual account audit is to identify material errors in the annual accounts. A piece of information is considered material if an error within that information or its absence would have led to a different (entrepreneurial) decision by the reader of the annual accounts.

For example, imagine that an investor, having read the revenue numbers in the audited annual accounts of a company, has decided to purchase that company. It later turns out, however, that the actual revenue was much lower than stated in the annual accounts. Had the investor known this beforehand, he would not have purchased the company; the error must therefore be regarded as material.

Principle of materiality: Focus on errors which, if known, would have caused the reader of the annual accounts to make different entrepreneurial decisions.

3.2.2 PROCEDURE OF THE RISK-ORIENTED AUDIT APPROACH

The two principles of annual account auditing (efficiency and materiality) have led to the development of the "risk-oriented audit approach". Today, this approach is used worldwide for audits of annual accounts and has been specified in international[9] and national standards.

The risk-oriented audit approach is based on the auditor defining a materiality threshold that identifies relevant items, then taking random samples from the group of relevant

9 - International Standard on Auditing 200 – Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing



items and auditing them. This procedure allows the audit risk to be lowered to a level where the auditor can confirm with adequate certainty that the annual accounts are error-free. It also means, however, that the final verdict by the auditor (auditor's opinion) does not represent a guarantee or 100 % certainty of the audited annual accounts being correct, only that they are devoid of material errors.

Risk-oriented audit approach: Take random samples above the materiality threshold with the goal of identifying all material errors.

A cloud service must therefore be taken into consideration during the annual account audit if that cloud service produces data that are relevant to accounting and influence a material item in the annual accounts.

The audit risk (AR) in regard to the annual account audit is made up of the inherent risk (IR), the control risk (CR), and the detection risk (DR) according to the following formula:

PR = IR x CR x DR

Inherent Risk (IR)

In a first step, the auditor examines the company in terms of the industry segment and markets it operates in, as well as in terms of its business activity. Corresponding analyses are conducted and the company's management is interviewed. Together with the auditor's own experience, this serves to estimate the inherent risk, which is a measure for the error-proneness of the annual accounts and therefore relevant to the auditor. The existence of outsourced (IT) services should already be discussed in this step.

The inherent risk is referred to as the first component of the overall error risk of the annual account audit. It cannot be influenced by the auditor.

First step: Estimation of the inherent risk.

Materiality Threshold

Relevant items in the annual accounts and the areas for specific audit are defined on the basis of the materiality threshold determined by the auditor.

Second step: Determination of the materiality threshold.

Survey of Business Processes and IT Systems

The next step is the survey of the company's business processes and associated IT systems through which the business transactions and data for the selected items and areas for audit are processed and displayed. This includes determining whether any business functions (e.g. IT processes) are outsourced, and if so, which ones.

Third step: Survey of business processes and IT systems and their outsourcing, if applicable.

Control Risk (CR)

Over the course of the abovementioned steps, the auditor gains an understanding of the ICS for accounting at the audited company. This ICS must be planned and implemented by the company in a manner appropriate for the inherent risk. Should the company's ICS not sufficiently address the inherent risk or be otherwise faulty in its planning or implementation, the company would be at risk of not being able to recognise or prevent material errors in time.

The control risk is therefore defined as the risk that although an ICS has been planned and implemented at the company, that ICS is not sufficiently effective. The estimation of this control risk serves to evaluate to what degree audit certainty can be achieved on the basis of the ICS itself.

The control risk is referred to as the second component of the overall error risk of the annual account audit. Like the inherent risk, it cannot be influenced by the auditor.

Based on the estimation of the control risk, the auditor decides in which areas of the audit to rely on the ICS (areas with low control risk) and in which areas not to do so.



Fourth step: Estimation of control risk and determination of type and scope of ICS audit.

Function Test

The assessment of the ICS is described as the function audit or function test. Such a test is conducted by the auditor only if he can assume sufficient effectiveness of the ICS in his risk estimation. If the auditor considers the ICS to be ineffective (= high control risk), there is no need for further testing of the ICS, since flawed results are to be expected. Any additional testing effort would therefore be uneconomical.

The function test of the ICS is performed in two steps. In the first step, the ICS is assessed within the IT processes. These IT processes support the effectiveness of automatic and IT-dependent controls in the business processes and the reliability of data in system-generated reports (e.g. the list of open accounting items).

Depending on the result of the first step, the type and scope of the audit of the ICS in the business processes are determined for the second step.

Fifth step: Function test of the ICS.

Detection Risk (DR) and Substantive Testing

Based on the estimation of risks (inherent risk and control risk) and the results of the ICS test (IT and business processes), the auditor must now perform so-called substantive tests.

These substantive tests (analytical procedures and tests of details of balances, e.g. the checking of individual receipts) are very time- and cost-intensive.

With a view to efficiency, the audited company as well as the auditor therefore have an interest in keeping the extent of this substantive testing as small as possible. This is only possible, however, if the ICS is effective.

The risk of the auditor overlooking a material error during substantive testing is called the detection risk. This risk can and will be influenced by the auditor.

Sixth step: Determination of type and extent of substantive tests.

Returning to the original risk "formula" AR = IR x CR x DR, and assuming the inherent risk as given, it is clear that in the case of a high control risk, the auditor will need to increase the number of substantive tests to reduce the detection risk. For economic reasons, there is thus a significant benefit in finding a low control risk, as this allows cost-intensive substantive tests to be reduced to a minimum while still maintaining a sufficiently low overall audit risk, thereby allowing an acceptably certain verdict on the annual accounts.

3.2.3 CONCLUSION

In summary, only accounting-relevant and material cloud services need to be taken into consideration during annual account auditing. The inherent risk is primarily influenced by the markets and industry segments that a company is active in, as well as by the overall situation of the company. The use of cloud services nevertheless affects the inherent risk as well. In particular, the auditor must obtain a general understanding of what forms of cloud services are in use (e.g. from which cloud providers, at which locations, with what functionality, and affecting which processes).

The annual account auditor must take into consideration the effect of the use of cloud services on the control risk.

Cloud-specific audits that provide clear information on the type of cloud services employed and their implementation, as well as on the cloud service provider and its subcontractors, are therefore of great benefit to the auditor (see Section 3.1)

Cloud services support and change business processes, including IT processes, in companies. This means that the auditor primarily needs to examine the effects of the use of (accounting-relevant) cloud services on the control risk (ICS in business and IT processes).

Cloud service providers that are able to produce detailed audit reports containing sufficient



information about contractual, security-relevant and process-relevant circumstances of their accounting-relevant cloud services thus offer a significant advantage to auditors.

Cloud-specific audit reports are beneficial to the auditor.

3.3 FUNCTION TEST OF THE ICS IN THE AREA OF IT

It has been mentioned that the annual account audit has a limited focus, namely bookkeeping and accounting as well as the financial statements derived therefrom (annual accounts and consolidated accounts).

Furthermore, Section 3.1 stated that one goal of the annual account audit is to confirm with sufficient certainty that the audited annual accounts conform to the applicable accounting laws and regulations under consideration of the generally accepted accounting principles (GAAP) and are free of material errors.

Section 2.3 explained that the principles applied to the annual account audit, and the approach taken by the auditor based on those principles, may require evaluation of the ICS of the audited company as well as that of the cloud service provider, as these ICSs support conformity with the GAAP.

The following section describes all the relevant steps to be taken by the auditor in the event that the audited company uses IT services (i.e. also cloud services) and the auditor has to perform a function test of an existing ICS that has been determined to be effective as per Section 3.2.2.

Not described are all steps taken by the auditor in any case during the annual account audit regardless of the possible function test of the ICS. These steps are known as substantive tests and consist of analytical procedures and tests of details of balances (e.g. checking of individual receipts).

The beginning of this section will once more emphasise why the IT environment and the ICS of the audited company as well as the cloud service provider are relevant for the annual account audit. Thereafter, the three fundamental components of an ICS in the area of IT will be described: the IT control environment, general IT controls and application controls.

For reasons of completeness, it should also be mentioned that not only should an IT-based ICS be in place, but every company should have a second ICS as well. This second ICS should include e.g. manual checking of incoming invoices against the corresponding orders, as well as the checking of contracts and accounting records, by the staff. As this guideline is focussed on the challenges posed for the annual account audit by the use of cloud services, however, non-IT-based ICSs and their components will not be discussed in detail.

Not only should an IT-based ICS be in place; every company should have a second ICS as well.

3.3.1 IT SYSTEM TEST

It is a fact that IT-based accounting systems are used almost exclusively today. As explained in Section 3.2.2, a test of the ICS in the IT processes is conducted before the test of the ICS in the business processes.

This is because in IT-based accounting systems, the security of the employed IT systems reduces the risk of a material error in the annual accounts and is also a prerequisite for compliance with the accounting principle of orderliness, which in turn also positively affects the overall risk situation. An effective ICS that supports compliance with the GAAP and thereby reduces the risk of material errors thus requires an effective ICS in the area of IT as a component of the overall ICS.

What does security mean in this context? Data security in IT focuses on three primary goals: confidentiality, integrity and availability. Authenticity is sometimes mentioned as a fourth goal.[10]

From the perspective of the annual account audit, this means that evaluation of the error risk under consideration of the orderliness of the accounting processes is only possible via assessment of the employed IT systems in regard to the abovementioned data security goals. This assessment is referred to as an IT system test, and naturally also applies to any accounting-relevant cloud services that are in use.

10 - Vgl. https://de.wikipedia.org/wiki/Informationssicherheit



The goal of an IT system test is to determine the risk of material errors caused by the use of accounting-relevant IT systems.

What constitutes an IT system in the given context?

The goal of an IT system test is to determine the risk of material errors caused by the use of accounting-relevant IT systems.

An IT system consists of an IT infrastructure, IT applications and IT-based business processes.[11] Each of these aspects brings about corresponding risks that need to be addressed within a suitable ICS.

The task of the annual accounts auditor and his team is to assess the risk of IT errors (cf. Section 3.2.2) and test the ICS — if its basic effectiveness can be assumed.

Which components of the ICS in the area of IT must the audit team therefore evaluate?

An ICS in the area of IT consists of three components:

- Component "IT control environment"
- Component "general IT controls"
- Component "application controls"

3.3.2 COMPONENT "IT CONTROL ENVIRONMENT"

Measures within the component "IT control environment"[12] serve to establish the prerequisites for proper use of IT.

Examples of this are:

- An appropriate and current IT staff organisation taking into account the principle of function separation (organisation charts, task and job descriptions),
- An appropriate IT strategy and IT risk analysis,
- A current and complete documentation of the essential IT processes (information security, development, introduction of and changes to IT applications, IT operation),

12 - Vgl. IDW PS 330 Abschlussprüfung bei Einsatz von Informationstechnologie (Institut der Wirtschaftsprüfer, 2002), TZ 50f sowie KFS/DV1 Ordnungsmäßigkeit von IT Buchführungen (Kammer der Wirtschaftstreuhänder, 2011), TZ 59f

- Corresponding current guidelines and specifications,
- Suitable monitoring of the ICS in the area of IT, and
- Appropriate reporting to management.

Measures within the component "IT control environment" serve to establish the prerequisites for proper use of IT.

If parts of the IT are outsourced, e.g. in the form of cloud services, then this fact must be taken into consideration within the "IT control environment" component, in particular in terms of information on the type and scope of the usage of the respective cloud services.

This is because the use of cloud services has consequences for the ICS, i.e. for each of the components "IT control environment", "general IT controls" and "applications controls". This must be taken into consideration during evaluation of the ICS.

3.3.3 COMPONENT "GENERAL IT CONTROLS"

General IT controls are controls integrated into the IT processes, not into the business processes. They apply to the IT infrastructure and IT applications, and thus to all applications that are developed, changed, operated and controlled using these IT processes. That is why they are referred to as "general" or "application-independent".

General IT controls are controls integrated into the IT processes, not into the business processes. They need to be sufficiently implemented in the application layer, the operating system layer, the database layer and the network layer.

The expert opinion of the Austrian Chamber of Commercial Fiduciaries states the following: "General IT controls must be sufficiently implemented in the application layer, the operating system layer, the database layer and the network layer."[13] General IT controls thus contribute directly to the security and reliability of data.

13 - Vgl. IDW PS 330 Abschlussprüfung bei Einsatz von Informationstechnologie (Institut der Wirtschaftsprüfer, 2002), TZ 50f sowie KFS/DV1 Ordnungsmäßigkeit von IT Buchführungen (Kammer der Wirtschaftstreuhänder, 2011), TZ 59f



The effectiveness of general IT controls affects all applications. This means that a flaw in the general IT controls can lead to errors in all applications.

General IT controls are usually differentiated into four areas or domains[14]:

1. Controls Relating to the Procurement or Development of IT Systems

The purpose of these controls is to ensure that only such IT systems are procured and/or developed whose functionality meets the requirements related to the business processes of a company. Typical control areas are therefore the evaluation and clearance of purchases, authorisation of requirements for proprietary development, appropriate development processes, documented tests along with evaluation and clearance of test results, clearance for productive use, and separation of the functions for development/testing and productive use.

A secure procurement and development process and the change management process described in the following section support all three IT security goals (confidentiality, integrity and availability).

2. Controls Relating to Change Management

The same requirements as for proprietary development apply to controls in the area of change management. The goal is to ensure that authorised requirements enter the production system only via a documented process. This includes compliance with development specifications, documented tests, clear approval processes and the maintaining of function separation.

3. Controls Relating to Information Security and Access Protection

The purpose of this important area is primarily to ensure the integrity and confidentiality of data. The goal is to guarantee that only authorised persons within a company have access to precisely those data and applications that they need for their work. Among other things, these controls include:

- An authorisation concept,
- A documented user management process (clearance of new/changed users and permissions as well as timely deactivation of no longer needed users and permissions),

14 - KFS/DV1 Ordnungsmäßigkeit von IT Buchführungen (Kammer der Wirtschaftstreuhänder, 2011), TZ 61

- Written security guidelines (concerning system settings like passwords and logging),
- Regular checking of users and their permissions, as well as of security settings (e.g. passwords, virus protection, firewall rules, patch levels of operating systems), and
- Physical security (e.g. access controls, fire prevention measures).

4. Controls Relating to Operation of the IT Systems

The purpose of these controls is to ensure error-free and uninterrupted data processing. They are therefore primarily focussed on the protection goal of availability and include:

- Controlled and documented job management and monitoring,
- Regular data backups,
- Recovery instruments and processes for emergency cases, and
- Planning for emergencies.

3.3.4 COMPONENT "APPLICATION CONTROLS"

Application controls are controls that are integrated into individual IT applications, i.e. controls that are part of an application, operate automatically and ensure that accounting-relevant processing steps occur in compliance with the GAAP.[15]

Application controls are controls that are integrated into individual IT applications and operate automatically.

"Application-based controls can be classified into input, processing, and output controls. The effectiveness of application-based controls in preventing errors depends heavily on the effectiveness of the application-independent access protection controls and the controls relating to software change processes."[16]

Examples for application controls are required fields for data input, (automatic) checking for duplicates during the entry of master user data, (automatic) sum checking during data transmission, or (automatic) matching of orders, delivery notes and invoices (so-called three-way matching).

15 - The area of application controls is often understood to also include manual controls in the business processes, which will however not be discussed in this document.
16 - KFS/DV2 Abschlussprüfung bei Einsatz von Informationstechnik (Kammer der Wirtschaftstreuhänder, 2004), C.5. b)



The task of the annual account auditor, respectively of an IT specialist employed as part of the audit team, is to evaluate the consequences of the use of cloud services for the ICS and thus on the abovementioned IT areas, processes and controls under consideration of the three protection goals.

For companies with accounting obligations, this means that the criterion of orderliness as well as the suitability and effectiveness of the ICS in the abovementioned areas must already be taken into account during the selection of cloud services.

4 CHALLENGES AND RECOMMENDATIONS

For his work, the auditor can resort to the abovementioned auditing standards and expert opinions. At the international level, there is also the ISA 402 (International Standard on Auditing 402 "Audit Considerations Relating to an Entity Using a Service Organisation"), which has been adopted into various national standards. For Austria, the ISA 402 is primarily reflected in the PE 14 (Richtlinie des Instituts Österreichischer Wirtschaftsprüfer über die Prüfung bei ausgelagerten Funktionen); in Germany, in the IDW PS 331 (Institut der Wirtschaftsprüfer "Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen"); and in Switzerland, in the PS 402 (Treuhand-Kammer Schweizer Prüfungsstandard: "Unternehmen, die Dienstleistungsorganisationen in Anspruch nehmen – Auswirkung auf die Abschlussprüfung").

In the case of cloud services being used by the audited company, the auditor must proceed as follows:

- Determine the degree to which the use of cloud services is relevant to the annual account audit.
- Assess the error risks, in particular the control risk.
- Depending on the result of the error risk assessment, especially that of the control risk, test the ICS, and here especially the ICS in the IT processes.

In summary, the auditor's procedure in the case of the use of cloud services does not differ significantly from the general procedure or the procedures for other outsourcing setups. There are, however, several aspects that are specific to the cloud service setup and must therefore be taken into consideration.

4.1 RELEVANCE FOR THE ANNUAL ACCOUNT AUDIT (CLOUD SERVICE)

The auditor of the outsourcing company must first determine how significant the outsourced processes (cloud services) are and whether they are relevant to the annual account audit (keyword: accounting-relevant).

The auditor requires information about the service provider itself, its locations, the type and significance of the service, the contract terms, and the scope of the cloud usage.



The auditor therefore requires general information e.g. about the service provider itself, its locations, the type and significance of the service, the contract terms, and the degree to which the accounting system (e.g. GAAP, number and type of business transactions, affected accounts) and the ICS are affected by the use of the cloud service.

Challenge 1: Collecting Information

How can the auditor obtain this information? There are several possibilities that are best applied in combination with each other.

First there is the information collected in the interviews with the management of the outsourcing company and through investigations on the company itself conducted by the auditor. At this time (at the latest), the fact that outsourcing using cloud services occurs at the company should be recognised.

In addition, however, it is also necessary to collect information from the cloud provider itself about the employed cloud services. This constitutes a new challenge for the auditor as well as for the management of the audited company, which should likewise have an interest in this information being communicated as it is responsible for the ICS as legal representative. Collecting (and verifying) this information on-site with the cloud service provider can, however, be difficult or even impossible, particularly when dealing with large international cloud providers.

Recommendation:

The auditor as well as the management of the audited company are dependent on information provided by the cloud provider. As alternatives to on-site auditing at the provider's location, the following sources may also provide information on the relevance of the employed cloud services for the annual account audit:

- The contract between the outsourcing company and the cloud provider,
- Publicly available information (e.g. website of the cloud provider),
- Certificates or reports like EuroCloud StarAudit, for which a large amount of relevant information is evaluated and which are transparent and easily accessible through published self-assessments and validated audits,

- Audit reports according to ISAE 3402[17] and its local equivalents like SSAE 16[18] (USA), PS 951 (Germany), PE 14 (Austria), or according to the BSI C5 requirement catalogue[19] or the CSA STAR certification[20], or
- Reports by the internal revision department of the cloud provider, if they sufficiently address the required topics and are accessible to the auditor.

It should be noted that most certificates like the CSA STAR certification or ISO/IEC 27001[21], as well as reports from internal revision, generally contain little general information for the purposes discussed here — if any actual contents beyond the certificate are publicly accessible at all.

On the other hand, standardised self-assessments or, even better, audit reports created using the EuroCloud StarAudit system have proven to be very useful to auditors. These reports contain a multitude of relevant details in the control area A01 "Cloud Service Provider Profile" as well as in the control area A02 "Adequate Contract Terms".

The advantage of a standardised report is that the compilation of information on the cloud provider always leads to the same standardised report scheme, and the report is therefore easily understandable for the auditor.

One of the advantages of such a standardised report is that the compilation of information on the cloud provider always leads to the same standardised report scheme, and the report is therefore easily understandable for the auditor. Another advantage is that such a report (EuroCloud StarAudit) can be requested not by the cloud customer (i.e. the company subject to statutory audit), but rather by the cloud provider. The relevant information is thus not collected by the auditor or the customer, but provided by the cloud provider itself. This transfers responsibility for the correctness of the provided information to the cloud provider, who is therefore liable for any damages caused by serious errors in the information provided. The cloud service provider can compile such a StarAudit report easily and inexpensively online using a self-assessment process, and subsequently use the report as often as needed.

17 - International Standard on Assurance Engagements (ISAE) No. 3402 "Assurance Reports on Controls at a Service Organization", Report Type 1 and 2
18 - Statement on Standards for Attestation Engagements (SSAE) No. 16 "Reporting on Controls at a Service Organization", Report Type 1 and 2
19 - Bundesamt für Sicherheit in der Informationstechnik, Cloud Computing Compliance Controls Catalogue
20 - Cloud Security Alliance, Security, Trust & Assurance Registry



For the auditor, the existence of such a StarAudit report equates to quick and transparent access to a plethora of relevant basic information about the cloud provider, its service, and the involved subcontractors. In many cases, this report will provide the auditor with the opportunity to judge the relevance of the cloud provider respectively the employed service for the annual account audit, and estimate the complexity of any required additional tests.

The same essentially applies to BSI C5. Here the relevant information can be found in the requirement area "Environment Parameters". This section provides information on the framework conditions for the provision of the cloud service.

Reports according to ISAE 3402 or local equivalents usually contain this information in Section 2, "Description of the System for Provision of the Service".

If the annual account auditor concludes that the assessment of the control risk is independent of the outsourcing activity using cloud services, then the employed cloud services have no influence on the annual account audit.

If after collecting and evaluating this information the annual account auditor concludes that the assessment of the control risk is independent of the outsourcing activity using cloud services, then there is nothing more to be done in this context, as the employed cloud services have no influence on the annual account audit.

This can be the case e.g. if, simply put, an industrial manufacturer uses a cloud service for its staff cafeteria. If this cloud service clearly does not affect any significant business process and therefore no relevant accounts, it is not accounting-relevant in the context of the annual account audit.

If after collecting and evaluating the required information, however, the annual account auditor concludes that the assessment of the control risk is affected by the outsourcing activity using cloud services, then the general information from a self-assessment or audit report like StarAudit, ISAE 3402 or BSI C5 can provide basic details about the outsourced service and its provider. Further audit-specific information will nevertheless have to be collected.

4.2 ERROR AND CONTROL RISK (CLOUD CUSTOMER)

If the auditor concludes that the employed cloud services are relevant for the annual account audit, then he will need to assess the control risk along with the inherent risk.

If the auditor concludes that the employed cloud services are relevant for the annual account audit, then he will need to assess the control risk along with the inherent risk.

The auditor will have to examine how the outsourcing company takes the use of the respective cloud services into consideration within its own ICS.

To do so, he will need to collect additional information about cloud governance at the outsourcing company.

Challenge 2: Cloud Governance

While collecting information about cloud governance at the outsourcing company, the auditor will need to consider three key areas:

1. Identification of Cloud Services:

As the auditor's client, the outsourcing company should have mechanisms in place that allow cloud services used at the company to be identified. This applies in particular to cloud services that are not employed in a planned fashion by management ("shadow IT"). Such shadow IT services have to be included in an appropriate risk management system. For example, a process should be established that deals with the question of which data is allowed to enter the cloud at all, and who is responsible for it.

Cloud computing leads to changed and new tasks and responsibilities in supplier management and IT operation at the outsourcing company, and the control environment[22] plays an important role in this context. Affected aspects include risk awareness among staff, the risk management philosophy, and the way in which competences and responsibilities are distributed and subsequently monitored within the company. The control environment affects the way in which risks are recognised, evaluated and

22 - Vgl.: https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf



ultimately reduced to an acceptable level through appropriate measures.

Cloud computing leads to changed and new tasks and responsibilities in supplier management and IT operation at the outsourcing company.

2. Risk Management for Cloud Services:

The outsourcing company should integrate the use of cloud computing into its risk management system and adapt the system accordingly. Important topics to address are data privacy, the sensitivity of data, reliability (GAAP-compliant registration, processing and output of data), resilience and elasticity, and the regulations to be observed. A business partner due diligence process should also take into account the specific requirements of cloud computing. The company should be able to recognise and evaluate the risks caused by the use of cloud computing and take appropriate measures.

3. Control (ICS) of the Cloud Services:

The goal is to establish appropriate measures to control the recognised risks, beginning with the installation of strategies and guidelines and continuing to the adaptation of processes and the establishment of new and changed internal controls. For the annual account auditor, it is essential that the use of cloud services is reflected in the (accounting-relevant) ICS of the outsourcing company.

Recommendation:

The recommendation for the annual account auditor is to acquire knowledge on whether cloud services are currently in use at the audited company or will be in use there in the future, and advise the company to implement an appropriate cloud governance system ahead of time. The cloud governance system should generally be in place for the entire fiscal year, or the entire time of the use of cloud services during the respective fiscal year.

If the annual account auditor finds such a documented and properly configured cloud governance system in place at the audited company, then this constitutes an excellent basis for the assessment of the control risk.

In regard to the business partner due diligence process, i.e. the quality assurance and risk assessment for the employed cloud service, it is once again beneficial if the cloud provider has a quality certificate like EuroCloud StarAudit. The areas A02 (Legal Compliance) and A03 (Security and Data Protection) evaluate a multitude of requirements and make the results of those evaluations transparent.

Cloud service certificates simplify the processes of selecting and assuring the quality of a provider or cloud service and support due diligence.

For the customer, this simplifies the processes of selecting and assuring the quality of a provider or cloud service and supports due diligence. It simultaneously reduces the required effort on the part of the cloud customer and transfers liability for the correctness of the information about the cloud provider and its service to the provider itself, respectively to the auditor who compiled the corresponding report.

4.3 ERROR AND CONTROL RISK (CLOUD PROVIDER)

As mentioned above, it is also necessary to collect information from the cloud provider about the provider itself and the employed cloud services. This constitutes a new challenge for the auditor as well as for the management of the audited company, which should likewise have an interest in this information being communicated as it is responsible for the ICS as legal representative.

Challenge 1: Collecting Information

The annual account auditor requires information about the service-related ICS at the cloud provider, especially about the processes through which the cloud services are provided as well as about the relevant risks and established internal controls. These internal controls must incorporate the components described in Sections 3.3.2. to 3.3.4 (IT control environment, general IT controls, application controls). The goal is to allow the auditor to evaluate the adequacy of the service-related ICS at the cloud provider.



Recommendation:

The auditor as well as the management of the audited company are dependent on information provided by the cloud provider. The following sources are particularly useful for collecting information on the adequacy of the service-related ICS at the cloud provider:

- Audit reports according to ISAE 3402 Type 1 and 2, or according to local equivalents like SSAE 16 (USA), PS 951 (Germany), PE 14 (Austria),
- Audit reports according to BSI C5, which is based on international and national auditing standards for its auditing and reporting — like ISAE 3402 or the U.S. SOC (System and Organization Controls)[23],
- Audit reports according to CSA STAR, which is based on the U.S. auditing standard SOC and carries the AICPA[24] logo, and
- Internal revision reports by the cloud provider.

For these reports to be relevant for the assessment of the control risk, they must provide concrete information on processes, risks (including control goals, if applicable) and controls.

For reports to be relevant for the assessment of the control risk, they must provide concrete information on processes, risks (including control goals, if applicable) and controls.

Challenge 2: Cloud Governance

Used only on the customer side, not on the provider side.

Challenge 3: New and Changed Risks

From the point of view of the outsourcing company, the use of cloud-based applications or services represents an externally provided service, which creates additional and changed risks and expands the area of application of the ICS to include this external service.

The additional and changed risks are not caused by the factor of outsourcing itself, but rather by the specific characteristics of cloud computing. These include the features

23 - Cf. https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/CPAs.aspx
24 - Vgl.: http://www.aicpa.org/Pages/default.aspx

mentioned in Section 2.1, among others. This fact entails a need for new and changed controls that take the additional and changed risks into account, e.g. in the area of general IT controls.

The task of the annual account auditor, respectively an IT specialist as part of the audit team, is to recognise and take into account the additional and changed risks resulting from the use of cloud services.

The task of the annual account auditor, respectively an IT specialist as part of the auditing team, is to recognise and take these risks into consideration during evaluation of the adequacy of the corresponding controls.

Recommendation

The auditor as well as the management of the audited company are dependent on information provided by the cloud provider.

Analysis of the contents and control areas of EuroCloud StarAudit, CSA STAR and BSI C5 with a view to the requirements for the component "general IT controls" described in Section 3.3.3 has revealed that

- EuroCloud StarAudit is very broad in regard to IT risks, but does not yet address many of the requirements for general IT controls. Publication of a new control catalogue for auditors is planned for September 2017.
- CSA STAR has a strong focus on information security and addresses most of the requirements for general IT controls, and
- BSI C5 similarly addresses most of the requirements for general IT controls, albeit with a somewhat less heavy focus on information security.

For the sake of completeness, it should be mentioned that wherever the requirements for general IT controls are addressed in the abovementioned audit schemes, the additional and changed risks are likewise covered and appropriate new and adapted controls are described.



Examples:

- IT control environment: Changed risk due to virtuality — with a view to function separation, the role definition regards the management systems for virtual machines as an additional layer.
- Change management: New risks resulting from multi-tenancy (resource pooling) — changes affecting all systems are evaluated in terms of their effects on different customers in the same virtualisation environment and formally cleared for use by the individual customers.
- Information security and access control: Higher risk due to open connection to the Internet: two-factor or multi-factor authentication on the basis of certificates or tokens; automatic temporary assignment of user accounts and permissions.
- IT system operation: Higher risk due to self-service and elasticity. The backup process must ensure that the restore process will work even after changes to services and the system itself.

It should be noted, however, that application controls are not covered by these standards and specifications. This is naturally due to the individuality of the various applications. Hence these certificates and audit schemes can only be used for the evaluation of the components "IT control environment" and "general IT controls". Within the component "general IT controls", the requirements in the area "procurement or development of IT systems" are the least addressed in all abovementioned certificates and audit schemes.

Since ISAE 3402 and its local equivalents are audit standards that impose no requirements in terms of content, reports according to these audit standards can potentially include additional application controls for certain applications of a cloud provider.

When dealing with IT topics, the content of audit reports according to ISAE 3402 and their local equivalents is typically based on standards like COBIT[25], a CSA Cloud Controls Matrix, or BSI C5 requirements.

It is important for the auditor to study the contents of the audit reports and certificates closely and compare them to his requirements to evaluate whether the available information is sufficient for his analysis.

25 - Vgl. http://www.isaca.org/COBIT/Pages/default.aspx

It is therefore of the utmost importance for the auditor to study the contents of the audit reports and certificates closely and compare them to his requirements to evaluate whether the available information is sufficient for his analysis. The disadvantage that these audit standards do not uniformly standardise their contents can be mitigated by the auditor by obtaining the entire respective audit report(s) and analysing it (them) in detail. With certificates such as EuroCloud StarAudit, the audit contents are standardised and predefined in detail, which means that the audit reports are likewise standardised and comparable section by section.

Challenge 4: Knowledge and Experience of the Auditor(s)

The issues discussed under "Challenge 3" lead to another significant aspect that should not be underestimated:

The annual account auditor must be capable of understanding additional and changed risks resulting from the use of cloud services and be aware of appropriate controls in order to correctly assess the control risk and evaluate the adequacy of the ICS. This in turn means that auditors will require more technical background, knowledge and experience in combination with their understanding of the audit approach, revision processes and business management than ever before. Appropriately trained and knowledgeable specialists are already in high demand today.

The increasing use of cloud services by companies subject to statutory audit will continue to drive demand for specialists – it will become more and more difficult to find experienced audit personnel.

The increasing use of cloud services by companies subject to statutory audit will continue to drive demand for such specialists. It can be assumed that it will become more and more difficult to find experienced audit personnel with sufficient know-how.



Recommendation:

Only very general training policy recommendations can be made here, as the topic is obviously well beyond the scope of this guideline.

Audit firms that recognise the impending lack of sufficiently qualified personnel and wish to counteract it can do so with a combination of measures:

One possible measure is to seek qualified employees among the graduates of appropriate higher education facilities with curricula in the field of commercial information technology. As this is generally already the case, but the combination of auditing and cloud is a very specific one, this approach alone will not be sufficient.

An appropriate internal training scheme should be established in addition. The training curricula need to focus specifically on the new challenges concerning the area of cloud computing and auditing.

Furthermore, audit firms must ensure that employees are able to gain experience in appropriate annual accounts audit projects in which accounting-relevant cloud services must be assessed. Two approaches are possible: training of employees who possess sufficient know-how in both areas (IT/cloud and auditing), or the establishment of teams consisting of an audit specialist and an IT specialist. This paired combination of specialists will naturally lead to increasing understanding for the respective other partner's challenges and contents over the course of several audit projects.

It should be noted, however, that many audit firms may currently not be faced with a sufficient number of appropriate audit orders to warrant the training of such specialists or teams. The high demand for such specialists, and the demand for well-trained and experienced IT staff in general, has been driving salary requirements continually over the past years, and this trend cannot reasonably be expected to change in the near future. Under these circumstances, many audit firms will likely be unable to employ an appropriate number of such specialists. One possible path out of this dilemma may lie in increased cooperation between audit firms and IT consulting firms.

4.4 EFFECTIVENESS OF THE ICS (CLOUD PROVIDER)

If the annual account auditor concludes on the basis of the assessment of the control risk that the ICS is sufficiently reliable, then the next step is to test the effectiveness of the ICS.

To test the effectiveness of the ICS, the auditor must collect a sufficient amount of evidence that the controls are applied as planned and described, continuously and in a timely manner, throughout the entire audit period (fiscal year).

On the client side (i.e. at the outsourcing company), the auditor can also perform these tests efficiently and in a targeted manner regarding cloud governance.

On the cloud provider side, the auditor could conduct tests on site at the provider. In practice, however, problems might ensue if every auditor wanted to conduct tests at the provider's location.

On the cloud provider side, the auditor could in principle conduct test activity on site at the provider. In practice, however, problems might ensue if every auditor for every company outsourcing to the cloud provider wanted to conduct tests at the provider's location. Besides the high costs of such "audit tourism", the operations of the cloud provider might be seriously hampered and various security issues raised by this activity.

Alternatively, the annual account auditor may request suitable specific information from the cloud provider. The provider is obliged to provide comprehensible information on control goals, control descriptions, performed tests and their results. The procedures for these tests must conform to the procedures that the auditor would have applied if conducting the tests himself (i.e. according to the ISA standards) to ensure that the resulting information provided by the cloud provider can be used by the auditor.

In this case, the auditor is once again faced with the abovementioned challenges of collecting information, of new and changed risks, and of his or her own knowledge and experience in regard to the effectiveness of the ICS.



As for the evaluation of adequacy, the controls implemented at the cloud provider must include the components mentioned in Sections 3.3.2 to 3.3.4 (IT control environment, general IT controls, application controls).

Recommendation:

Sources suitable for evaluation of the effectiveness of the service-related ICS at the cloud provider by the annual account auditor currently include:

- Audit reports according to ISAE 3402 Type 2 and their local equivalents,
- Audit reports according to the BSI C5 Requirement Catalogue, which is based on international and national auditing standards for its auditing and reporting — like ISAE 3402 or the U.S. SOC (System and Organization Controls), or
- Audit reports according to CSA STAR, which is based on the U.S. auditing standard SOC and carries the AICPA logo.

Only such audit reports allow the annual account auditor to rely on the controls described and tested within them and achieve certainty in regard to the annual account audit.[26] And only these types of audit reports ensure that the controls have been tested according to the auditor's requirements.

From the point of view of cloud service users, appropriate audit reports and certificates like EuroCloud StarAudit provide the advantage that they support the confirmation of observance of due diligence during the selection and use of an external service provider.

26 - See Section 3.1

5 SUMMARY

In summary, it can be said the use of cloud services by a company subject to statutory audit creates a number of new challenges. The outsourcing company itself, i.e. the annual account auditor's client, will need to take various measures, especially in regard to governance of the cloud services.

When examining the steps taken by the auditor, it is clear that while the approach is essentially very similar to that taken in regard to traditional outsourcing, the auditor is also faced with several new challenges. Unfortunately, not all of these new challenges currently have clear-cut and comprehensive solutions. The annual account auditor will nevertheless have to deal with many of these aspects in order to establish appropriate expertise and internal know-how.

There are several different possibilities for the auditor to collect information on the type and accounting relevance of the employed cloud services. The available sources have quite different scopes, however, and therefore provide different elements of information. Special mention should be made of the following certificates and audit schemes: EuroCloud StarAudit, CSA STAR, ISO 27001, and ISAE 3042 Type 2 with local equivalents. These sources provide additional opportunities for the auditor to obtain an understanding of the type and effectiveness of the established internal control systems.

In regard to cloud providers, it can be stated with certainty that they need to tackle the task of establishing sufficient and comprehensive transparency to allow their cloud services to be assessed by annual account auditors.



6 APPENDIX

6.1 LEGAL INFORMATION

General

The information provided in this document serves as a general description of particular legal aspects in connection with cloud computing. This information does not constitute legal counsel nor can it replace it, as proper legal counselling generally requires knowledge of all specific circumstances of the concrete individual case.

Contents of the Guideline

The editor and authors assume no liability for the correctness, completeness or currentness of the information provided in this document. This applies in particular to new developments in jurisprudence or legislation. Any liability claims against the editor or authors related to material or ideal damages caused by the use or non-use of the information provided in this document, as well as by the use of incorrect or incomplete information provided in this document, are excluded on principle.

References and Links

In regard to direct or indirect references to foreign content (e.g. web links) outside of the responsibility of the publisher/the authors, a liability obligation would arise only if the publisher/the authors had knowledge of the information and were technically able to, and could reasonably be expected to, prevent its use in the case of unlawful contents. The publisher/the authors hereby declare that no unlawful contents were recognizable on the linked webpages at the time of placement of the links. The publisher/the authors have no influence on the current or future design, contents, or authorship of the linked webpages. They explicitly distance themselves from all contents of the linked webpages which were changed after placement of the respective links. Only the offeror of the respective linked webpage shall be responsible for any unlawful, incorrect or incomplete contents, and in particular for any damages resulting from the use or disuse of information thus provided, and not the person referencing the webpage by way of web links.

Copyright

The content provided in this guideline, including texts, graphics or images, is protected by Austrian copyright law. Any use not permitted by copyright law requires prior written consent by the publisher. Contributions by third parties are identified as such. This applies in particular to any duplication, editing, processing or reproduction of contents in databases or other electronic media. Unauthorised duplication or dissemination of the whole or any part of this guideline is explicitly prohibited. Individual and private use is excluded from this prohibition, but private use does not include any right to pass the guideline on to others. The same applies to publications or other documents.

Compensation

This guideline is provided to its addressees/recipients free of charge.



6.2 AUTHORS

Mag. Markus Ramoser CISA, CIA, CRMA
PwC Österreich GmbH Wirtschaftsprüfungsgesellschaft
Senior Manager, Risk Assurance
Erdbergstraße 200
A-1030 Wien
Tel.: +43-1-50188-2129
E-Mail: markus.ramoser@at.pwc.com



Dr. Tobias Höllwarth
SOURCING INTERNATIONAL
Palais Savoy, Johannesgasse 15
A-1010 Wien
Tel.: +43 664 4060900
E-mail: tobias.hoellwarth@hoellwarth.at



Jörg Asma
DXC Technology
Ettore-Bugatti-Straße 6-14
51149 Cologne
E-mail: jasma@dxc.com



Manfred Scholz
SEC4YOU Advanced IT-Audit Services GmbH
In der Fischerzeile 13/10
A-2100 Korneuburg
E-mail: manfred.scholz@sec4you.com





PRINTING SPONSORED BY

SOURCING INTERNATIONAL
Digital Transformation Advisors

EuroCloud.Austria
Verein zur Förderung von Cloud Computing
Museumstraße 5/14
1070 Vienna, Austria

E-Mail: info@eurocloud.at
Web: http://www.eurocloud.at
Seat of the Association: Vienna
Copyright: EuroCloud.Austria 2017



EuroCloud.Austria - Verein zur Förderung von Cloud Computing
Museumstraße 5/14
1070 Vienna, Austria

E-Mail: info@eurocloud.at
Web: http://www.eurocloud.at
Seat of the Association: Vienna
Copyright: EuroCloud.Austria 2017