Guide to the Audit of IT Applications

May 2009

Authors: Peter R. Bitterli • Jürg Brun • Thomas Bucher • Brigitte Christ
Bernhard Hamberger • Michel Huissoud • Daniel Küng • Andreas Toggwyler • Daniel Wyniger
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of contents</td>
<td>1</td>
</tr>
<tr>
<td>General presentation and introduction</td>
<td>2</td>
</tr>
<tr>
<td>Analysis of the balance sheet and the profit and loss account</td>
<td>5</td>
</tr>
<tr>
<td>Identification of business processes and data flows</td>
<td>7</td>
</tr>
<tr>
<td>Identification of core IT applications and the main IT relevant interfaces</td>
<td>11</td>
</tr>
<tr>
<td>Identification of risks and key controls</td>
<td>16</td>
</tr>
<tr>
<td>Walkthroughs</td>
<td>20</td>
</tr>
<tr>
<td>Assessment of control design</td>
<td>22</td>
</tr>
<tr>
<td>Testing operating effectiveness</td>
<td>26</td>
</tr>
<tr>
<td>Overall assessment and conclusions</td>
<td>30</td>
</tr>
<tr>
<td>Annex 1 – Application controls</td>
<td>32</td>
</tr>
<tr>
<td>Annex 2 - Glossary</td>
<td>36</td>
</tr>
</tbody>
</table>
General Presentation and Introduction

Objective of approach
For process-oriented application-dependent audits, an integrated audit approach of both auditors and IT auditors will ensure that all important areas are adequately taken into account and, at the same time, that any IT-specific areas with a significant influence on the audit objective are also reviewed. The absence of an agreed-upon procedure between auditors and IT auditors constitutes a high audit risk.

This paper puts forward an integrated approach for business process oriented application audits designed to counter this audit risk.

Scope and delimitation of scope
The audit approach presented here is limited to the audit of IT applications within business processes. Related areas are mentioned insofar as they interface with the audit approach, but are not dealt with in detail. Examples of this are sampling, required qualifications for auditors and general IT controls (application independent controls).

The application of this approach is not limited to statutory audits; indeed, it was deliberately kept generic and can therefore also be applied to other types of audit (e.g., compliance audits).

Users
The description of the approach and the examples mentioned are oriented towards the audit of the annual accounts. Given its generic character, the approach can be used by both financial and IT auditors.

The audit of a company's financial statements (i.e., financial reporting) presents financial auditors with an increasing number of challenges; on the one hand, there has been a rapid development in accounting standards and, on the other hand, an increasingly automated “production” of financial data by means of ever more complex information systems. This latter aspect is the subject of this paper.

The quality of financial data depends substantially on the quality of the business processes and the related data flows. It is therefore clear that the auditor will concentrate on the control environment of these business processes and include the audit of the corresponding IT applications in his/her audit approach.

The approach presented below aims to help the financial auditor develop an integrated audit approach and, by including the audit of the relevant business processes and the corresponding IT applications, lead him/her to an efficient and more risk oriented audit procedure. The approach therefore begins with an analysis of the company's financial statements and ends with an appraisal of the impact of the audit results on these statements.
An 8 step approach:

1. **Analysis of Balance Sheet and Earnings Statement**
2. **Identification of Business Processes and Information Flow**
3. **Identification of Major Applications and the most Important IT-relevant Interfaces**
4. **Identification of Risks and Key Controls**
5. **Walk-through**
6. **Evaluation of Control Design**
7. **Testing Operating Effectiveness**
8. **Overall View and Final Conclusion**

To consistently focus the audit activities for the business processes and IT applications on risks related to financial reporting, we will first analyse its financial statements. This analysis will allocate all significant accounting items to the relevant business processes, or more specifically, it will determine which data flows “produce” which accounting items and which core IT applications manage these data flows.

Once the core IT applications have been identified, the auditor will examine the quality of the control system. First of all, he/she will determine whether the design of the control system represents an adequate response to the existing risk situation of the business process and then whether the intended controls are implemented and are effective.

The assessment of the control system used for the business processes within the audit scope enables the auditor to obtain evidence as to how far he/she can rely on the procedures used to produce the relevant accounting items and, where applicable, establish to what extent he/she will need to carry out additional substantive testing procedures.

Explicitly, this approach does not cover “general IT controls“. The auditor must, if need be, evaluate and test the general IT controls so as to develop a suitable strategy for his/her audit of application controls. General IT controls are largely decisive for determining whether an (IT) application control that is judged to be effective from the design point of view can be assumed to have worked effectively throughout the audit period, or whether the auditor will need, for example, to assess it explicitly through direct tests (e.g., substantive testing).

The approach is based on the four layers model schematically pictured below. In reality, the links may be much more complex, but this simplified model will facilitate understanding our approach.
Delimitation of the audit approach

The figure above gives a simplified picture of the layer model used in this audit approach. Each of the four layers represents a specific set of process and resource types:

- The upper layer (blue) contains all the company’s essential (manual) processes – typically broken down by responsible departments and sub-processes and individual activities.
- The second layer (red) contains the automated parts of the business processes, the actual IT applications. With perhaps the exception of really small SMEs, most commercial transactions in practically all companies are handled via IT applications of this sort.
- The third layer (yellow) contains the core IT systems. This term covers a multitude of possible platforms on which the actual IT applications in the second layer run. Examples of this would be actual data base management systems (e.g., Oracle, DB2), basic components of integrated IT applications (e.g., SAP Basis, Avaloq etc) or more technical processing systems (e.g., middleware).
- In the lowest layer (green), we can find the IT infrastructure. Essentially, this layer includes the actual hardware (mainframe, peripheral systems, servers) as well as the relevant network components and technical operating and surveillance systems.

The approach presented in this document mostly concerns the upper two layers (indicated with a green arrow) – in other words, application dependent controls in the business processes and the IT applications that support them. The lower two layers, the IT infrastructure including the underlying IT processes (indicated with a red arrow) are, of course, important from the auditor’s point of view but are not further discussed here.
1 Analysis of the Balance Sheet and the Profit and Loss Account

Overview

Content and objective: We are assuming that the audit objective is the regularity of the accounts. The procedure is therefore as follows:
- Establish which items in the balance sheet and the profit and loss account are relevant for the audit
- Identify the transactions or transaction classes that generate these items

Background: An analysis of the balance sheet and the profit and loss account is essential to a targeted risk-oriented audit and serves to identify the relevant items on the balance sheet and in the profit and loss account. This analysis provides the auditor with important information needed to identify risks and ascertain any current developments that may influence the annual accounts. At the same time, it will serve as a planning instrument to enable him/her to establish the main audit priorities and the audit methods to be applied.\(^1\)

Approach

Material Accounts e.g. Accounts receivables

- RISK
  - Assertions, e.g.:
  - Validity
  - Valuation
  - Completeness
  - Rights and Liabilities

1 A “transaction class” is a group of operations or business transactions within a business process that have a similar subject matter and can substantially be booked in the same way.

Identification of relevant accounts/groups of accounts

The auditor carries out a risk assessment and identifies any risks that may influence the annual accounts so that he can then direct his/her audit activity towards these. The establishment of materiality plays an important role in this.

The auditor identifies the accounts/groups of accounts which exceed the materiality threshold and consequently fall within the scope of the audit.

The auditor also identifies the accounts/groups of accounts whose existence or modification are subject to specific risks or is indicative of specific risks, for example because of unexpected changes in key operating figures.

Identification of significant transactions and transaction classes

Once the accounts/items have been identified, the auditor can then analyse which transactions or transaction classes have the greatest influence on them. Here, it may be advisable to carry out a data analysis to identify which entries have been made to specific accounts. This will enable the auditor to work out which transactions were at the origin of these entries. This could be done in an ERP environment by sorting the electronic accounting transactions by transaction type.

The auditor can therefore work from the main accounts and groups of accounts via the major transactions back to the underlying business operations that generated those transactions.

The advantage of this reverse approach is that it can exclude, from the outset, unimportant transaction classes resulting from less-relevant sub-processes. Once the auditor has identified the relevant transaction classes and the underlying business operations that generated them, he/she can carry out a risk analysis for the individual stages of the process as described in the following step.

Special considerations

In an IT applications audit, the auditor will generally concentrate on routine transactions, as these are predominantly processed by the IT application and include the majority of the automated and IT-dependent controls. The non-routine transactions, particularly in estimation procedures, are often governed by mostly manual controls.

At this point in his/her work, the auditor should also take into account the main events in the company that have influenced the accounts or transaction classes selected, like, for example:

- the introduction of a new IT application;
- the migration of IT applications or application data.

---

3 Swiss Audit Manual, 1998, Chapter 3.114: “All elements that influence the evaluation and presentation of the individual accounts, the consolidated annual statements or individual items thereof, insofar as the statement is modified to such an extent that the recipients of the individual accounts or consolidated statements may be influenced in their decisions regarding the company concerned.”
2 Identification of Business Processes and Data Flows

Overview

<table>
<thead>
<tr>
<th>Content and objective</th>
<th>Identify the relevant business processes which are at the origin of the transactions and transaction classes determined previously. The expression “relevant business processes” refers to the important processes that have a direct influence on financial reporting. It includes the accounting process as such, business processes like invoicing or support processes, e.g., in the area of human resources. IT processes as defined in COBIT, for example, are not affected.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background</td>
<td>A company’s financial statements are the result of the interaction of a number of activities, which can be grouped together in processes of different types (complex processes limited in time; processes that may influence a number of transactions etc). Potentially, certain weaknesses in these processes may cast doubt on the validity of the financial reporting. This is why a careful identification of the business processes and data flows is indispensable to be able to evaluate the risks within each process.</td>
</tr>
</tbody>
</table>

Procedure

Identification of relevant processes

On the basis of the transactions or transaction classes identified, the auditor now identifies the processes that influence these items. The spectrum ranges, for example, from the year-end process, which is limited in time (with a direct influence on the amount of a provision, for example), to a complex sales and invoicing process which influences the flow of goods and the financial flows. In this latter case, a number of items on the balance sheet and profit and loss account will have the same process as their “source”.

Processes can be shown in the form of a process map in a table or graph. These two forms of representation have advantages, which it may be useful to combine in the case of complex process contexts.

Utilisation of existing documentation

Where available, the auditor should base his/her work on existing process documentation. This documentation will generally concentrate on activities and will specify, for each step in the process, the input, processing, output and roles of the various players. However, this type of documentation rarely contains the process risks or the key controls, which must therefore be identified and documented by the auditor at a later stage in the (IT) application audit.

Creation of new documentation – forms of representation

The auditor must acquire a sufficiently detailed understanding of the selected processes. A distinction must be made here between the routine business processes (e.g., the sales process) and the non-routine financial processes (e.g., consolidation of the quarterly figures of a branch or the calculation of the annual depreciation of a fixed asset). There are risks in both types, which may materially affect the annual accounts.

---

4 A process may be defined as a “chain of manual, semi-manual automated tasks that serve to create or process information, products or services. Examples: sales, debt collection, production, inventory, bookkeeping etc.”
Presentation in table form – suitable for simple facts and contexts

<table>
<thead>
<tr>
<th>Item on the balance sheet or in the profit and loss account</th>
<th>Amounts in thousands of CHF</th>
<th>Output</th>
<th>Process</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turnover</td>
<td>675'123</td>
<td>Invoices</td>
<td>Sales</td>
<td>Contracts, services provided</td>
</tr>
<tr>
<td>Costs</td>
<td>422'234</td>
<td>Payments</td>
<td>Purchases</td>
<td>Orders</td>
</tr>
<tr>
<td>Inventory</td>
<td>57'000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment</td>
<td>121'000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creditors</td>
<td>45'000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff expenditure</td>
<td>121'111</td>
<td>Payments</td>
<td>HR management</td>
<td>Contracts, performance</td>
</tr>
<tr>
<td>Social charges</td>
<td>13'000</td>
<td></td>
<td></td>
<td>Etc</td>
</tr>
<tr>
<td>Plant</td>
<td>121'000</td>
<td>Depreciation</td>
<td>Closure</td>
<td>Value</td>
</tr>
<tr>
<td>Various</td>
<td></td>
<td>Consolidated items</td>
<td>Consolidation</td>
<td>Items of a branch</td>
</tr>
</tbody>
</table>

Graphical presentation (process model chart) – suited for complex interactions

Example A
Example B

Graphic presentation (dataflow form) – suited for the analysis of complex interactions
Special considerations

Level of detail

A generic description makes it more difficult to identify risks but too much detail may adversely affect the analysis and readability. Depending on the complexity of a process, it may be advisable to subdivide it into a number of sub-processes.

Examples

- The purchase process consists of the following sub-processes: management of supplier master data, supplier invoicing and booking of purchases.
- The sales process consists of the following sub-processes: management of client master data, client invoicing and booking of sales.
- The salary process consists of the following sub-processes: management of staff data, preparation of salary statements, establishment of salary, salary payments and booking of salaries.

Management of parameters and master data

For certain business processes, it is advisable to consider the administration (i.e., initiation, maintenance, deletion) of parameters and master data as two distinct sub-processes:

- The parameters of an IT application are constant and common values that steer the processing of similar types of transactions (e.g., the deduction rate for a pension fund in a salary application).
- The master data are permanent attributes of an object, e.g., accounts payable master data, client master data, product master data.

Manual interfaces

The objective of this step is to understand the flows of relevant information and data. This does not mean just electronic data; an adequate analysis will also take into account document flows (e.g., stock evaluation reports) as well as manual interfaces.
3 Identification of Core IT Applications and the Main IT Relevant Interfaces

Overview

Content and objective
Identification of relevant IT applications and their interfaces

Background
Many controls are automated and integrated in the IT applications. The automation of process steps may cause further inherent risks. This includes, for example, the problem of implementing an adequate segregation of duties and also a generalised lack of human control due to the high level of integration, real time processing and the single point of entry principle, whereby, once entered, transactions are processed automatically and immediately booked.

It is therefore useful to identify the IT applications concerned, their characteristics and their interfaces early in the audit process. This information makes it possible to establish a detailed definition of the audit scope and to determine the audit programme.
Procedure

Determine the IT application landscape

The representation of the relevant IT applications in a landscape map may not always be in sync with the data flow overview. In particular with heavily integrated IT applications (e.g., Enterprise Resource Planning Systems, ERP), several business processes are supported by one and the same IT application (e.g., automatic integration of a purchase process with a sales process).

Example

Inventory and categorisation of financially relevant IT applications

We distinguish between the following types of IT application. As these have very different risk profiles, the type of IT applications is an important feature to be taken into consideration for the planning and execution of the audit and must therefore be documented:

- standard IT applications
- highly adapted standard IT applications
- internally developed IT applications
Standard IT applications

Standard IT applications with a certain maturity level generally have a multitude of relevant embedded controls. The table below gives an example of some basic controls aimed at ensuring the integrity of processed transactions:

<table>
<thead>
<tr>
<th>A standard bookkeeping application must contain the following functionalities (non-exhaustive list)</th>
<th>These functionalities offer (or imply) the following controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations and transactions automatically dated with system date</td>
<td>Access protection for the system date</td>
</tr>
<tr>
<td>User identifications with authentication mechanisms</td>
<td>One way encryption of password</td>
</tr>
<tr>
<td></td>
<td>Password syntax check</td>
</tr>
<tr>
<td></td>
<td>Password validity check</td>
</tr>
<tr>
<td></td>
<td>Logging of failed access attempts</td>
</tr>
<tr>
<td>Parametrisable authorisations</td>
<td>Access protection via profiles or individual authorisations</td>
</tr>
<tr>
<td>Change log for parameter and master data changes (security parameters, chart of accounts, creditor and debtor master data, etc)</td>
<td>Automatic storage of changed values in a history file (with date valid from/to, change date and identification of the user who carried out the change)</td>
</tr>
<tr>
<td></td>
<td>Access protection for parameters and history file</td>
</tr>
<tr>
<td>Delete prevention</td>
<td>The IT application should not have a delete function.</td>
</tr>
</tbody>
</table>

Furthermore, the controls listed below are also very important:

- validation of input (e.g., selection lists, validation formulae etc),
- management of processing (job control, order of daily, monthly, end of year etc processing),
- processing of transactions (e.g., workflow management, limit checks, four eyes principle and electronic signature, match controls between order/delivery/invoice),
- output management (availability of reports, etc).

In the assessment of standard IT applications, answers should be provided to the following questions:

- What type of standard application does the company use?
- Is the standard application usual in the sector of activity concerned?
- Is the standard application certified?
- Is the standard application a well established and widely used application or a new one?
- Is information available about this application and potential security or processing weaknesses (remark: standard IT applications sometimes contain errors and the auditor must obtain a sufficient knowledge of known sources of error).
- Does the auditor have sufficient knowledge and experience of the application?
The replies to these questions serve, as stated in paragraph 10 of Swiss Audit Standard 310, to “identify audit areas that require particular attention or knowledge”. They provide the auditor with an understanding of the inherent risks arising from the utilization of the software in question.

If the auditor comes to the conclusion that there are no known weaknesses in the standard IT application in the relevant areas, he/she will be able to limit his/her efforts in the identification of risks and the assessment of the relevant controls in the subsequent steps of the approach. As a minimum procedure, the auditor should ensure that:

- the expected controls exist and are applied
- in the case of IT application parameters, that these were active during the audit period concerned

*Highly adapted standard IT applications*

Highly adapted standard IT applications are software packages that provide the basic functionalities and tools for the design of processes and work flows but they can be given strong client-specific characteristics via customizing and individual additional programming. Here, the auditor is faced with a great challenge, insofar as, even if he/she has information concerning the reliability of the components (as may be the case with very mature systems), but the auditor will not have any public information concerning the interaction of these components and possible configurations and additional programming in a client-specific environment. In situations of this type, the auditor must allow for more time for the identification of risks and the assessment of the relevant controls. The more a standard IT application has been adapted to the specific requirements of a company, the more the analysis of parameters, workflow management and technical programme adaptations is important.

*Internally developed IT applications*

In the case of internally developed IT applications, the auditor will find a situation in which he/she is least able to use generally known information and experience with the IT application and must therefore adapt his/her audit procedure to the IT application concerned. Internally developed IT applications generally require more audit work. In situations of this kind, cooperation between the auditor, the people responsible for the IT application and, where applicable, the IT application developers is of great importance.

For reasons of efficiency, in the case of highly adapted standard IT applications and internally developed IT applications, the auditor will base his/her work as far as possible on documented tests within the company. If the expected tests do not exist or are not relevant (test design or test documentation lacking, errors not corrected after tests, no formal acceptance by users etc), he/she must carry out the tests required for his/her audit himself.

*Outsourcing*

The outsourcing of activities or business processes involves additional inherent and control risks because of the shared responsibility. Of particular relevance are the audit procedures performed by the auditor of the service organization. In this context, two standards are of particular importance: Audit Standard 402 and SAS 70 must be taken into account in this case.
Centralised or decentralised use of the IT application

Moreover, because of the shared responsibilities and also because of an often considerably greater technical complexity (e.g., with regard to data integrity due to redundant data storage or process steps over different time or date zones), the decentralised use of an IT application involves additional inherent and control risks and increases the complexity of the audit.

Representation of information

Table based representation

<table>
<thead>
<tr>
<th>Balance sheet item</th>
<th>Amount in 000 CHF</th>
<th>Process</th>
<th>Application used</th>
<th>Comment / upstream system</th>
<th>Type</th>
<th>Internal/external</th>
<th>Centralised/decentralised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue</td>
<td>675’123</td>
<td>Invoicing</td>
<td>SAP FI</td>
<td>Invoice and delivery interfaces</td>
<td>Standard</td>
<td>Internal</td>
<td>Centralised</td>
</tr>
<tr>
<td>Salaries</td>
<td>59’123</td>
<td>HR management</td>
<td>SAP HR</td>
<td>ASP external</td>
<td>Standard</td>
<td>External</td>
<td>Centralised</td>
</tr>
</tbody>
</table>

Inventory of the main interfaces

Interfaces from and to a financially relevant IT application must be considered to be sources of risk. It is important to identify and review them.
Overview

Content and objective
In this step, we identify the “control universe”, which will subsequently be evaluated and tested. This involves establishing what key controls can be used to mitigate each relevant risk (damage scenarios), i.e., how key controls reduce the potential impact and/or the probability of its occurrence. Moreover, the impact on the assertions in the financial statements is also analysed (e.g., completeness, validity, evaluation, on period matching or representation in the annual accounts).

Background
Given the complexity of the processes and IT applications, it is important to concentrate the audit work on material aspects. The identification of risks and the corresponding expected key controls constitutes the basis for an efficient audit.

The auditor then compares his/her expected key controls with the ones that were actually implemented and assesses the coverage of the risks.
**Procedure**

**Risks, control objectives and controls**

The auditor identifies risks that could lead to material errors in the financial statements within the main processes and the systems concerned. This gives an overview of the risks that are liable to prevent the achievement of the objectives of the process. This risk analysis will also enable the auditor to establish the scope of the audit procedures.

The control objectives are derived from the risks. A control objective can be defined as an assertion concerning the desired outcome that should be achieved by the implementation of the controls. The control objectives are therefore often the expression of “inverted” risks, in other words, their objective is to reduce a given risk.

Subsequently, the auditor establishes his/her expectations in terms of the typical and expected controls for the identified risks. These controls need to be subdivided into “key controls” and others. The key controls, either individually or in combination, are indispensable for an acceptable reduction of risks. They are therefore meant to ensure the reliability of the process results and the financial data. The key controls constitute the backbone of the control system and it is therefore essential that they be verified by the auditor. The other controls are less relevant to the auditor.

The key controls expected by the auditor are compared to the controls that are actually implemented and the coverage of risks is evaluated in relation to the actual key controls existing in the process concerned.

**Standard frameworks**

There are generic inventories of typical risks, control objectives and control practices for some processes and applications. The CoIT® framework is a well-known example of this in the area of IT processes. Another example for generic application controls can be seen in Annex 1. These aids can provide useful support in actual audits, but they are no substitute for the auditor’s professional judgement on the individual processes.

**Types of controls**

The following matters are relevant for the subsequent progress of the audit and must therefore be documented:

- Preventative controls versus detective controls: Does the key control prevent or detect an error?
- Automated controls versus manual controls: Is a control implemented manually or is it automated within an IT application?
Presentation of information

An appropriate way to present the information is a risk/control matrix showing, on the left-hand side, how identified risks are covered by controls:

<table>
<thead>
<tr>
<th>Risks</th>
<th>Controls</th>
<th>Action</th>
<th>Assertions</th>
<th>Effect</th>
<th>Control Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>What could go wrong?</td>
<td>What is controlled when, how and by whom?</td>
<td>Operative Control</td>
<td>Validity</td>
<td>Valuation</td>
<td>Periodicity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Control Design</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Is control capable of meeting criteria?</td>
</tr>
</tbody>
</table>

As an additional element, the central part of this risk/control matrix shows what assertions in the financial statements are addressed by each key control. In this way it is ensured that the requirements are covered by corresponding controls. Finally, the right-hand side of the risk/control matrix can be employed in the subsequent steps of the audit approach to document the assessment of the control design and its actual implementation.

Special considerations

Completeness of risks and controls

Just the identification of the transaction controls is not sufficient; risks and controls with regard to related parameters and master data must also be taken into consideration. Typical such controls are access controls and authorisations.

All the important controls related to the applications must be taken into consideration, i.e., all manual or automated controls that have a direct influence on the process result. The quality of the controls with an indirect influence (e.g., general IT controls) must be taken into consideration for the overall audit conclusion but are not discussed any further in this document.

Focus on key controls

If the auditor does not restrict his/her work to the key controls, this may lead to a too broad and therefore inefficient audit. Moreover, he/she should avoid compiling an excessively detailed description of the expected controls, because this would lead to extra effort without producing any relevant additional benefits.

---

5 The effectiveness of the controls is examined in the steps described in chapter 7
6 There are also various reference models concerning the assertions in the financial statements e.g., the 1998 Swiss Audit Manual.
Documentation of application controls

An appropriate documentation of the application controls is of fundamental importance for understanding the controls themselves and, in particular, for a subsequent assessment of their design. This documentation should allow the auditor to understand what business rules the control in question is meant to ensure. Moreover, it should be clear what design decisions were taken in regard to the implementation of the controls. Finally, it must be clear what parameters and customising were applied so that the control can function as the business rule prescribes.

The table below presents two examples:

<table>
<thead>
<tr>
<th>Description</th>
<th>3-Way Match</th>
<th>Segregation of Duties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Rule</td>
<td>No invoices paid if the order, delivery note and invoice do not agree within a tolerance of 10%</td>
<td>Segregation of duties between accounting staff responsible for accounts receivable and accounts payable. Nobody who pays invoices can conclude contracts with new suppliers.</td>
</tr>
<tr>
<td>Design</td>
<td>Reference to the 3-way-match functionality of the ERP</td>
<td>Separate roles for all accounting staff responsible for accounts payable and accounts receivable and master data maintenance. Documentation of a function segregation matrix.</td>
</tr>
</tbody>
</table>
5 Walkthroughs

Overview

Content and objective

Before undertaking a walkthrough, the overall process must be understood from start to finish. In a walkthrough, manual or automatic steps of the process/transaction class are run through and documented on the basis of a typical transaction. Walkthroughs serve to verify the auditor’s understanding of the process concerned, the relevant risks and controls and therefore they also serve as a confirmation of the analysis carried out beforehand.

The level of detail of a walkthrough depends on whether the auditor intends to rely on the existing control system or not.

- If the auditor intends to rely on the controls, he/she will analyse the individual controls in detail in terms of how they function and whether they actually cover the existing risks or not.
- If the auditor does not intend to rely on the effectiveness of the controls, he/she will carry out a less detailed walkthrough. This walkthrough should ensure that he/she understands all material (financial) risks that can emerge from the process. In this case, he/she will base his/her substantive testing on the identified risks.

Background

With walkthroughs, the following are systematically verified:

- understanding of flows and processing,
- the consistency and significance of existing documentation and flow charts,
- the accuracy and completeness of the information regarding the relevant controls and
- the existence of relevant controls in day-to-day routine processing.

Procedure

Transaction data

One transaction is selected per transaction class. Its handling is followed through the whole process, from the initiation of the transaction to its authorisation, recording, processing and finally its booking.

The process/transaction class must be followed through by means of real supporting documents and steps in the application. During the walkthrough, the existing controls are verified and the choice of key controls analysed.

During the walkthrough, staff must be asked about their understanding of existing job specifications and control guidelines, in particular with regard to exceptions in the process or error rectification.

The following questions must be taken into consideration during the walkthrough:

- Who should be asked for explanations of details, e.g., concerning the area of activity?
- Where do existing documents, reports, flowcharts, screenshots come from, and from whom?
- What control procedures are performed as part of the individual activities?
- Is the control implemented to prevent errors or to detect them?
- How is the control implemented (automated or manual) and what is the frequency of its occurrence?
- Is the automated control really implemented?
- What audit trail is available to document the execution of the control?
Presentation of information

The documentation of a walkthrough, where manual and automated steps are “performed” based on a typical example transaction, is normally carried out on the basis of descriptions, screenshots, supporting documents, flow diagrams etc.

Special considerations

In practice, during walkthroughs, the auditor will often additionally carry out his/her assessment of the control design and, in the case of automated controls, also perform his/her assessment of the implementation of the controls. These two steps, which logically follow on the walkthrough, are dealt with separately in the next two chapters.

Walkthroughs are often broken down into several parts. Therefore, interfaces between them often get forgotten when walking through parts of processes or IT applications.
6 Assessment of Control Design

Overview

<table>
<thead>
<tr>
<th>Content and objective</th>
<th>In the previous steps we identified significant risks and key controls and developed a basic understanding of the process, which was then verified by means of a walkthrough. At the same time, an initial examination of the adequacy of the controls was carried out. In the assessment of the design effectiveness described below, the internal control system is examined as a whole and with reference to all the significant business processes to see if it is adequate (coverage of risks, completeness, current relevance) and effective (redundancies, overlapping). The design of the controls, in particular their positioning in the business process, must be reviewed to determine whether: • the risks identified are completely covered, • the established control objectives can really be achieved, • the controls really enable a reduction of the risk of error or fraud, • the risks are covered in a manner that is effective, • or whether, on the other hand, a different control or combination of controls, in particular high-level company-wide controls, could lead to more efficiently achieving the same control objective. The objective of this step must be to achieve an adequate control coverage with the lowest possible number of controls. A detailed understanding of the control design is necessary to establish an adequate audit strategy for the assessment of the implementation of the controls.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background</td>
<td>A careful analysis of the design effectiveness should allow to: • identify gaps, overlapping or duplication in controls; • avoid the execution by user departments and the testing of their operational effectiveness by the auditor of unsuitable controls; • identify how the same or even better results could be achieved through the adaptation of other – e.g., already established – controls.</td>
</tr>
</tbody>
</table>

Procedure

Assessment of control design

The internal control system is assessed as effective when compliance with the controls provides a reasonable assurance that errors and fraud will not significantly impact financial reporting. Process-oriented audit activities are an appropriate means of obtaining audit evidence as to whether the control design prevents material errors or detects and helps correcting them. Only in the next step on "testing operating effectiveness" do we look at the question of whether the designed controls were effectively implemented over the entire audit period7.

7 AS 400 paragraph 27: “risk assessment and internal control”.
Audit procedures

Audit procedures for the assessment of control design include interviews, observations, walkthroughs, the examination of relevant documentation and the assessment of the adequacy of specific controls. The auditor will form an opinion with regard to the control design by:

- interviewing members of the management and employees with supervisory tasks;
- consulting supporting documents relating to transactions and other important documents of the company;
- inspecting the performance of specific activities and controls;
- following individual transactions through the information system (walkthrough).

In accordance with current audit standards, the audit procedures for the assessment of design effectiveness must be documented.

Questions to be asked concerning the assessment of control design

Significant shortcomings in control design can be discovered by discussing a number of typical questions with the audited department:

- Are the steps of the process and the related controls arranged in a logical and sensible order?
- Is the responsibility for the implementation of the controls clearly established?
- Is it possible to implement the controls in a correct and meaningful manner?
- Are manual or hybrid controls replaced by automatic controls wherever possible?
- Are upstream (preventative) controls used, wherever possible, instead of downstream (detective) controls?
- Do the controls comply with the requirements of guidelines and procedural instructions?
- Is the required input for the effective functioning of the control available?
- Does the implementation of the control provide for a control document that can be checked?
- Are the controls carried out by a suitable, qualified and trained member of staff?
- Are the controls carried out within an appropriate period and sufficiently often?
- Can the designed controls be implemented in view of organisational, staff or cost constraints?
- A portfolio approach can be applied to the assessment of the individual controls by assessing their degree of automation (manual, semiautomatic, automatic), impact (preventative, detective), control frequency and risk coverage.
- With regard to the level of automation, automatic controls are more efficient than manual controls, although they do involve a one-off implementation effort. Moreover, their effectiveness remains stable as long as no significant changes are made.
- It is commonly accepted that preventative controls are more effective in terms of achieving the control objectives than the downstream detection of errors by detective controls.
- Generally speaking, in the case of manual and semiautomatic (i.e., hybrid) controls, a higher control frequency is more expensive and time-consuming as compared with automatic controls, where control frequency has very little influence on running costs. A lower control frequency, on the other hand, can adversely affect the effectiveness of a manual or semiautomatic control.
- A control that covers a number of control objectives/risks is considered to be generally more effective, more reliable and cheaper than a control which is targeted at only one risk.

---

Technical questions for the assessment of control design

In his/her assessment of the design of application controls, the auditor will clarify in greater detail the technical requirements needed for the control to work as required. The auditor will ask him/herself, in particular, the following questions:

- Can the control be circumvented or overridden (e.g., by horizontal navigation, super user)?
- To what extent does the control depend on customising, that is to say the specific adaptation of the IT application to the company?
- To what extent does the control depend on the actual implementation of the access control system?
- What combination of authorisations would enable the control to be circumvented?
- What master data and parameters are relevant to ensure that the control functions as it should?
- Who verifies the master data?
- Can the functioning of the controls be recorded for later verification (logging)?

Special considerations

Optimisation potential

In order to ensure the efficiency of the control system, it is necessary to review the question of whether the established controls are actually necessary and whether they do not overlap with other process controls or entity level controls or are merely redundant. Considerable potential for savings combined with a more reliable assessment are offered by upstream (preventative) controls and by automatic controls.

In order to identify the improvement potential of a control design the auditor should make use, above all, of the knowledge and the experience related to the relevant business areas as well as the opinions of management and employees. In addition to the already known shortcomings, the analysis of entity level controls is, above all, an effective aid for the optimised use of the control design. Because of their pervasive effect over all processes, these entity level controls have the potential to support individual controls in the process, compensate their shortcomings or even replace them. Often, because of the time pressure involved in setting up internal control systems, the same control objectives are achieved both by redundant process controls and entity level controls. Entity level controls, however, need to be assessed as to their timeliness of identifying and acting upon risks. Further redundancies and overlaps might exist between controls in support and core processes and should therefore be identified.

Ineffective key controls

If the auditor, in his/her assessment of control design, identifies ineffective key controls, uncovered risk will result. In order to resolve this, the auditor must identify other key controls/compensating controls and evaluate their effectiveness. When doing this, the auditor will always consider the entire selection of key controls as a whole to avoid costly redundancies.

---

9 Entity level controls, like general IT controls, are controls with a company or group-wide effect; they are normally covered by the COSO enterprise risk management framework dimensions: control environment, risk assessment, information and communication system and monitoring. They involve enterprise-wide guidelines and procedural instructions with considerable effects on the regularity of business activities in relation to strategy, objectives or cultural aspects. Unlike process controls, entity level controls are pervasive and therefore have a broad effect. (Menzies 2006, p. 21).
Test effort

An adaptation of the selection of key controls to be tested is also indicated when the walkthrough or assessment of the control design shows that the amount of effort needed to test a key control is unacceptably high.
7 Testing Operating Effectiveness

Overview

| Content and objective | The purpose of tests of operating effectiveness (TOEs) is to obtain an audit opinion on the internal control system. TOEs entail evaluating whether each control operates as planned, whether it was actually and fully implemented and whether the person responsible for its implementation was appropriately qualified and authorised\textsuperscript{10}. |
| Context | TOEs are the only means whereby managers and auditors can obtain the necessary assurance that controls actually work, that risks have been covered and control objectives been met and that the controls were operational throughout the audit period concerned. The need for testing is determined by the audit strategy. |

Procedure

Steps

TOEs comprise the following steps:
- Selection of controls to be audited, if the control system as a whole is not subject to audit;
- Choice of audit strategy (compliance testing/substantive testing);
- Choice of test procedure and, in particular, sample size;
- Execution of compliance testing/substantive testing audit procedures;
- Assess control deficiencies and the criticality of errors and weaknesses.

Substantive testing to obtain audit evidence

The auditor obtains audit evidence for the assessment of controls by implementing substantive testing procedures. These break down into test of details (inspection of records or documents, observation, inquiry/corroboration, calculations and replications/repeat controls) and analytical audit procedures (e.g., data analysis\textsuperscript{11}). Generally speaking, observation and inspection only offer moderate audit assurance, and test of details is mainly used in the case of undocumented or poorly documented controls. However, the re-performance of individual controls delivers a high level of assurance. Manual controls are usually tested via a combination of inquiry, observation, inspection of control evidence and, if necessary, re-performance.

Audit strategies for IT application controls

- "Test-of-one": In principle, automated controls need only be tested once, after which, provided a stable IT environment and effective general IT controls during the audit period, they can be considered to be just as effective thereafter. When conducting a test of one, the auditor should verify whether the tested control works as expected in all possible applicable circumstances.
- Direct testing: The effective operation of the control is verified by means of sampling or the analysis of transaction data.

\textsuperscript{10} Grant Thornton 2007, p. 5.
\textsuperscript{11} Swiss Audit Standard 500 - "Audit evidence", paragraph 19 ff
• **Baselining/benchmarking**: The objective of this strategy is to reduce the extent of substantive testing in subsequent audit periods. To this end, the results of testing application controls are carried forward to subsequent audit periods. The tests conducted during the first audit period serve as a benchmark. Provided that no changes have been made to the IT application controls in subsequent periods and that the relevant general IT controls have been tested as effective, the IT application controls are deemed to be effective without further testing. Nonetheless, a new control benchmark must be set at regular intervals. This audit strategy can be used where, for example, an IT application control is clearly assigned to a specific software release or if any changes are clearly documented. In case of multiple system changes, due to increased interdependencies, or in case of non-effective IT general controls this approach should not be used.

• **Data analysis**: The effectiveness of a control is verified by means of computer-assisted data analysis, whereby, ideally, all the relevant data are taken into consideration.

**Testing controls vs “end-to-end” transaction testing**

Most auditors select controls from within the flow of transactions and evaluate and test their effectiveness as individual controls. However, this is not the usual approach to the design and implementation of IT applications, where the objective is to verify a given software functionality by setting up end-to-end test cases. These are designed for all relevant transactions and are run through “end-to-end” via the IT application. In such situations it should be possible to achieve considerable synergies by involving the auditor in the definition of the test cases, allowing him/her to contribute towards the design of tests, which, in addition to the business functionality, also implicitly cover the required key controls. This approach may in particular also provide the basis for a subsequent baselining approach.

**Regression testing**

Regression testing entails re-performance of all or parts of the test cases to identify potential impacts of changes on already tested components of an IT application. Such changes regularly arise, for example, following software maintenance, updates or corrections. Regression testing is suitable in the case of IT applications that are frequently subject to change or adaptation, particularly if it can be automated.

In conjunction with the approach, described above, of testing controls implicitly by means of end-to-end tests of transactions, regression testing can be used to test the correct functioning of application controls at little extra cost, even where IT applications are regularly updated.
Test procedure, sampling and sample size

Sampling is used when auditing the implementation of a large number of controls. A population can reasonably be sampled if it at least satisfies the relevant requirements of the PCAOB (such as Auditing Standard No 5) or the IT Governance Institute. The following table illustrates the use of sampling based on AS5:

<table>
<thead>
<tr>
<th>Control frequency or period</th>
<th>Minimum sample size error risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Annually</td>
<td>1</td>
</tr>
<tr>
<td>Quarterly (to end of period, i.e. +1)</td>
<td>1+1</td>
</tr>
<tr>
<td>Monthly</td>
<td>2</td>
</tr>
<tr>
<td>Weekly</td>
<td>5</td>
</tr>
<tr>
<td>Daily</td>
<td>15</td>
</tr>
<tr>
<td>More than once daily</td>
<td>25</td>
</tr>
</tbody>
</table>

Questions to be raised for the assessment of control implementation

The following factors may influence the audit procedure and the level of audit assurance:\(^{12}\):

- Control frequency – the less frequently a manual control is performed, the smaller the test sample;
- Control significance – the more importance the auditor attaches to an individual control when forming his/her audit opinion, the more thoroughly that control should be tested;
- Soundness of control evidence – smaller samples can be taken of controls that generate direct evidence of effectiveness (traceability, exhaustiveness, accuracy and time references) than of controls offering no direct evidence;
- Relative importance of errors and anomalies – the impact of these varies according to materiality and the complexity and number of processed transactions;
- Management override – the likelihood that managers will bypass or override a control;
- Frequency of changes to controls – a control’s effectiveness may be very significantly affected by changes to the control itself or to the control environment.

Evaluating anomalies in the testing of controls

An auditor encountering an unexpected result must determine whether it is an isolated, and therefore acceptable, statistical anomaly. With unexpected or recurrent anomalies, however, the cause must be examined. One way of assessing whether the number of anomalies lies within the bounds of acceptability is to increase the sample size. If the results of testing indicate that a control is ineffective, compensating controls should be devised. If no such controls can be found, or if they too prove ineffective, the entire audit approach must be revised.

\(^{12}\) Ernst&Young, Evaluating Internal Controls, p. 10.
Impact of company size

Swiss Audit Standard 400 ("Risk assessment and internal control") requires the auditor to obtain an identical degree of assurance irrespective of company size. However, the auditor may allow for the fact that certain internal controls are not practicable for smaller companies or organisational units. For example, insufficient separation of duties may be offset by stronger direct compensating controls of management, or the auditor may compensate for a lack of control documents or audit evidence by adapting the audit strategy to include additional substantive testing (adapted audit strategy). Audit Standard 400 also defines the limits of reliance on internal controls that must be considered in the audit opinion. The control risk is deemed to be high if the internal controls fail to prevent, reveal or correct a material misstatement in financial reporting.

Special considerations

Documentation of audit findings

The following information in particular should be included:

- Audit topic, auditor’s name and date;
- Which controls (including versions) and control objectives were audited;
- Test procedure (sampling, entire population);
- Test results, statement of the type, timing (periodicity) and scope of testing;
- Sufficient detail for an informed third party (e.g., another auditor) to be able to appraise the effectiveness of testing in terms of the assessment of audit risk;
- The auditor must also document the causes of deficiencies, the status of remediation actions and any further information of a qualitative nature;
- In the event of material deficiencies and control test results as well as the type and cause of each deficiency.
8 Overall Assessment and Conclusions

Overview

Content and objective
In the final step, the findings of each successive step in the audit are evaluated for their impact on the financial reporting and combined into an overall assessment. The auditor delivers a final statement as to whether the internal control system is able to provide reasonable assurance that material errors are avoided in financial reporting.

There is also a global assessment of:
- the extent to which the audited application makes an effective contribution to the business process (control design and implementation);
- whether there are significant control weaknesses in the application;
- the impact of control weaknesses on the application’s effectiveness, the overall system and the corresponding assertions in the accounts;
- whether the business process has any compensatory controls to offset the impact of control weaknesses in the application, and whether there is a need for further testing of controls and additional substantive testing procedures.

Context
Where control weaknesses in the application are such as to materially compromise the accuracy of the assertions in the annual accounts, and where this risk is not offset by compensatory controls (e.g., detective controls performed manually), the impact of those weaknesses on the year-end financial reporting must be evaluated. This assessment is performed from three angles:
1. Does the control weakness have an impact on the financial statements?
2. Do they constitute violations of legal or statutory requirements?
3. Does the weakness affect the audit opinion? When evaluating the impact on the audit opinion, the auditor considers whether substantive audit procedures should be used to assess the potential impact of ineffective controls.

Indicators of ineffective application controls may include the overriding or disabling of controls, the inappropriate use of IT-generated data, incorrect master data and parameters, ineffective IT general controls, missing control evidence and an overemphasis on just detective or just preventive controls.

Procedure

Conclusions

The findings of all the preceding audit steps are compiled. Missing or poorly designed controls and controls that were not effective throughout the whole audit period must be assessed for their impact on the financial reporting. The link between the (IT) application and the financial reporting is expressed in the assertions in the annual statement of accounts, which state objectives for each item in the accounts, and are assessed as to the level of probability that control weaknesses could have a negative impact on the achievement of those objectives.

Notwithstanding the availability and deployment of aids (frameworks, checklists, etc), the degree to which the conclusions reflect company-specific, process-specific and risk-specific requirements depends on the auditor’s professional judgement. Therefore, this necessitates an intensive discussion with the entire audit team, to the introduction of any further audit procedures must be fully discussed by the audit team.
Presentation of information

The auditor also uses the overall assessment to prepare a management summary of the risk situation in the audited processes and IT applications.

Special considerations

Shortcomings found in key controls for which there are no compensatory controls should ipso facto be judged more critically than weaknesses in the other controls.
Annex 1 – Application Controls

Companies must take the necessary measures to ensure the security and conformity of (IT) applications – and thus of business processes. Each business process, part-process or activity must therefore be run in a manner that enables the stated business objectives to be achieved. In this context, “controls” means “all concepts, procedures, practices and organizational structures that deliver reasonable assurance concerning the achievement of business objectives and the prevention or detection and correction of undesirable events”.

Within each (IT) application, and therefore each targeted business process, there are controls designed to ensure that the specified objectives are achieved. These are known as application-specific or application controls. They include, for example, controls of completeness, accuracy, validity and the separation of duties. Another category of controls, which are not application-specific, consists of general IT controls. These are used in areas such as systems development and update, security and exploitation and are not dealt with further here.

Different types of applications naturally require correspondingly different controls, as each type of business activity has different inherent business risks that may prevent objectives from being achieved.

Key requirements of application controls

The purpose of application controls is to ensure that transactions have been processed correctly and securely and to confirm the accuracy of results. To this extent they make an essential contribution to the corporate objectives of asset protection, accurate and reliable accounting and the observance of corporate policy.

A company will use application controls to ensure that the capture, system input and subsequent processing, storage and output of all significant transactions in its applications have been exhaustively, correctly, validly and verifiably performed. Application controls are therefore geared, above, all to the capture, input, processing and output of transactions and databases. They apply throughout the entire business process.

Types of application controls

Five types of application controls are distinguished here:
1 Data creation and authorisation
2 Data capture and input
3 Data processing
4 Data output
5 System boundaries/interfaces
1 Data creation and authorisation

Key principles of creation and authorisation:

• Errors and omissions are reduced to the minimum.
• Errors and irregularities are identified, documented and reported as soon as possible and corrected without delay.
• Corrections are checked by an independent agency/person.
• Transactions are executed only by authorised persons and/or by means of approved procedures.
• The originators of transactions are identified.
• Original documents approved for release are complete and accurate and are forwarded without delay.
• Original documents are held as long as statutorily required and in the prescribed form or can be reconstructed internally.

Typical creation and authorisation controls are as follows:

• Rules establishing who has the authority to produce original documents (e.g., signing rules) and their implementation via authorization checks by access protection systems;
• Separation of duties for the production and approval of original documents;
• Stamp or signature on original documents;
• Clear and user-friendly data input forms (e.g., with pre-completed areas);
• Processes for the early identification and resolution of errors and irregularities;
• Systematic filing of original documents (e.g., by date stamp or consecutive numbering);
• Microfiching or digitalisation of original documents and storage in such a form that the original information can be reproduced for as long as statutorily required.

2 Data capture and input

Key principles of data capture and input:

• Data may only be input by authorised persons or by means of approved procedures.
• The accuracy, completeness and validity of key data (e.g., account numbers, amounts and item codes) are checked as early as possible.
• Data capture/input errors and irregularities are identified, documented, reported and corrected in good time.
• Error corrections are checked by an independent agency/person.

Typical data capture and input controls are as follows:

• Rules establishing who has the authority to capture/input transactions and their implementation via authorization checks by access protection systems;
• Clear and user-friendly input masks with built-in format checks (e.g., date fields, numerical data only, compulsory fields and predefined recurrent data);
• Advanced automatic verification of input values (e.g., exceeding upper/lower limits, content plausibility check, reconciliation with stored data);
• Full text shown when the corresponding code is entered (e.g., entry of an article number gives the article description);
• Comparison of individual items: i.e., one-to-one comparison between input data on-screen or via listings with the original documents (a laborious approach that is only appropriate in the case of particularly important transactions such as master data amendments);
• Batch controls: number of receipts, total for the items shown on the receipts or numerical totals (amounts, quantities), hash totals (mathematical addition of receipt numbers or account numbers);
• Numbering checks of the documents in a consecutively numbered batch to reveal any missing numbers or documents input twice;
• Reconciliation of data with stored values (e.g., open items with new accounting entries);
• Key verification: where important values are input twice by separate persons (enforced by the access control system) or, conceivably, by one and the same person (e.g., undisclosed change of a password);
• Critical review (visual check), usually by a second person. This approach is suitable for critical cases and where there are only few transactions;
• Processes for the early identification and resolution of errors and irregularities – amended transactions should be checked again in full.

3 Data processing

Key principles of data processing:
• The completeness, accuracy and validity of data processes are routinely verified so that processing errors can be identified, documented and reported as early as possible and corrected in good time.
• Inaccurate transaction details are corrected without unnecessarily hindering the processing of other transactions.
• The programme correctly performs calculation, consolidation, analysis and classification operations.
• The separation of functions is also applied to data processing.
• Transactions generated automatically by the application (e.g., the periodic crediting of interest, orders triggered by stock shortfalls) are checked for completeness, accuracy and validity in the same way as one-off transactions.
• Important decisions based on automatically-generated calculations are taken or verified by human interaction.

Typical subjects of data processing controls:
• Many of the data capture and input controls described above can also be applied to data processing (e.g., the direct comparison of individual items, batch controls, consecutive-number checks and data reconciliation, automatic reconciliation of the general ledger with sub ledgers). It is important that the documents and totals used for these controls are the ones obtained after processing;
• External corroboration of internally-processed data (e.g., inventories, confirmations of current and deposit account holdings);
• Processing integrity is ensured by means of the four key process goals: atomicity (the indivisibility of activities, where either all component parts are successfully executed or none are), consistency (if the transaction does not reach a stable final state, it must be reinitialised in the system), isolation (the behaviour of a transaction is unaffected by other simultaneous transactions) and durability (the consequences of a completed transaction remain, even in the event of system failure). These controls are often implemented independently of any IT application (e.g., in database systems), and this aspect should be verified in each case.
4 Data output

Key principles of data output:
• Data are output on schedule, to the right beneficiaries and in accordance with the applicable procedures.
• The completeness and accuracy of output data are routinely verified by taking relevant control totals for comparison with the corresponding processing totals.
• Output data are handled, stored and destroyed in accordance with data protection and security requirements (both before and after they are circulated to users).
• Data printouts are stored in accordance with the applicable rules.

Typical data output controls are:
• Controls govern the sending and receipt of data (to whom which evaluations can be sent, when and how many copies);
• Access control systems ensure that user authorisations are verified in the event of computerized searches or online orders;
• Consecutive-number and completeness checks ensure that critical data for evaluations (e.g., checks, vouchers or bonds) are managed, delivered, returned, redeemed or destroyed (e.g., in the case of test runs) in accordance with guidelines;
• The accuracy and completeness of periodic outputs (e.g., the results of six-monthly and annual processing) are checked by sampling.

5 System boundaries/interfaces

Key principles of system boundaries:
• The authenticity and integrity of information received from outside the organisation are adequately tested before any potentially critical action is taken, whether the information was communicated by telephone, voice-mail, paper copy, fax or e-mail).
• Suitable measures are taken to protect sensitive information being transferred/transmitted outside the IT application from unauthorised access, modification or misdirection.

Typical subjects of controls at system boundaries:
• Many of the data capture and input controls described above can also be applied to interfaces at boundaries (e.g., the direct comparison of individual items, batch controls, consecutive-number checks and data reconciliation);
• All messages are authenticated by means of encrypted hash codes;
• All (important) messages are encrypted to safeguard:
  - data confidentiality,
  - data integrity,
  - the sender’s identity.

Remark: many controls at system boundaries mainly target the transport/transmission and electronic storage of data. In most cases these are not IT application controls and as such are not considered here.
Annex 2 – Glossary

Analytical audit procedures: see Audit procedures, analytical

Application Service Provider (ASP)
ASPs operate IT applications (e.g., ERP systems) that they offer to clients via a public or private network. The necessary software is not purchased but merely rented as required. The ASP takes charge of all administrative needs, such as data security, patches, etc. Unlike software hosting, the work of an ASP extends to the provisioning of related services (such as user administration).

Applications
Two kinds are distinguished here:
Standard IT applications: commonly used/marketed software that was developed for widespread corporate use and of which many copies are sold. Examples are sector-specific business software, multifunctional programmes used for office automation, workflow management or document management, and specialised IT applications such as ERP and CAD systems, distribution software, goods and inventory management software, accounting software and human resources management software. From the internal control point of view, the advantage of standard IT applications is that, since a great many developers and clients work on them, they generally demonstrate superior design, development, testing and documentation.

Dedicated IT applications are usually tailor-made for an undertaking or developed to meet a specific need (either internally or by external contractors). In contrast with standard IT applications, dedicated software is often affected by a range of problems (e.g., less qualified developers, software and hardware not up-to-date, incomplete solutions, inappropriate development input by the client, etc.).

Assertions (in financial statements)
Explicit or implicit assertions used by corporate management in financial statements. Assertions come under the following categories:
Existence: an asset or liability actually exists at the reference date;
Rights and obligations: the company actually has a given asset or liability at the reference date;
Event: a transaction or (other) event arose during the reporting period and is attributable to the undertaking;
Completeness: no asset, liability, transaction or other event has been omitted and all items have been disclosed;
Valuation: an asset/liability is entered on the balance sheet for an appropriate amount;
Entry and period matching: the value of a transaction or (other) event is correctly entered and it is assigned to the correct period;
Presentation and publication: items are published, categorised and worded in accordance with the applicable accounting standards.

Audit evidence
Information used by the auditor to reach conclusions that justify his/her audit opinion. This includes the documents and accounting entries underlying the financial statements, as well as corroborative data from other sources.

Audit procedures, analytical
Procedures designed to obtain audit evidence (often IT tool-supported data analysis). Used in the analysis of key numerical data and trends, including the verification of changes and entries that deviate from other relevant information or from forecast values.
Audit procedures, procedure-oriented; i.e. controls and compliance testing
Procedures used to obtain audit evidence that the accounting system and internal controls are appropriately designed and effective.

Audit procedures, result-oriented; i.e. substantive testing
Procedures used to obtain audit evidence of material financial misstatements. A distinction is made between discrete testing and analytical audit procedures.

Baselining/benchmarking for (IT) application controls
An audit strategy according to which the results of testing IT application controls are carried forward to subsequent audit periods: the baseline audit period is that during which IT application controls are first tested. Provided that it can be shown that the IT application controls are unchanged in subsequent periods and that the relevant general IT controls have withstood testing, the IT application controls are deemed to be effective without further testing. The aim of this strategy is therefore to reduce the extent of substantive testing in subsequent audit periods.

Benchmarking: see Baselining

Business rules
A technical term for the rules that typically have to be considered when giving specifications for an IT application and during development, testing and delivery, since as key control requirements they may have a significant impact on ICS design.

Control environment
Corporate management's general attitude towards, awareness of and treatment of internal controls and their significance for the undertaking. Influences the effectiveness of individual internal controls.

Control objective
A statement of the desired result (aim) that is to be obtained by implementing controls/control procedures in a given area of activity.

Controls
Controls are concepts, procedures, practices and organisational structures that deliver reasonable assurance concerning the achievement of business objectives and the prevention or detection and correction of undesirable events.

Types of control include:

Compensatory controls
Internal controls that reduce the risk that an existing or potential control weakness will result in error or omission.

General IT controls
General IT controls are the basis for the correct functioning of automated IT application controls. They address risks in the area of access rights, data quality and security and system changes (hardware and software) and maintenance.

IT application controls
IT application controls cover automated controls (e.g., edit check, limit check) as well as IT-dependent manual controls (e.g., reconciliation report, error report)
Hybrid controls
A combination of manual and automatic controls

Corporate management
The persons responsible for the supervision, senior management and governance of an undertaking (e.g., the Board of Directors of a PLC). This term is used where no clear distinction is made between, on the one hand, those responsible for direction and control and, on the other hand, executive management.

Data
Two kinds are distinguished here:

Master data: “static”, generally less time-specific data used for identification, classification and description, often by more than one application. Master data are therefore data (such as parameters and client and product data) that remain unchanged over a long period of time.

Variable/transaction data: development oriented data characterised by a certain variability that are generally time related (e.g., have a validity end date). These data are continuously being created as a result of the company’s operational processes and are typically used by just one or a small number of IT applications.

Remark: The classification of information as master or transaction data is not always obvious and is context-contingent. Master data in one IT application or database (e.g., data on inventory items) may be classed as transaction data in another application (e.g., product data in a database used to draw up a corporate product brochure).

Management and supervision
Functions of the persons responsible for supervision, senior management and governance in a company (e.g., the Board of Directors of a PLC). Executive managers are not part of this group unless they exercise these functions.

ERP
Enterprise resource planning. The purpose of ERP systems is to bring all business processes together, at all stages, in a centralised system. ERP software is typically used in finance and accounting, materials management, production, sales and marketing, etc., as well as in the management of the corresponding master data. As companies place very varied demands on their ERP systems, despite standardisation, these systems are often extremely heterogeneous.

General principles of audit and related services
Principles governing the correct exercise of the profession of auditor:
• Independence (when engaged on audit or review);
• Integrity;
• Objectivity;
• Professional competence and diligence;
• Discretion;
• Professional conduct;
• Compliance with legal rules and requirements.
Interface
A part of a system that is used for communication, i.e., the exchange of information between separate components and sub-systems. Interfaces are subject to a number of rules.

In the case of data interfaces, data files or sets are exchanged.

Software interfaces are logical contact points in an IT system. They determine how commands and data are exchanged between different processes and components (e.g., access to system routines, other processes, other software components, etc.).

Internal control system
Narrow definition (see Swiss Audit Standard 890 - “Risk assessment and internal control”):
In the new Audit Standard, the ICS applies only to control objectives associated with proper accounting and financial reporting. In practice, an ICS is generally understood to be composed of “control components”: the control environment, the company risk assessment process, information and communication system for facts relevant to accounting, control activities and monitoring. Particularly in smaller environments the control components frequently vary or can be combined.

Broad definition: the body of principles and procedures that corporate management establishes for the purpose of ensuring the regularity and effectiveness of operations (including compliance with those management principles), the security of assets, the prevention and disclosure of illegal acts and errors, the accuracy and completeness of entries in the accounts and the timely preparation, where practicable, of reliable financial information.

Management report
An annual report containing the audited financial statements and the auditor’s report (as well as other information, where appropriate). Legally, the external auditor’s report on the consolidated accounts is not part of the management report.

Materiality
Information is material if its omission or misstatement could influence the economic decisions of users taken on the basis of the financial statements. Materiality depends on the size of the item or error judged in the particular circumstances of its omission or misstatement. Thus, materiality provides a threshold or cut-off point rather than being a primary qualitative characteristic which information must have if it is to be useful.

Parameter
In IT, a parameter is an argument introduced into a programme or sub programme (i.e. an external control variable).

Patch
A software or data fix supplied to the end user in order to, for example, bridge gaps in security or expand functionality. A patch is often a temporary measure pending a full solution. As a patch will often have been less rigorously tested than the programme itself, it may make the IT application susceptible to new weaknesses and security problems.

Regression testing
Repetition of a test previously conducted in full, e.g., following maintenance, an update or corrective action. Comparing the results of regression testing with those of the previous test facilitates the assessment of results.
Release
A complete published version of an IT application is known as a release. Generally, all changes from one release to the next are systematically registered through software configuration management, date-stamped and given a user reference. It is important to ensure that all users have the latest version and that the auditor, for example, is able to tell that a release change has taken place.

Review
The purpose of a review of the financial statements is to state whether the auditor encountered any elements compelling a conclusion that the statements did not comply, in all material respects, with the applicable rules for the presentation of the accounts. The auditor makes this assertion where the audit procedures do not supply all the evidence required for the audit. A similar aim underlies the review of financial or other information drawn up in accordance with appropriate criteria.

Rotation
Generally refers to the audit principle that not all key controls are to be tested every year, it being left to the auditor’s discretion to conduct minimum tests of key controls each year in a limited number of areas. Care must however be taken to include all key controls in a planning cycle, established by the auditor, that is appropriate to the risk situation (generally 3 years).

SaaS: see Software as a Service

SAS 70
Statement on Auditing Standards (SAS) No 70, Service Organizations, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). SAS No 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers’ auditors in a uniform reporting format. This enables them to demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

Software as a Service (SaaS)
A method of making software available on demand on the Internet. Similar to the use of an ASP, compared with which SaaS can be better integrated with other procedures/IT applications, thus offering better support for service-oriented architecture (SOA).

Traceability
The information processed in a system and the processes effected by the system can be checked and verified later on.

Walkthrough
A walkthrough involves going through (replicating) a process step by step so that the auditor can get to know and verify the process concerned. During this verification, the auditor follows paths through the process that are determined by the preconditions of the process and any choices made by users.