Journal of Financial Risk Management, 2025, 14(1), 18-36
https://www.scirp.org/journal/jfrm
ISSN Online: 2167-9541
ISSN Print: 2167-9533

Developing a Model for an Internal Control System for Usage in Financial Accounting and Controlling

Leander Fritze, Otto Jockel

Department of International Management, Logistics & Operations, International School of Management, Cologne, Germany
Email: leander.fritze.2020@student.ism.de, otto.jockel@ism.de

How to cite this paper: Fritze, L., & Jockel, O. (2025). Developing a Model for an Internal Control System for Usage in Financial Accounting and Controlling. *Journal of Financial Risk Management, 14,* 18-36.
https://doi.org/10.4236/jfrm.2025.141002

Received: December 6, 2024
Accepted: February 5, 2025
Published: February 8, 2025

Abstract

Purpose: The study aims to develop a working and usable model for an internal control system for processes within financial accounting and Control. A case study was conducted in which experts were reviewed and asked their opinions on how an internal control system should work and what it should contain. As a result, a new model is presented. Drawing on the COSO model from 2013, its levels were redefined and brought into a more process-focused context. By using this model, a company can implement an internal control system for all of its relevant finance processes. The findings are based on a case study within the chemical industry, and therefore, the usability of the model for other companies in other sectors is still to be verified. It can be used, though, as a guideline for setting up company-specific systems.

Keywords

Financial Report, Financial Controlling, Financial Risk Management

1. Introduction

In a constantly changing and unpredictable business environment, which is influenced by complex global economic interrelationships, the challenge for enterprises is to ensure the efficient and secure ongoing of their core processes. A central element in this is the control and supervision of these processes to be able to react quickly to changing circumstances. The implementation of an internal control system can therefore be a massive advantage. Many literary sources exist that explain the structure and use of an internal control system in practice, and consulting companies have already specialized in this field.

Especially in the finance sector, the existence of an internal control system is of

great importance to save companies from financial risks and preserve their competitiveness. The Finance department of a company serves almost every operational process as the last responsible authority and is therefore reliant on the dependability of the transmitted data and information.

Many companies still do not know how to implement an effective internal control system or are not willing to implement such a system. The system often has negative connotations because of its name. Who likes to be controlled? Who likes to deal with control and sees it as a useful and valuable tool? In addition, ICS is associated with a strongly audit-driven topic that primarily represents a regulatory requirement (Hübner, 2009). However, this way of thinking should be strongly discouraged, as these initial misjudgments, which are mainly caused by ignorance, are offset by the numerous advantages of an ICS. It helps companies to achieve their development and profitability targets and avoid a loss of resources. It supports the creation of reliable financial reporting and compliance with laws and regulations to avoid reputational damage and other consequences. To summarize, the ICS helps a company achieve its goals by identifying and avoiding unexpected hurdles and surprises along the way (Bungartz & Strobl, 2012). Therefore, in this study, a new model for an internal control system is created, which can be used for finance processes in general. A case study of a company running in the chemical industry is used for primary research.

The motivation and general objective of this study is to develop a working and usable model for an internal control system for financial accounting and Controlling. There are already several existing models and several definitions of what an ICS should be. The state of research has drastically increased over the years but especially the model designed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) is often used. The model was first published in 1992 and has been updated over the years. Looking at the published literature one can also see that especially the implementation of an ICS within the separate departments of a company (HR, Sales, etc.) has been discussed very extensively. Many best practices exist as well as checklists and defined requirements.

Another topic that is looked at closely in this study is the implementation of risk management. Going along with this is an appropriate monitoring strategy and a well-thought-out review protocol, which must also be established. Several pieces of literature on this subject can also be found. It can be stated that there is already a regulated DIN standard for risk management, which provides specifications for its structure (IDW, 2017). There are also numerous models, instruments, and procedures for the individual components of risk management that have already been defined, explained, and applied.

2. Literature Review

The importance and function of internal control systems have already been greatly discussed in various sources. In the following, the most important sources of each subarea of the research are presented.

An ICS can be used in various company sectors but is especially considered for financial security and performance and how it is important for its success.

It was investigated whether the internal control system and corporate governance principles affect financial performance. The study concluded that "the internal control system has a moderator effect on the financial success of corporate governance". This result indicates that the efficiency of the internal control system should be increased for the financial success of corporate governance in enterprises.

Furthermore, there exists a whole book about how to implement internal control systems within the financial sector of companies. It provides four steps to a successful ICS and explains basics as well as specific recommendations for actions (Hunziker, Renggli, & Fallegger, 2018).

Within an ICS, risk management is always a highly considered factor.

The general functions and steps of risk management are explained by Wilfried Hoffmann in his book about the risk management process. Within it, a general understanding of the basics of risk management is described (Hoffmann, 2017).

Stefan Hunziker gives a more detailed and step-by-step-oriented view. In his book "Risk Management in 10 Steps", he provides not only a solid basis for risk management implementation but also explains which factors define successful risk management (Hunziker & Meissner, 2016).

In contrast to the chemical sector, which this publication is focused on, it has already been investigated how risk management can be implemented in small and medium enterprises in the UK construction industry. It was found that it was extremely difficult to implement risk management due to a lack of management skills, and knowledge in the adoption of the right tools or techniques to identify and analyze the risks (Rostami, Sommerville, Wong, & Lee, 2015).

Certain rules and guidelines on how effective risk management should be designed are given by Robert Chapman. He supports these guidelines by giving mini-case study examples and thus brings his rules into practical use (Chapman, 2019).

Also, studies exist on how an ICS should be designed to be most effective.

The most commonly known ICS model comes from COSO and their cube model. It is often referred to when asking how an ICS should be built up. It has been described and reviewed by many authors and is seen as the standard of an ICS model (Annen, 2008).

Some consulting companies such as PwC or KPMG have designed several models of their own ICS, which can be implemented in several company branches.

KPMG, for example, introduced a highly detailed chart on how an ICS is defined, what is necessary regarding regulations, and how it can be designed (KPMG, 2021).

PwC did something similar and designed their chart, also using the COSO cube but focusing more on a periodical cycle of implementing an ICS (PwC, 2015).

In some cases, an ICS has already been implemented and its procedure has been

recorded in depth.

The city of Dortmund, for example, used an ICS approach for its processes and developed its system.

They divided the ICS into three steps with a planning phase before them.

Planning Phase:

Creation of a process landscape for each department. Show all relevant processes for each department and assign processes to sub-departments and teams.

1) ICS overall analysis

A short evaluation by management is performed for all relevant department processes and showcases all possible damages, risk control activities, and countermeasures.

2) Risk management in specialized departments

Listing all global risks and the results of the overall analysis. Prioritizing of an ICS creation for defined processes.

3) ICS specialized processes

Detailed ICS for defined processes with process documentation and risk analysis. Furthermore, it provides a detailed description and evaluation of new and existing countermeasures.

For the ICS within processes, they created a special concept consisting of 5 steps that are repeated constantly:

1. Process documentation
2. Process analysis
3. Process optimization
4. ICS "should be" concept
5. Evaluation of the ICS

(Dortmund, 2018)

An ICS for financial and controlling activities has also already been developed within a master thesis. The main focus was on internal control systems in the field of state-owned enterprises. The author then created his model for an ICS consisting of three independent layers. The innermost circle represents the three objective categories of the COSO framework: Operations, Reporting, and Compliance. The next layer of the model also reflects a part of the COSO framework, where its elements are incorporated. To implement an internal control system, the components of the COSO framework—Control Environment, Risk Assessment, Control Activities, Information and Communications, and Monitoring—must be taken into account. The outermost layer represents the Three Lines of Defense model (**Figure 1**). The three lines of defense complete the model (Prem & Stahile, 2017)

Looking at the presented literature, it becomes clear that regarding an ICS and risk management there is already a detailed collection of different sources. Also, the fact that alternative models other than COSO have been developed is a pleasant sight.

However, the need for an operationally designed ICS with a focus on financial controlling and accounting, capable of being implemented within large organizations is still something to be desired.

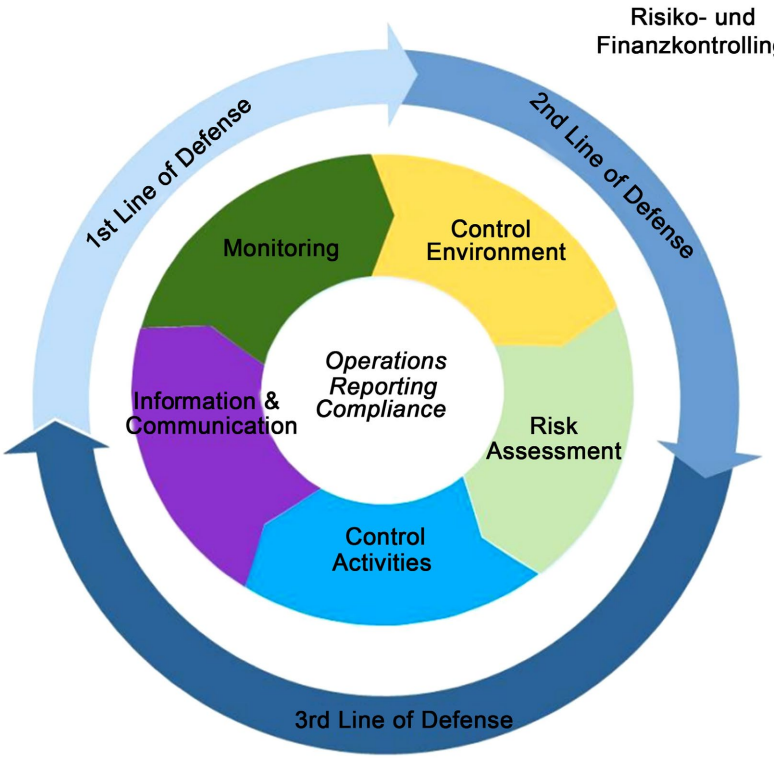

Figure 1. Three lines of defense model.

3. Theoretical Concept and Hypothesis Development

3.1. Internal Control System

An internal control system is a structured approach to ensure the efficiency and effectiveness of a company's operative processes, retain internal and external guidelines and regulations, and secure the company's assets. Usually, an internal control system is applied to an entire organization; however, in this study, the focus lies on applying an ICS to certain processes. Furthermore, one has to mention that often the term "risk management" is equated to an internal control system, but in this case, risk management is considered a central part of the control system and so it is defined and explained individually.

There is no real definition of an internal control system, but it is certainly a leading instrument in well-functioning corporate governance (Paschke, 2013). The Institute of German Business Auditors defined three major objectives of an ICS (IDW PS 261, 3.1.2.1.)

- The insurance of the efficiency and effectiveness of the operative tasks of a company as well as the protection of company assets (**operations**)
- The reliability and regularity of the financial reporting (**Financial Reporting**)
- The compliance with relevant guidelines and legislation (**Compliance**)

Special legal requirements apply especially to stock companies. These must comply with sections §91 (2) and §107 (3) of the German Stock Corporation Act. On the one hand, the Management Board must take suitable measures and, in particular, set up a monitoring system so that developments that could jeopardize the company can be recognized at an early stage. On the other hand, the Supervisory Board can appoint an Audit Committee, which is responsible for monitoring the accounting process, the effectiveness of the internal control system, the risk management system, and the internal audit system, as well as the audit of the financial statements.

A central model for the use of an internal control system within companies is the COSO model. COSO is short for "Committee of Sponsoring Organizations of the Treadway Commission". It was founded in 1985 in the USA and has the main objective of developing and promoting frameworks and guidelines for risk management and internal control (Olaniyi & Omubo, 2023). Researchers like Moeller (2014) emphasize its comprehensive approach, which integrates five key components: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities. These components are designed to provide a systematic approach to internal control, bridging financial reporting, operational processes, and compliance with legal standards. COSO defines the internal control system as a "process that is carried out by supervisory bodies, management, and employees and ensures with reasonable assurance that the specified objectives are achieved" (Tadesse et al., 2022).

The application of the COSO model and limitations hereto have been explored in different geographic, industry and business contexts. Jiang and Xie (2017), for instance, note that small and medium enterprises (SMEs) often struggle to adopt COSO due to limited resources and expertise. Vallabhaneni (2023) discusses the key components of the COSO framework, its impact on organizational success, and its role in maintaining compliance and achieving business goals in the context of cloud data. Chan et al. (2020) examine the impact of internal control and its five components on corporate innovation using the Committee of Sponsoring Organizations (COSO) framework with a sample of Chinese firms.

Nugraha (2023) examines the internal control system based on the COSO ERM within the Indonesian banking sector and finds deficiencies in implementation. This study aims to analyze how the management of PT JOY applies internal control, whether it is in accordance with the COSO ERM perspective.

The model this study is referring to is the so-called "COSO cube" (**Figure 2**). The model is three-dimensional and is divided into the following dimensions. The first dimension (x-dimension) consists of the three main targets of an internal control system, as mentioned earlier. The second dimension (z-dimension) defines the five core elements to which the ICS system is related. The third dimension (y-dimension) describes the entrepreneurial units the system is used in (Bungartz & Strobl, 2012). All those dimensions correlate with each other and one dimension cannot function on its own.

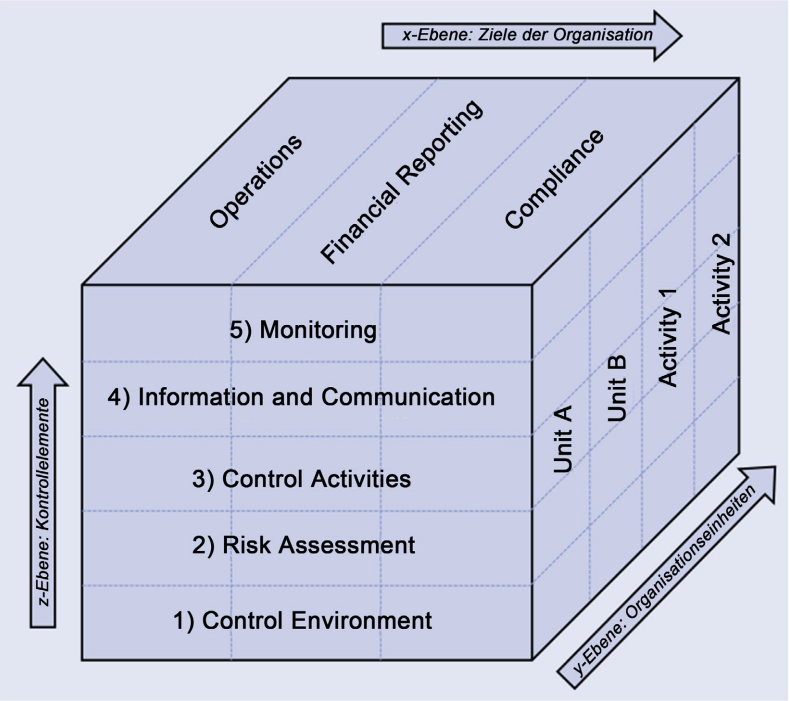

Figure 2. COSO model (2013).

The z-dimension given core elements can be defined as follows:

1) Control Environment

It describes the company culture, the style of leading by the management, established ethical values, and forms the basis for the ICS. It is the basis of the COSO system and assumes a basic part in molding an organization's culture of integrity, moral behavior, and responsibility. Laying out clear governance structures and elevating initiative obligation to moral qualities gives a strong base for successful inward controls. An advanced control environment strengthens risk management endeavors as well as improves administrative strength, adjusting execution to both internal values and external expectations (El Junusi, 2020; Vasilev et al., 2017).

2) Risk Assessment

This can be understood as the constant intake and evaluation of possible risks that might threaten the achievement of the previously defined targets for the ICS and, thus, a fundamental part of the COSO system, empowering organizations to recognize and address risks that might block their goals. Moreover, risk assessment upholds dependable reporting by determining financial risks and executing controls to prevent errors and fraud in financial reporting processes, in this manner advancing transparency and dependability (Chan et al., 2020).

3) Control Activities

Control activities are fundamental approaches and methodologies that assist organizations with mitigating risks and guaranteeing the accomplishment of their goals. These activities include preventive and criminal investigator systems like approval, compromises, and isolation of obligations, as well as all intended to shield resources, improve functional proficiency, and guarantee the reliability

of monetary announcements. They are critical for ensuring compliance with laws and regulatory requirements, as they embed internal controls within daily operations (Chan et al., 2020).

4) Information and Communication

An effective communication of relevant information includes the preparation and transmission of this information to the corresponding addressees. To be most effective, communication should be vertical and horizontal within the corporate structure. This component highlights the significance of dispersing precise and opportune information to employees and partners, empowering them to understand their jobs inside the internal control framework (El Junusi, 2020).

5) Monitoring

This includes the constant process of integrated auditing for the effectiveness of the implemented controls. This needs to take place to define the weak points of the ICS in an early stage. (Paschke, 2013)

Although it might seem that an internal control system is flawless, one has to be reminded that there are also some boundaries to this system (Bungartz & Strobl, 2012):

- Processes which are not a routine act are covered barely or not at all by the ICS
- The abuse or ignoring of the control responsibilities from employees
- The ineffectiveness of the ICS due to changing environmental- and business conditions
- Human failure, for example, due to carelessness, diversion, miscalculations, or misunderstandings of work instructions

Nevertheless, the positive aspects of an ICS are not to be forgotten and positive side effects also occur. On the one hand, from the results of process optimization and the identification of operational weaknesses within the processes and, on the other hand, from the achievement of increased risk awareness among employees, which in turn contributes to the detection and avoidance of sources of error in the company. (Bungartz & Strobl, 2012)

3.2. Risk Management

Risk management is a central component of an internal control system. It is the systematic analysis of, assessment, and control of company risks. (Brauweiler, 2018). Its main task is the early identification of critical situations within a company and to reduce or avoid them, but many other objectives are mentioned in the following (Brauweiler, 2018):

- The development of an early warning system for all the relevant risks
- The consequent and regular analysis, evaluation, and treatment of risks
- The improvement of external and internal audits
- Compliance with regulations
- The increase in transparency within the company

In Germany, the requirements for risk management are primarily characterized by the Corporate Control and Transparency Act (KonTraG), which came into

force in 1998. The following requirement in Section 91 (2) of the German Stock Corporation Act (AktG) is central to this: "The Management Board must take appropriate measures, in particular, to set up a monitoring system, so that developments that jeopardize the continued existence of the company are recognized at an early stage."

A known model for a risk management system is the DIN ISO 31000. It can be used as an instruction for action for effective and efficient risk management, regardless of the industry the company is active in. (ISO DIN 31000, 2009). The risk management process consists of several process steps, but the basic principles and core processes can be found in DIN ISO 310000 (**Figure 3**).

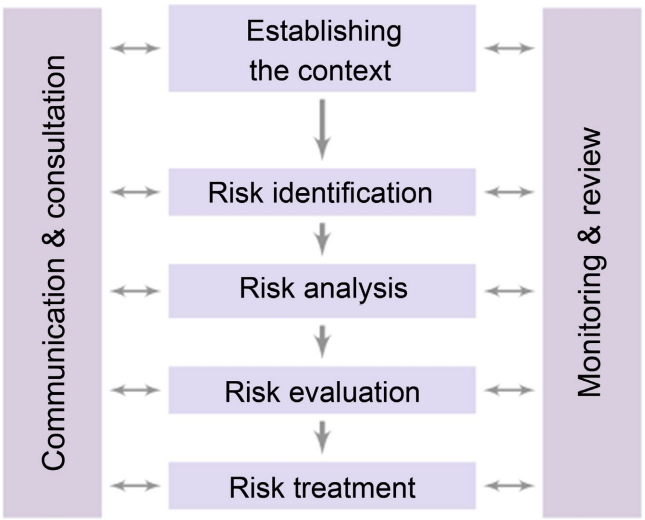

Figure 3. Risk management process as described in DIN ISO 31000 (Hoffmann, 2017).

The different process steps can be explained in more detail as follows:

Establishing the context

Before implementing risk management, certain principles need to be set. This also contains setting objectives that the risk management needs to fulfill and setting framework conditions within the organizational structure of the company. (Hoffmann, 2017)

Risk identification

To determine the treatment of risks, they need to be identified first. The trick is to recognize all current and future potential risks as early as possible. The risk identification process is, therefore, a continuous task, especially as companies are exposed to constant change and new framework conditions in today's world. Risk identification aims to provide a structured presentation of all existing and potential risks, including their effects, in a risk catalog. It is thus possible to present the overall risk profile of a company, project, or process. (Hoffmann, 2017)

Risk analysis

How risk is analyzed correctly is given in the DIN EN 62198. Risk analysis involves analyzing the causes and sources of risks, their positive and negative effects

on project objectives, and the likelihood of these effects occurring. Factors that influence the impact and probability should be determined. It therefore serves to determine the causes of the identified risks. This is not a point-in-time analysis, but rather a process-accompanying observation of all risk factors (Schmitz & Wehrheim, 2006).

Risk evaluation

Risk evaluation aims to visualize the potential danger posed by the identified risks. The effects of the risk position on the company must be identified and quantified. Therefore, the probabilities of occurrence, the potential amount of loss, and the frequency of loss occurrence must first be determined to determine the individual extent of risk. Determining the amount of loss depends on the company's objectives. The impending loss of assets should be identified. Attention should be paid not only to the direct losses when a risk materializes but also to the possible consequential losses (Fiege, 2006).

The results of a risk assessment are usually presented in a risk matrix (**Figure 4**), whereby the likelihood of occurrence and the impact of damage of a risk are made transparent in a coordinate system. The axis of the level of damage usually ranges from very low to very high, and the probability of occurrence ranges from rare to very frequent. This can then look as follows:

Impact

Likelihood	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Figure 4. Risk matrix.

The intersection of those two measurements divides the risk into several clusters, which define the total evaluation of the risk.

Risk treatment

Following the evaluation, the risks need to be treated according to their evaluated significance. This can be done by either active measures, which are cause-oriented, or passive measures, which are impact-oriented. Active measures mainly focus on the avoidance and reduction of the impact and likelihood of the risk, whereas passive measures accept the risk and try to compensate for the expected outcome. In total, there are four types of measures: **risk avoidance** and **risk**

reduction are seen as active measures and **risk transference** as well as **risk acceptance** are seen as passive measures. (Hoffmann, 2017)

Risk avoidance

This strategy focuses on not entering a risk at all and is done by finding other solutions or implementing suitable protective measures (Höcker, 2013). It provides the highest security of all alternative risk treatment measures (Diederichs, 2006).

Risk reduction

This measure usually takes place when a risk has already occurred. Then, it is necessary to reduce the future probability of risk and minimize the damage it causes (Sevda et al., 2022). This can be done by taking some of the following measures into account:

- Gather information
- Detailed research (Tests, Evaluations, etc.)
- Additional quality assurance measures
- Qualification measures for employees

Risk transference

In this strategy, the risk is transferred onto several people involved, mainly by making insurance (Diederichs, 2006).

Risk acceptance

By accepting the risk, the company takes the risk into account without taking any regulating or preventive measures. By doing so, a certain residual risk is taken which usually only contains negligible effects and a very unlikely probability. This measure is often taken when the measures for a risk treatment would outcost the damage of the risk. (Hoffmann, 2017)

In general, one has to consider that risks are not static elements but rather dynamic elements that have to be checked and measured constantly. Only by doing so, it is possible to measure the effectiveness of the measures taken and determine whether further steps are necessary to treat the risks.

Monitoring and review

The risks need to be checked and evaluated constantly. Furthermore, it is necessary to determine who is responsible for the monitoring and review process in general. The interaction of monitoring and review is the basis for further optimizing processes and delivers the basics for risk databases, checklists, and criteria for the assessment of implemented risk treatment measures. The review process needs to ask the following questions to ensure the effectiveness of the implemented treatment measures (Reichmann, 2001).

- Have the targets of the ICS been reached?
- Were the treatment measures appropriate enough?
- Were correction measures necessary?
- Did any losses occur?
- Was the effect desired?
- Have all risks been identified?

Communication and consultation

Only by using adequate communication and coordination between the responsible employees, the success of the ICS can be ensured. Therefore, an open and constructive communication culture must be established which comes along with a solution-oriented work atmosphere (Boutellier et al., 2007). Only by doing so adequate solutions for improved monitoring and decision-making can be implemented.

4. Research Methodology

The study uses secondary sources as well as primary sources. The secondary sources contain mainly the analysis of the wide variety of already existing literature as well as other already existing models. The majority of them were explained in section 3 of this study.

As a primary source, a case study was conducted. Experts working in finance were interviewed, and their opinions on how an internal control system should work and what it should contain were asked. The company these experts are working for is active in the chemical sector. The interviews should help to answer the following questions:

1) *What requirements does a newly created model of an ICS have to fulfill in order to be used in Financial Accounting and Controlling and to be effective in an operational working environment*?

2) *How does Risk management need to be designed to fit in with* those *requirements*?

Therefore, an interview questionnaire was created which concludes with questions regarding the structure of ICS itself and the design of effective risk management. With the answers to these questions, the different requirements of the ICS system have been defined.

To answer the first research question the following questions were asked:

- Which people or departments are responsible for the execution and monitoring of the ICS?
- How should the ICS and the risk management be documented and recorded?
- How should incidents be communicated?
- In which intervals should the ICS be reviewed?

To then answer the second research question, the experts were asked to answer the following:

- Which factors are relevant for the assessment of the identified risks?
- How do you choose the adequate control design?
- Which criteria do you need to observe and which questions must be asked to review the established controls for the risks?

5. Results and Discussions

The interviews gave some general information on what should be achieved by implementing an ICS. It became clear that, in general, it should improve the ongoing

relevant business processes, such as the purchase-to-pay process or the planning of investments. It should be a valuable tool to prevent violations against the existing regulations and policies within the company, but it should also provide better reporting with transparent, reliable numbers. This is advantageous when thinking about external audits. Furthermore, the ICS should also be a system that works complementary with already existing control systems within the company. Those were the general requirements of an ICS, as said by the experts beforehand without context to the interviews.

5.1. Model Design

From theory, the COSO model is known as a good example of implementing an ICS. In this study, this COSO model is taken as the basis, but its levels will be redefined and based on new components. Within these new levels, risk management is seen as its component, and the philosophy of this new model is that the ICS and risk management are seen as separate systems.

5.1.1. Framework and Structure

At first, the overall structure and framework conditions of the ICS need to be clarified. This includes setting relevant objectives. From theory and a general understanding of internal control systems mainly, three objectives are always set:

- The insurance of the efficiency and effectiveness of the operative tasks of a company as well as the protection of company assets (**operations**)
- The reliability and regularity of the financial reporting (**Financial Reporting**)
- The compliance with relevant guidelines and legislation (**Compliance**)

These objectives will also be used in this case and relevant to the new ICS model.

When interviewing the experts it became clear that it is not particularly necessary to create a new model and new control measures from scratch. Expert 3 explained, "We need to modernize what we already have and bring it into a new context". This is a valid point. Many companies already have existing control systems to monitor their actions and in some cases also functioning reporting tools. It would simply not be intelligent to not use them or consider them when creating an overall ICS. Therefore it should always be made sure to fall back on what is already existing.

A newly implemented system would not function without well-set responsibilities. The experts made it clear that they desire a "centralized responsibility for the system and its general supervision". However, they are aware that when it comes to the supervision and monitoring of the defined processes within the ICS, each department or process owner responsible for the defined processes should also be responsible for the effectiveness of the process. So, summarized, this means that there should be an overall responsibility for the management and supervision of the entire ICS, as well as a subordinate responsibility for the processes within the ICS.

Documenting the ICS is a central piece and necessary for its effectiveness. It

should be as transparent as possible and understandable for an independent third party. All interviewed experts showed great interest in transparency and public accessibility within the company. Furthermore, it was added that procedural instructions of the ICS and incident reports should be documented and published as well.

Another central piece for every ICS is the communication and the further processing of relevant information. The interviewed experts made it clear that the decision of who is being informed should be dependent on the seriousness of an incident. The use of an Incident Report is intended, and depending on the seriousness of the financial impact, it is decided which people will send the report.

Lastly, the ICS needs to be reviewed and checked by revising. The interviewed experts showed interest in a yearly control schedule in which the system itself is reviewed and checked to see if it is still in line with the company's guidelines and compliance requirements. However, it is necessary to look into the system regularly as well and adapt the frequency of the reviews based on anomalies and frequent incidents.

All these results regarding the overall framework and structure of the ICS form the first level of the model

1) Definition of relevant objectives
2) Falling back on already existing systems and controls
3) Documentation
4) Communication
5) Revision

Now that the Framework is set and defined, one could argue that risk management can be structured based on it. However, without relevant processes and defined objectives, risk management cannot be implemented. Therefore it is necessary to carry out a "process analysis".

5.1.2. Process Analysis

The experts made it clear that to carry out adequate risk management for the ICS, the most relevant processes need to be identified and analyzed.

When identifying the processes, the experts referred to the creation of a "process landscape" divided into three levels, with each level having a different degree of detail for the process.

This can be understood as follows:

In level 1, the company's main processes and the scope of the process landscape are shown. A good example of this could be the "Source to pay" process.

In level 2, these main processes are explained in further detail. For example, the previously defined "Source to pay" process could be split up into the processes "Source to contract" and "Purchase to pay".

In Level 3 a further subdivision takes place. For example, the "Purchase to pay" process would be divided into steps and subprocesses.

This meets the expert's request to do the process analysis very thoroughly to cover every detail of the process and so every possible risk that might occur.

After the process landscape is completed, a process diagram needs to be created. This is to divide every process into its single steps and to make it possible to transfer every process into a "risk-control-matrix" which is being used in the ICS´s risk management. As this forms the basis for the risk assessment, this step needs to also be done very carefully and thoroughly.

Lastly, the objectives of each identified process need to be defined. This can be KPIs as well as general objectives. This is necessary to implement the correct control measures within the risk management.

All components define the level as the following:

1) Generating a "process landscape"

2) Define relevant process steps (process diagram)

3) Identify objectives for each process

Once these steps are taken and every process is analyzed and divided into its steps, risk management can be designed.

5.1.3. Risk Management

Risk management can be described as the executing arm of the ICS which acts under the given structure of it. Concerning the already existing theory, it only seems logical to divide it into the following three components.

1) Risk Assessment

2) Risk Control

3) Revision

Risk Assessment

The first step always involves the identification of the relevant risks. In theory, there are many ways to identify risks with various tools, such as an environmental analysis or a company analysis. Furthermore, one can analyze the already existing control measures and, by using the "reverse engineering" approach, identify the related risk. The basis for the risk assessment is the process landscape, especially the process diagram for each process.

With the Risk Assessment comes the evaluation of the identified risks. This is done by using the already mentioned risk matrix, which categorizes the risks based on their probability of occurrence and their damage impact when occurring.

Risk Control

Risks can be controlled by using the known methods of risk treatment. In total, there are four types of measures: **risk avoidance** and **risk reduction**, **risk transference** as well and **risk acceptance**.

Furthermore, it became clear that the interviewed experts also tend to use another method of controlling risks. First, the risk is reduced by technical measures, such as using a release lock for payments within the company's ERP system. If a risk cannot be resolved by this, **organizational measures** are being taken. These include, for example, the separation of responsibilities and the existence of approval processes. Lastly, **personal measures** come into play. These can be, for example, the further training of employees to keep them updated on the latest

developments in their field of work. However, by using all these measures, such as the traditional ones, a certain residual risk needs to be calculated.

Revision

Risks are constantly changing and therefore it is necessary to keep the measures to control and reduce them updated. The experts spoke out in favor of a yearly revision of the entire control system. This includes not only the evaluation of the effectiveness of the system but also the review of the issued incident reports and the effectiveness of the introduced control measures.

The effectiveness of the system needs to be reviewed, as well as the efficiency of the identified processes. This is done by looking if the set objectives for each process were met, no matter if they are measurable or just generally formulated.

Another part of the revision is the previously briefly mentioned incident reports. Based on these reports, the necessary actions can be identified and brought forward in the processes.

5.2. Final Model Design

After consideration of all levels and their precise definition, the model can be depicted as presented in Figure 5.

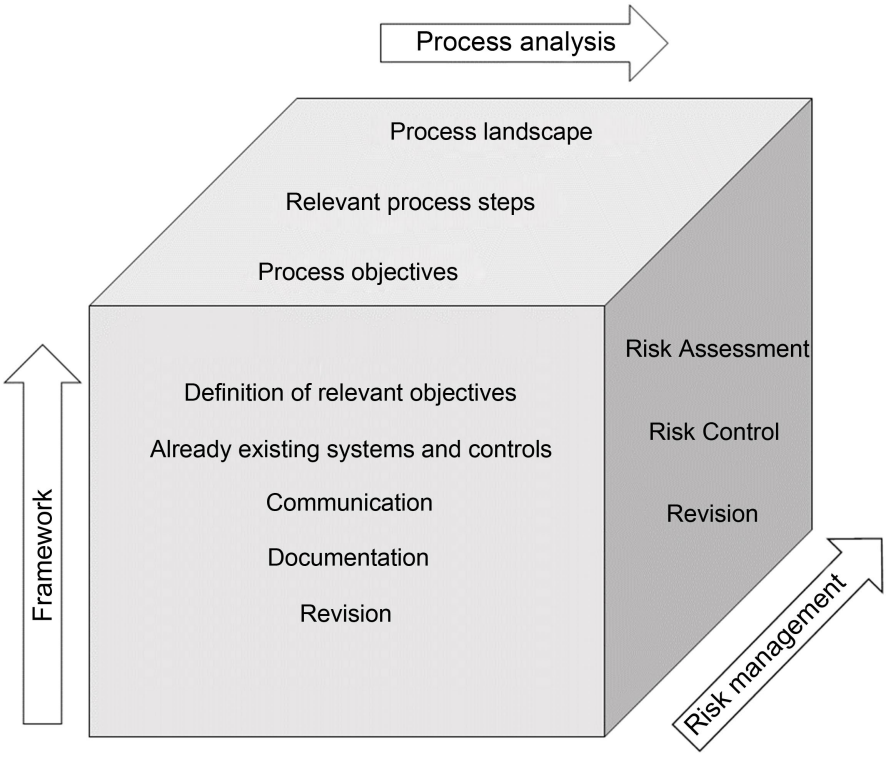

Figure 5. New ICS system based on COSO.

Notice that the model is based on the COSO model for an ICS system but as previously mentioned, the levels have been redefined. The configuration of the components at different levels can vary from industry to industry and from company to

company. Nevertheless, it provides a solid basis for implementing an ICS within any company and can be changed depending on specific needs.

5.3. Risk Control Matrix

It was mentioned that Risk Management is the executing arm of an ICS, but for it to function accordingly, it needs a tool. The central tool of risk management is the so-called **risk control matrix**. It illustrates everything that needs to be completed in dealing with process risks. The matrix has been put together in close collaboration with the experts to fulfill their standards and guarantee the best possible fit for the company.

The Matrix is individually put together for each identified process but follows a standardized procedure which is the same for each identified process.

First, the process diagram which has been created previously within the process analysis is used to be able to portray each risk for each process step. Then all other now following components are applied to each step:

1) Definition of the risk type—Financial, compliance, or other

2) Risk description—What exactly is the risk that can occur

3) Impact on the defined objectives for each process if the risk occurs—High, medium or low

4) Probability of occurrence—High, medium or low

5) Control design—Intersection of points 3 and 4—High, medium or low

6) Control description—Exact description of the measure to control the risk

7) Control method—Technical, organizational, or personal

8) Control object—Process

9) Responsibility—Who is responsible for the control of the process step

10) Frequency—How often is the process step controlled

11) Effectiveness—How effective are the control measures—High, medium, or low

12) Documentation—Is the control measure documented—Yes or no

6. Limitations and Future Research

The main limitation of this study is that it only covers a small base of the entire field of research and only one case study. Therefore, the results can only be transferred to the whole to a certain extent. An ICS system for another company could work similarly but also very differently than what was developed in this study. Therefore, it would be necessary to analyze more companies' case studies to verify the correctness of the ICS model and its components.

One central finding of this study is that the ICS model shown here uses a slightly different approach to the regular literature, mainly because of the newly defined levels and the differences between the commonly known COSO model. Nevertheless, it provides a new look at this field of research and could be the base for further research projects.

Another possibility would be to carry out a quantitative study based on this qualitative study to verify or falsify the ICS model.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Annen, M. (2008). *Internes Kontrollsystem und Risikobeurteilung*. TREX Léxpert Fiduciaire.

Boutellier, R., Gabriel, P., Barodte, B., & Montagne, E. (2007). Zeitsparendes Risikomanagement mit einem standardisierten Risiko-und Maßnahmenkatalog. *Projektmagazin, 1,* 1-8. https://www.projektmagazin.de

Brauweiler, H. C. (2018). *Risikomanagement in Unternehmen*. Springer.

Bungartz, O., & Strobl, G. (2012). *Mehrwert durch Interne Kontrollsysteme (IKS). Zeitschrift Interne Revision*. https://doi.org/10.37307/j.1868-7814.2012.03.06

Chan, K. C., Chen, Y., & Liu, B. (2020). The Linear and Non-Linear Effects of Internal Control and Its Five Components on Corporate Innovation: Evidence from Chinese Firms Using the COSO Framework. *European Accounting Review, 30,* 733-765. https://doi.org/10.1080/09638180.2020.1776626

Chapman, R. (2019). *The Rules of Project Risk Management*. Routledge.

Diederichs, C. J. (2006). *Immobilienmanagement im Lebenszyklus. Projektentwicklung, Projektmanagement, Facility Management, Immobilienbewertung*. Springer.

Dortmund, S. (2018). *Arbeitshilfe für den Aufbau von, Internen Kontrollsystemen (IKS) in der Stadt Dortmund*. https://rathaus.dortmund.de/dosys/gremrech.nsf/0/9A7ECCA99C495C62C1258297002B42C1/$FILE/Anlage_10722-18+Arbeitshilfe_IKS_Allgemein.pdf

El Junusi, R. (2020). Coso-Based Internal Control: Efforts Towards Good University Governance. *Journal of Islamic Accounting and Finance Research, 2,* 27-50. https://doi.org/10.21580/jiafr.2020.2.1.4773

Fiege, S. (2006). System des Risikomanagements. In *Risikomanagement und Überwachungssystem nach KonTraG*. Springer.

Höcker, T. (2013). *Risikomanagement als Teilleistung der Projektsteuerung in allen Projektphasen.* DVP-Tagung at 22.11.2013 in Munich.

Hoffmann. W. (2017). *Der Risikomanagement*. Springer.

Hübner, S. (2009). Internes Kontrollsystem (IKS). *Controlling, 21,* 276-278. https://doi.org/10.15358/0935-0381-2009-4-5-276

Hunziker, S., & Meissner, J. O. (2016). *Risikomanagement in 10 Schritten*. Springer.

Hunziker, S., Renggli, S., & Fallegger, M. (2018). *Interne Kontrollsysteme im Finanzbereich: Wirksame und effiziente Steuerung, Kontrolle und Überwachung*. Springer.

IDW Prüfungstandard (2017). *Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken*. https://shop.idw-verlag.de/Feststellung-und-Beurteilung-von-Fehlerrisiken-und-Reaktionen-des-Abschlusspruefers-auf-die-beurteilten-Fehlerrisiken-IDW-PS-261-n.F./20458

ISO DIN 31000 (2009). *Risk Management*. https://www.dgwz.de/din-iso-31000-risikomanagement

Jiang, L., & Xie, X. (2017). Factors Influencing the Implementation of Enterprise Risk Management: A Systematic Review. *Risk Management, 19,* 31-50.

KPMG (2021). *Mit Effizienz & Sicherheit—Unsere Ansätze für die Ausgestaltung des internen Kontrollsystems (IKS) im Financial Services-Umfeld*. https://assets.kpmg.com/content/dam/kpmg/de/pdf/Themen/2021/02/20210104-poster-iks-bf.pdf

Moeller, R. R. (2014). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes*. Wiley.

Nugraha, M. T. (2023). Analysis of Implementation of Internal Control Based on COSO ERM Perspective (Case Study of PT Joy). *International Journal of Scientific and Research Publications, 13,* 146-152. https://doi.org/10.29322/ijsrp.13.06.2023.p13821

Olaniyi, O. O., & Omubo, D. S. (2023). The Importance of COSO Framework Compliance in Information Technology Auditing and Enterprise Resource Management. *International Journal of Innovative Research & Development, 12,* 1-6.

Paschke, K. (2013). *Internes Kontrollsystem—Umsetzung, Dokumentation und Prüfung*. BoD—Books on Demand.

Prem, J., & Stahlie, C. (2017). *Internal Control Systems and Risk Management in the Field of Financial and Risk Controlling of Autonomous State Enterprises*. Master Thesis, University of Applied Scince. https://pub.fh-campuswien.ac.at/obvfcwhsacc/content/titleinfo/2063704?lang=en

PwC (2015). *Dynamische Ausgestaltung des internen Kontrollsystems*. https://www.pwc.de/de/finanzdienstleistungen/banken/dynamische-ausgestaltung-des-internen-kontrollsystem-2015.pdf

Reichmann, T. (2001). *Controlling mit Kennzahlen und Managementberichten. Grundlagen einer systemgestützten Controlling-Konzeption*. Vahlen.

Root, S. J. (2000). *Beyond COSO: Internal Control to Enhance Corporate Governance*. Wiley.

Rostami, A., Sommerville, J., Wong, I. L., & Lee, C. (2015). Risk Management Implementation in Small and Medium Enterprises in the UK Construction Industry. *Engineering, Construction, and Architectural Management, 22,* 91-107.

Schmitz, T., & Wehrheim, M. (2006). *Risikomanagement: Grundlagen, Theorie, Praxis*. Kohlhammer Verlag.

Sevda, K., Fikret, C., Engin, D., & Karakaya, A. (2022). The Moderator Effect of the Internal Control System on the Financial Success of Corporate Governance. *Uluslararasi Ekonomi ve Yenilik Dergisi, 8,* 311-335.

Tadesse, A. F., Rosa, R. C., & Parker, R. J. (2022). The Adoption and Consequences of COSO 2013. *Accounting Horizons, 36,* 241-260. https://doi.org/10.2308/horizons-18-123

Vallabhaneni, R. (2023). Enhancing Internal Controls with the COSO Framework: Addressing Deficiencies and Ensuring Regulatory Compliance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4944856

Vasilev, V. L., Bakhvalov, S. I., Prikhod'ko, A. N., & Kazakov, A. V. (2017). Internal Control in the System of Innovation Management in the Modern Business Environment. *International Journal of Economic Research, 14,* Article 409. https://core.ac.uk/download/pdf/197459849.pdf