UHASSELT

Faculteit Bedrijfseconomische Wetenschappen

master handelsingenieur in de beleidsinformatica

Masterthesis

Discovering risk factors auditors take into account when assessing business processes

Kobe Broux
Scriptie ingediend tot het behalen van de graad van master handelsingenieur in de beleidsinformatica

PROMOTOR :
Prof. dr. Mieke JANS

BEGELEIDER :
Mevrouw Manal LAGHMOUCH

UHASSELT

**2022
2023**

Faculteit Bedrijfseconomische Wetenschappen

master handelsingenieur in de beleidsinformatica

Masterthesis

Discovering risk factors auditors take into account when assessing business processes

Kobe Broux

Scriptie ingediend tot het behalen van de graad van master handelsingenieur in de beleidsinformatica

PROMOTOR :
Prof. dr. Mieke JANS

BEGELEIDER :
Mevrouw Manal LAGHMOUCH

Risk factors auditors take into account when assessing business processes

Kobe Broux

ABSTRACT

This study aimed to evaluate the effectiveness of process mining in mitigating risk factors that auditors consider when assessing business processes. By investigating the relationship between process mining and risk factors, the objective was to uncover the potential of process mining as a valuable tool for managing risks in business operations. Process mining is a data-driven technique that leverages event logs recorded by an information system to extract valuable insights. It empowers auditors to visualise the actual flow of processes, identifies deviations from expected patterns and evaluates the efficacy of internal controls. Through a comprehensive approach involving literature review and interviews, this study identified the most prevalent risk factors that impact business processes. Subsequently, process mining was employed to address these risk factors by analysing event logs and identifying deviations from the standard process or potential control failures. The findings of this study highlight the significant role of process mining in enhancing risk management practices and ensuring the integrity and efficiency of business processes.

Keywords: process mining, risk factors, business processes, internal controls

1 INTRODUCTION

The use of data analytics is not a new concept and has been in use for over two decades. However, until 2015, data analytics were only used for basic queries due to limitations in technology. With technological advancements in 2015, a new generation of data analytics tools was developed, making it easier to extract, filter, analyse and present data. These developments have brought data analytics closer to the auditing profession. This is why data analytics is increasingly being used in the field of auditing. With these new tools, auditors were able to take a closer look at transactions, rather than just at the whole ledger or sub-administration [22]. Auditors can gain a more comprehensive understanding of their client's operations, especially when dealing with large volumes of data, through the use of data analytics [21]. By utilising data analytics, auditors can extract relevant information out of huge chunks of data [49] and distinguish financial data from non-financial data. Data analytics have proven helpful in identifying risks and risk factors through the analysis of unusual patterns and trends. Additionally, regulatory bodies highly recommend the use of data analytics as a robust tool to detect and prevent fraud incidents, with the PCAOB encouraging auditing firms to incorporate it into their auditing process [43].

The process of data analytics involves examining, cleaning, transforming and modelling business data to discover and communicate valuable insights and patterns. These insights can be used to suggest conclusions and support decision-making in the auditing process [19]. In an audit, data analytics can be used to identify patterns, trends and anomalies in the financial data that may indicate a risk of material misstatement [12]. Data analytics can also uncover errors or fraudulent activities that may have not been identified when using manual and IT-based audit procedures [30]. Additionally, data analytics can be used to evaluate internal controls [23] and assess the efficiency and effectiveness of business processes [31]. Using data analytics in auditing allows for continuous monitoring of the organisation's financial data. This means that auditors can track changes in financial data over time, providing a more comprehensive view of the organisation's financial health [30]. Effectively, the use of data analytics in auditing can lead to a more efficient and effective audit, minimising audit risk and having a better understanding of the client's business environment and internal controls [19]. While data analytics can be a valuable tool for

identifying and evaluating risks, it should not be considered a replacement for traditional audit techniques. Rather, data analytics should be used in conjunction with traditional audit methods to provide a more comprehensive and accurate assessment of an organisation's financial health [31]. Additionally, it is important for auditors to critically analyse and evaluate the patterns and trends identified through data analytics, as they may not always indicate a material misstatement or control weakness. Therefore, the use of data analytics in auditing should be seen as an enhancement to traditional audit techniques, rather than a replacement [12]. One specific application of data analytics is process mining. Process mining is a technique that uses event logs, such as data from an organisation's IT system, to map and analyse business processes. This allows auditors to understand how an organisation's processes are actually being carried out in comparison with the way they are meant to function as designed [31]. Process mining is a distinct approach in auditing as it concentrates on the flow of transactions, rather than solely validating their values and it utilises the entire data set, rather than just a sample of the data. This approach will assist the auditor in identifying areas of inefficiency or control weakness and provide opportunities for improvement [30].

The goal of an audit is to evaluate the financial statements of an organisation and provide an opinion on whether they present a true and fair view of the organisation's financial position and performance [43]. Auditors perform a risk assessment to identify potential risks that could lead to material misstatements in the financial statements. They not only aim to detect these misstatements but also to identify the underlying risk factors that led to them [37]. Knowing these risk factors is crucial for planning and executing the audit. Auditors then evaluate the effectiveness of internal controls in managing these risks and preventing material misstatements [26]. These risk factors are related to the assessment of financial statements and not necessarily when assessing business processes. This paper aims to identify the risk factors that auditors consider when assessing business processes. Once these factors have been identified, the study will examine how process mining addresses these factors and possibly others as well. With this in mind, the following research questions are formulated:

- What are the most common risk factors that auditors take into account when assessing business processes?

- How does a process mining analysis address these risk factors?

- Are there any additional risk factors that a process mining analysis addresses?

This study investigates the most common risk factors that auditors take into account when assessing business processes and how process mining addresses these risk factors. Additionally, the study will examine whether there are any additional risk factors that process mining addresses. The findings of this study provides valuable insights into the use of process mining in the field of auditing and its potential to improve the efficiency and effectiveness of the audit process. The study is valuable for auditors as it presents a comprehensive list of common risk factors that should be considered while assessing business processes. Being aware of these risk factors will enable auditors to quickly identify their presence and determine how a process mining analysis can address them. This will ultimately enhance the efficiency and effectiveness of the audit process.

The paper is organised as follows: Section 2 provides background information and a review of the relevant literature. In Section 3, I explain the research methodology and the experimental approach I will use. Section 4 presents the findings and discusses the results in detail. Section 5 provides concluding remarks and offers suggestions for future research in this field, highlighting opportunities for enhancing the experimental design and exploring additional areas of investigation. The final section of the paper discusses the limitations encountered during the course of this research.

2 BACKGROUND

A risk-based audit is a systematic approach to auditing that focuses on identifying and assessing risks that may affect the accuracy and reliability of financial statements. The first step in a risk-based audit is to obtain an understanding of the organisation and its environment and to assess the risks of material misstatement [37]. To gain a good understanding of the organisation, the auditor needs to perform a business process analysis of the key business processes. The auditor will emphasise more on comprehending the objectives of the processes, the associated risks, the internal controls and the impact of these risks

and controls on the financial statements [36]. Based on this knowledge, the auditor will perform a risk assessment [37]. The risk assessment begins with the identification of risks. There are two categories of risks, namely business risk and audit risk. Business risk is the risk that an organisation will not meet its objectives or set unrealistic goals or strategies [14]. An understanding of the business risks that can impact the financial statements helps the auditor in identifying potential risks of material misstatements. In case the business risks are not adequately identified, the audit may be unsuccessful [48]. However, the auditor's responsibility is limited to identifying only those business risks that have a direct impact on the financial statements, as the scope of business risks is broader than the risks of material misstatement [29]. Auditing Standard No.8 describes audit risk as follows: Audit risk is the probability that the auditor expresses an inappropriate opinion when the financial statements are materially misstated [1]. Audit risk is a function of two elements: the possibility of not detecting a material misstatement, known as detection risk and the risks of material misstatements [29]. The latter is evaluated at two levels: inherent risk, which is the evaluation of the likelihood of material misstatements before taking internal controls into account [37] and control risk, which is the risk that a misstatement will not be prevented or detected on a timely basis by the organisation's internal control [11]. The aim of auditors is to keep the overall audit risk at an acceptable level [28].

After identifying the risks, auditors try to identify all the underlying risk factors, which are the root causes of those risks [45]. The presence of risk factors varies based on the organisation and its environment. When it comes to identifying risk factors, there are typically four approaches an organisation can use: the sampling approach, the systems approach, the audit risk approach and the business risk approach. Currently, only the audit risk approach and business risk approach are commonly used in the auditing industry [5]. However, all approaches use some form of a questionnaire or a list of risk factors to direct the auditor's attention and guide their modifications to the audit plan and approach [38]. Mock and Turner discovered that risk factors related to fraud show a significant positive association with changes in extent and staffing, as well as with the addition and deletion of planned procedures. Risk factors associated with industry conditions also have a significant positive relationship with these changes. Similarly, risk factors associated with client operations show a significant positive association with changes in staffing and the addition of new audit procedures. They also showed that the method of identifying fraud risk factors, either through a checklist or an open-ended format, can impact the outcome of a risk assessment. Checklist users document fewer risk factors relying on pre-defined options. While an open-ended format allows auditors to document risk factors in their own words leading to the identification of more risk factors [38]. By recognising and considering risk factors, auditors can enhance the efficiency and effectiveness of the audit planning process and allocate resources accordingly [25]. The experience of an auditor is also an important factor in the identification of risk factors. An experienced auditor can gather relevant information more efficiently and identify patterns and anomalies more effectively, compared to a less experienced auditor [20]. So, the experience of an auditor can positively impact the identification of risk factors [45].

After the identification of risks and risk factors, auditors must develop an audit plan. The risk assessment will significantly influence the planning of an audit. The result of the planning process is a specific audit program that outlines the nature, timing and extent of audit procedures [39]. The nature of an audit involves determining the type of testing to be performed, while the timing refers to when the tests are conducted and the extent refers to the amount of testing [11]. Two commonly used risk-based audit methods are the audit risk method (ARM) and the business risk auditing (BRA). ARM focuses on maintaining an acceptable level of audit risk [31], while BRA focuses on the client's competitive environment, strategy for success and critical internal processes [35]. Both ARM and BRA have their own set of advantages and disadvantages. For example, BRA requires the auditor to have a deeper understanding of the client's business, while ARM is more focused on evaluating internal controls and may not require the same level of understanding of the client's business. The choice between these methods depends on the needs of the auditor and their level of experience. Additionally, they can be used together, with auditors often using BRA as a complement or supplement to ARM. However, their ultimate goal is to assess the financial statements and the internal controls of the organisation [45]. After planning the audit, auditors assess the internal controls to determine their effectiveness and efficiency in mitigating

---

[1] http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_8.aspx.

the identified risks. The evaluation of internal controls is a critical part of the overall auditing process [24]. Internal controls are integral mechanisms implemented to ensure that an organisation operates effectively, maintains transparency and complies to relevant laws and regulations. These controls have an impact on the entire organisation, with the primary responsibility for their implementation resting upon the top of the organisation, including management and the board of directors [10]. In order to be effective, internal controls should aim to prevent or promptly detect and correct material financial statement misstatements within a specific functional area before issuing financial reports [28]. The auditor will assess the design and effectiveness of the internal controls and test them during the course of the audit to evaluate the control environment [26]. This can identify any areas of weakness and vulnerability in an organisation's operations, financial reporting and internal controls. By doing so, the organisation can improve its operations, financial reporting and strengthen its internal controls [10]. Manually modeling business processes, conducting a risk assessment and evaluating financial statements and internal controls can be challenging, especially given the exponential growth of data. Utilising data analytics can streamline these tasks and increase efficiency [42].

Process mining, a specific application of data analytics, can provide significant benefits in an audit[31]. There are three basic forms of process mining: process discovery, conformance checking and process enhancement [1]. Process discovery is a process mining technique that aims to represent and visualise a process model from event data collected in an event log. The purpose of process discovery is to gain insights into the real-life process and identify areas for improvement [2]. Conformance checking is used to verify whether a real-life process adheres to a pre-defined process model or not. It compares the actual event log of a process with the model, to see if the events took place in the expected order, if the activities were performed by the right individuals and if the process took the expected amount of time. Conformance checking helps to identify deviations, errors and bottlenecks in a process. It also supports continuous process improvement by providing insights into how the process can be made more efficient and effective [3] The objective of process enhancement is to utilise the information about the actual process recorded in an event log to extend or improve an existing process model. Unlike conformance checking, which measures the alignment between the model and reality, this third form of process mining seeks to modify or expand the a priori model [1].

Process mining is an innovative approach that has emerged in the auditing industry. This technology leverages data analytics to gain insight into business processes [3] and it can serve as a link between the fields of data mining and model driven process management [2]. The aim of process mining is to gain insight into the actual workings of an organisation's processes by extracting information from event logs recorded by an information system, such as the Enterprise Resource Planning system (ERP). An event log is a sequential record of activities that take place on a computer system [16]. The use of the event log as the foundation for analytical procedures is particularly appealing because it not only includes data entered by the audit subject but also meta-data (data about data), which are automatically recorded and independent of the actions and processes being audited. This differs from traditional analytical procedures that rely on data entered by the auditee [30]. The greater the completeness and accuracy of the information contained in the event logs, the more closely the discovered process will match the actual underlying business process [1]. The utilisation of process mining techniques in audits enables auditors to gain a deeper understanding of the client's key business processes, detect potential risks and evaluate the effectiveness of internal controls [3]. With this technology, auditors can delve into the intricacies of a process and detect any deviations from the expected behaviour. By applying process mining to audits, auditors can uncover anomalies that might have gone undetected with traditional audit techniques. This can help to improve the accuracy and effectiveness of the audit and allow auditors to identify areas of risk more effectively [16].

The objective of this research is to identify the risk factors associated with business processes and examine how process mining can effectively address these risk factors. Firstly, it is necessary to identify the risk factors associated with business processes. According to Mock and Turner (2005), organisations typically provide auditors with questionnaires or risk factor lists to guide their attention and inform modifications to the audit plan and approach [38]. However, these risk factors refer to those related to the financial statements and the potential for material misstatement. The identification of risk factors associated with business processes often relies on the expertise and experience of auditors. However

once the risk factors, that auditors consider when assessing business processes, are listed, then process mining can be used to evaluate whether they are being adequately addressed [3]. To address these risk factors, two process mining techniques will be employed: process discovery and conformance checking. Process discovery aids auditors in understanding the process by visualising its flow and activities. While conformance checking provides auditors with the capability to identify anomalies or deviations from the expected process recorded in the event log [3]. Process enhancement will not be utilised in this context as it is primarily targeted toward management or internal auditors. This technique focuses on identifying opportunities for process improvements and may have limited relevance for external auditors. [31]. The use of process discovery and conformance checking allows the auditor to evaluate the efficiency of the process and the internal controls, identify all risks and address risk factors [30].

3 METHODOLOGY

This research aims to identify the risk factors that auditors take into account when assessing business processes and to investigate how a process mining analysis can address these. To achieve this, a literature review was conducted to gather information on the different risk factors that auditors consider during a risk assessment.

I collected all the articles from EBSCOhost using the search terms 'Risk factors in audit', 'Risk factor AND audit', 'business process AND audit AND risk factors' and 'process mining AND audit'. By gathering these articles, I gain valuable insights into the risk factors commonly encountered in audits. To streamline the article selection process and ensure relevance, I implemented filters. Specifically, I applied filters to include only articles written in English, those that underwent peer review and those with full-text availability. I chose English as the language for my search based on my knowledge in this language and the abundance of relevant literature available in English. Additionally, I used peer-reviewed articles, which undergo evaluation by experts in the field. This review process enhances the credibility and reliability of the articles, as they are assessed and approved by specialists who agree with the content and findings. Access to the full text of the article is required to read it and obtain complete information. Through this process, I came across a total of 273 articles. These articles are then screened based on their title, abstract and keywords, with the aim of identifying whether they mention risk factors in audits that are related to business processes. After applying the screening process, 24 articles were identified and added to my Zotero collection. I conducted both forward and backward reference searching on these articles to ensure comprehensive coverage of relevant information. As a result, the total number of articles increased to 37. The next step involves reviewing the articles, where each article is thoroughly read to determine if it mentions risk factors that are related to business processes. After reading the full text, a final total of 20 was included in this study. Upon completing the review of all collected articles, the most significant risk factors are identified.

After concluding the literature review, I proceed to conduct interviews with experienced auditors. These interviews serve two purposes. Firstly, they help determine the practical relevance of the identified risk factors from the literature review. Secondly, they provide insights into additional risk factors that auditors consider when assessing business processes, which may not have been identified during the literature review. The interviews conducted in this research provide a comprehensive overview of the relevant risk factors that should be considered. I have conducted interviews with three auditors, including one internal auditor from a hospital and two auditors from KPMG. I contacted the internal auditor, who then provided me with referrals to the other two auditors. In my interview, I incorporated a combination of open-ended and closed-ended questions. The open-ended questions allowed the auditors to share their experiences and provide insights based on their knowledge and expertise. The closed-ended questions were designed to specifically address the relevance of the risk factors. I began the interviews by outlining the objective of my thesis and the purpose of the interview. Following that, I asked the auditors to provide an overview of a typical audit process from their perspective. This allowed me to gain insights into how they identify risks and risk factors during their audits. Next, I asked the auditors to review the risk factors I had identified, in terms of their relevance in real-life auditing scenarios. This helped me assess whether the risk factors identified in the literature were considered in practice. Finally, I asked the auditors to share any additional risk factors they consider when assessing business processes. This allowed me to capture any additional insights and expand the scope of risk factors to be considered in my research. As a

result of the literature review and the interviews, I have obtained a comprehensive understanding of the relevant risk factors that are taken into account when assessing business processes.

The subsequent phase of this research involves examining whether a process mining analysis can effectively address the identified risk factors. Specifically, the study will focus on two process mining techniques: process discovery and conformance checking. Process discovery entails building a process model from event logs, which can provide valuable insights into the business process and its variations. On the other hand, conformance checking is used to compare an existing process model with event logs to pinpoint deviations and potential risks. These deviations and risks may be linked to specific risk factors. To address the identified risk factors, I use the insights provided by relevant literature to effectively address the risk factors through process mining techniques. Furthermore, I use my knowledge and experience in process mining gained during my studies. By combining external resources and personal expertise, I develop effective strategies to address the identified risk factors.

Lastly, I delve into additional risk factors that do not directly influence business processes but can still be effectively addressed through a process mining analysis. I analyse the articles collected during this research to identify these risk factors. To address these additional risk factors, I utilise relevant literature and use my knowledge in process mining to identify strategies for addressing the additional risk factors. This approach ensures that additional risk factors are thoroughly evaluated and managed. The outcome of this research will aid in formulating an approach for auditors to address the risk factors involved in business processes by utilising process mining techniques. Additionally, the study will offer valuable insights into the probable advantages of incorporating process mining techniques to enhance the efficiency and efficacy of audit operations.

4 FINDINGS

In this section, I will present the findings of this research. It begins with a literature review, which aims to identify the risk factors associated with business processes. Following the literature review, the interviews conducted with auditors will be examined to not only validate the identified risk factors from the literature review but also uncover additional risk factors considered in practice. Building upon the identified risk factors, I then explore how process mining techniques can address these risks. Lastly, the exploration of additional risk factors that can be addressed through process mining techniques will be discussed.

4.1 Risk factors associated with business processes

The objective is to identify the risk factors that are specifically associated with business processes. This is achieved through a literature review and interviews with experienced auditors. By examining existing research and gathering insights from industry professionals, the aim is to uncover the various risk factors that can have significant implications for organisations. The focus is on gaining a comprehensive understanding of the potential risk factors that organisations may encounter, ultimately enhancing the ability to address these risk factors.

4.1.1 Risk Factors related to business processes: A comprehensive literature review

In this literature review, the focus is specifically on exploring the risk factors that are directly related to business processes. By delving into relevant academic articles, I aim to gain a comprehensive understanding of the various risk factors that organisations encounter within their business processes. The risk factors that auditors consider when assessing business processes can vary depending on the industry and type of organisation being audited. Table 1 displays the risk factors that were identified during the literature review and are specifically associated with business processes.

SAS No. 82 presents two types of fraud, one related to fraudulent financial reporting and the other to the misappropriation of assets. Within the type of fraudulent financial reporting, SAS No. 82 identifies three categories: management characteristics, industry conditions and operating characteristics. The first category, management characteristics, primarily examines the capabilities, integrity and competence of management. These factors can significantly impact the effectiveness of internal controls and the execution of business processes. Industry conditions encompass changes in the external environment of the organisation like regulatory changes and technological developments. These factors directly influence

how business processes are designed and conducted [15]. The operational characteristics address the nature and complexity of the organisation and its transactions. Auditors conduct testing on transactions to examine the corresponding processes. By evaluating these transactions, auditors gain insights into the underlying processes and assess their compliance, efficiency and effectiveness [17]. For the misappropriation of assets, SAS No. 82 identified two categories of risk factors: susceptibility of assets to misappropriation and controls. Susceptibility of assets to misappropriation refers to the vulnerability of an organisation's assets to theft. According to SAS No. 82 and Strand et al. (2002), the risk factors within this category primarily impact financial assets and do not have an influence on business processes [44, 15]. The controls category encompasses the absence or insufficiency of controls that are specifically designed to prevent or detect the misappropriation of assets. Controls such as segregation of duties or system authorisation are directly embedded within the structure of business processes. The effectiveness of these controls has a direct impact on the efficiency, accuracy and reliability of the business processes [46, 18].

Management's characteristics significantly impact the design, implementation and execution of the control environment [15]. A first risk factor that can be added to this category is management integrity [47]. Management integrity refers to the ethical values, honesty and trustworthiness of the individuals in leadership positions within an organisation. It is a critical factor that can significantly impact the effectiveness of internal controls. Without the commitment and adherence of management, even the most robust control systems may fail to prevent or detect fraudulent activities or other irregularities. Assessing and addressing management integrity is essential for mitigating risks and ensuring the integrity of financial reporting and operations [34]. Another risk factor that can be added is management turnover. Management turnover refers to the frequency or rate at which key management personnel, such as executives or senior managers, leave or are replaced within an organisation. Management turnover can introduce risks and uncertainties in the business processes, as new managers may have different approaches, priorities or levels of understanding of the controls in place [15]. According to Fukukawa et al. (2011), auditors consider management turnover to be of medium importance as a risk factor [25].

Industry changes encompass a range of risk factors that reflect the environment in which an organisation operates. These factors include regulatory changes, technological developments, shifts in market conditions and industry-specific developments [15]. Van Buuren et al. (2014) found that auditors frequently consider regulation as an important factor in their auditing processes [13]. Regulatory changes involve updates or modifications to laws, rules and standards that govern the industry. When regulations change, organisations are required to adjust their operations accordingly. For instance, if there are alterations in the assessment of internal controls mandated by regulations, it can impact how business processes are conducted. This introduces a higher likelihood of risk exposure for the organisation. Consequently, organisations must ensure that their processes align with the applicable regulations and have adequate controls in place to effectively manage the associated risks [9, 15]. Another risk factor whiting this category is industry change. Industry changes can significantly influence business processes by introducing new risks due to shifts in consumer preferences, market dynamics and opportunities for operational improvement. Mock and Wright (1999) highlight the significance of this risk factor in the context of auditing. Their research indicates that auditors recognise the importance of staying updated and adapting to industry changes in real-life auditing scenarios [40]. The last risk factor in this category is technological development. In today's business landscape, technology plays a crucial role in storing data and supporting various business processes. Organisations heavily rely on technology to streamline operations, enhance efficiency and mitigate errors. However, the introduction of new technologies can raise new risks that organisations need to address. As organisations embrace new technologies, they must be mindful of the potential challenges and vulnerabilities that come with them [33]. According to Fukakawa and Apostolou, the risk factor of technological developments is rated as having medium importance. This suggests that auditors need to give due attention to the risks associated with technological developments but may prioritise other risk factors that are deemed to be of higher importance [25, 7].

The operating characteristics category encompasses various aspects related to the nature and complexity of an organisation's operations and transactions, as well as its financial condition and profitability [15]. business processes involve the initiation, processing and recording of transactions [30]. When a

transaction deviates from the expected norms and patterns, it is categorised as an unusual transaction. These deviations introduce higher risks as they can be indicative of errors, fraud or control deficiencies. Consequently, unusual transactions are recognised as a significant risk factor. [40, 4]. There are two types of unusual transactions identified: those with unusual amounts of items purchased and those with unusual types of items purchased. While some of these transactions may be deemed acceptable, it is still essential to detect and address them. Unusual transactions can potentially serve as indicators of fraudulent activity or control errors within the business process [30]. Duplicate transactions represent another risk factor, as highlighted by Chiu et al. (2019) in their research findings. When a duplicate transaction occurs, it could be possible that this is a separate payment for one transaction, but it could also be a duplicate payment for one transaction. If the latter occurs, it could indicate an internal control issue. This is why auditors check for duplicate payments to identify any control failures [18]. Chiu et al. (2019) also identify transactions that occur without proper approval as another type of transaction to consider. These transactions may lack the necessary authorisation or documentation required for processing. This can indicate potential control deficiencies, such as a breakdown in the approval process or bypassing of established controls. By identifying and addressing these transactions without approval, auditors help mitigate risks, strengthen internal controls and ensure the integrity and reliability of financial information [18]. The last risk factor is outdated systems. Bedard and Graham(2005) emphasise the significance of outdated systems as a critical risk factor. Such systems can introduce vulnerabilities and limitations that hinder an organisation's ability to perform tasks securely and efficiently. Failure to regularly update or maintain these systems may leave them exposed to known vulnerabilities, making them susceptible to security breaches and exploitation by malicious actors [9, 8].

Controls play a vital role within organisations as they encompass the systems, policies and procedures established by management to ensure the accuracy, reliability and compliance of reporting and operations. They play a crucial role in minimising errors and ensuring the smooth functioning of business processes [10]. By integrating controls into business processes, organisations aim to prevent errors and deviations from established standards, thereby promoting accuracy, efficiency and compliance throughout their operations [46]. The first control to consider is the segregation of duties, which is a vital internal control mechanism for all organisations. Quadackers highlights the significance of segregation of duty as an essential risk factor that auditors should consider and address in their assessments [41]. Segregation of duties refers to the practice of dividing key responsibilities and tasks among different individuals within an organisation. The goal is to ensure that no single person has control over multiple critical aspects of a business process. By separating duties, the organisation reduces the risk of fraud, errors and inappropriate activities [31]. Another crucial control is the order of execution. By ensuring that activities are carried out in the correct sequence, organisations can minimise the risk of errors or fraudulent behaviour [18]. For example, if an employee fails to follow the prescribed procedures, such as obtaining proper approval before placing an order for goods, it can result in errors in the process when the approval is denied [33]. Chiu et al. (2019) provide evidence that the order of execution is a significant risk factor that requires increased attention from auditors [18]. Strand et al. (2002) highlight the importance of system authorisation as a control to consider [44]. The authorisation is a control mechanism implemented by management within organisations to prevent potential misstatements. It involves the process of granting approval or permission for various activities or transactions. When there is a lack of authorisation controls, it creates a vulnerability that can be exploited by unauthorised individuals. Without proper authorisation controls, these individuals may be able to approve questionable transactions. This lack of control opens up the possibility for fraudulent activities within the system [6]. Lastly, access control is an important component of an organisation's overall security framework. It refers to the mechanisms and policies implemented to regulate and manage user access to systems, applications, data and resources. The primary goal of access control is to ensure that only authorised individuals or entities are granted access to the organisation's information systems. If access control fails and unauthorised individuals gain entry into a system, it can have serious consequences. These individuals may have the ability to modify data or gain access to sensitive information. This can lead to various risks and potential harm to the organisation, including data breaches, financial losses, reputational damage and regulatory non-compliance [6, 46].

The identified risk factors from the literature review are presented below in table 1, along with their respective categories:

Categories	Risk factors
Management characteristics	Management integrity
	Management turnover
Industry change	Government regulations
	Industry change
	Technological developments
Operating characteristics	Unusual amount of items purchased
	Unusual types of items purchased
	Duplicate transactions
	Payment without approval
	Outdated systems
Controls	Order of execution
	Segregation of duty
	Lack of system authorisation
	Access control

Table 1. Business process risk factors identified during literature review

4.1.2 Examining the significance of risk factors in business processes

In this section, I examine the significance of the risk factors related to business processes that have been identified through the literature review. I accomplished this by conducting interviews with three experienced auditors. Furthermore, I have included one additional risk factors that specifically relate to business processes, which was discovered during the interviews with the auditors.

The risk factors that emerged as particularly significant during the interviews were government regulation, segregation of duty and lack of authorisation. These factors were highlighted by the auditors as having a notable impact on the effectiveness and integrity of business processes. According to all three auditors, compliance with government regulations is of utmost importance for organisations, especially in heavily regulated industries. Ensuring adherence to these regulations can present a significant challenge. During the interviews, the two auditors from KPMG emphasised that mistakes and errors related to compliance with the appropriate regulations were prevalent. This highlights the importance of establishing robust processes and controls to effectively manage and monitor compliance requirements and mitigate associated risks. According to one of the auditors from KPMG, the segregation of duty control is commonly known and implemented by most organisations. However, the auditor highlighted that despite its presence, errors still occur. This is often due to personnel attempting to bypass or circumvent the control, rendering it ineffective. Such actions undermine the intended purpose of segregation of duty, which is to prevent fraud, errors and unauthorised activities by ensuring that no single individual has complete control over a critical process. These findings suggest that organisations need to not only establish segregation of duty controls but also ensure their proper implementation and enforcement to mitigate the associated risks effectively. All three auditors have recognised the absence of system authorisation as a critical risk factor. They unanimously recognise its significance in granting approval or permission for various activities or transactions. The auditors emphasise the importance of implementing and enforcing effective system authorisation controls to mitigate the risk of fraudulent behaviour. Another risk factor that is frequently considered is the order of execution. According to the internal auditor, addressing this factor involves mapping out the process to gain a comprehensive understanding of its flow. By doing so, the auditor can identify the expected sequence of activities and transactions within the process. Any deviations or anomalies from this established order of execution are carefully examined to determine the root cause of the problem. By thoroughly assessing and addressing the order of execution, the auditor aims to ensure that the business processes are carried out in a structured and controlled manner, reducing the risk of disruptions and improving overall operational effectiveness.

According to one of the auditors from KPMG, technological developments are often not given much consideration in practice. This is because organisations tend to stick with their existing technology. Auditors typically only consider technological changes when organisations undergo significant updates or transitions in their technology infrastructure. In such cases, auditors will assess the impact of these

changes on the organisation's systems, controls and overall business processes. However, if there are no substantial technological changes taking place, auditors may not focus extensively on technological developments during their assessments. Despite the infrequent consideration of technological advancements, this research will address this risk factor. The remaining risk factors identified in the literature review were not found to be highly significant or critical, but they were not completely disregarded either. While they may not have been prioritised as extensively as other risk factors, the auditors still acknowledged their presence and considered them during their assessments. The importance assigned to these risk factors may vary depending on the specific context and circumstances of each organisation.

In addition, the internal auditor identified one additional risk factor that is directly related to business processes: the risk of cyberattacks by hackers. With the increasing adoption of technology in organisations, the risk posed by hackers has become more significant. The potential consequences of a successful hack can be severe, leading to operational disruptions or even complete shutdowns. Therefore, addressing and mitigating this risk should be of utmost importance for organisations. Despite having implemented robust security measures such as firewalls, encryption and access controls, the internal auditor I interviewed acknowledged that cyberattacks continue to pose a significant threat. To mitigate the risk of hackers infiltrating the system, organisations must establish robust security control systems. Security control systems are vital in safeguarding the organisation against hackers. Hence, the risk factor "security control systems" is included in the controls category to address the vulnerability that arises if these systems fail.

Table 2 presents a comprehensive list of relevant risk factors associated with business processes, identified through a combination of literature review and interviews.

Categories	Risk factors
Management characteristics	Management integrity
	Management turnover
Industry change	Government regulations
	Industry change
	Technological developments
Operating characteristics	Unusual amount of items purchased
	Unusual types of items purchased
	Duplicate transactions
	Payment without approval
	Outdated systems
Controls	Order of execution
	Segregation of duty
	Lack of system authorisation
	Access control
	Security control systems

Table 2. All relevant business process risk factors

4.2 Exploring the role of process mining in addressing risk factors of business processes

This section will explore the potential applications of process mining in addressing the identified risk factors associated with business processes. This will be achieved by using relevant literature and combining it with my knowledge and expertise in the field of process mining. Process mining can be applied to identify bottlenecks, assess process conformance, predict potential execution issues and monitor process deviations. As a result, it can be utilised to address the risk factors listed in table 2.

4.2.1 Management characteristics

Management characteristics encompass the adherence of management to established rules and procedures, as well as the potential influence of turnover on business processes.

Process mining indirectly addresses management integrity by analysing event log data. It enables

auditors to gain insights into the execution of control activities, identifying deviations and anomalies that may indicate a lack of integrity. By utilising meta-data from event logs, process mining filters and identifies actions performed specifically by management [33]. Through this technique, auditors can analyse these actions and detect patterns suggestive of control bypassing or suspicious activities by management. By comparing actual process execution with predefined control rules, process mining identifies instances of control violations, empowering auditors to investigate further and evaluate the effectiveness of internal controls [18]. Overall, process mining serves as a powerful tool for auditors to assess management integrity by analysing event log data, identifying deviations in control activities and evaluating adherence to control procedures.

For addressing management turnover, Process mining indirectly provides insights into the impact of management turnover on business processes and the control environment. By analysing event log data, auditors can identify deviations from the normal process and assess the effectiveness of internal controls [33]. When the process deviates from the expected flow, it may indicate skipped tasks or a different sequence of execution, which can potentially lead to errors. Process mining detects these deviations by comparing the actual process execution with the expected process model [18]. This enables auditors to investigate and evaluate the validity of these deviations. In terms of assessing internal controls, process mining allows auditors to test the controls against predefined rules or expected patterns of behaviour. By analysing event log data, process mining techniques automatically compare the actual execution of processes with the predefined control rules. This analysis identifies instances of control violations or deviations [6]. When a deviation from the predefined rules is detected, process mining flags it as a potential control violation or anomaly. This information empowers auditors to conduct further investigations and evaluate the effectiveness of internal controls. In summary, process mining provides auditors with a valuable tool to assess the influence of management turnover on business processes. It helps identify deviations from the normal process and assess the adherence to internal controls, enabling auditors to take appropriate measures to mitigate associated risks.

In conclusion, process mining is a powerful tool that indirectly addresses risk factors related to management integrity and turnover. By analysing event log data, auditors can detect deviations, anomalies and patterns in the execution of control activities, providing insights into management's adherence to control procedures and identifying potential instances of a lack of integrity. Additionally, process mining allows auditors to track changes in business processes caused by management turnover and evaluate the effectiveness of internal controls. By comparing actual process execution with predefined rules and expected patterns, auditors can identify control violations and deviations, enabling them to take necessary measures to mitigate associated risks. Overall, process mining enhances the ability of auditors to assess and address risk factors related to management characteristics, ultimately contributing to the effectiveness and integrity of business processes.

4.2.2 Industry conditions
The category of industry conditions focuses on analysing the external factors and dynamics that impact the performance and operations of organisations. It aims to provide insights into the regulatory environment, technological developments and the changing industry.

Process mining analysis can help in detecting instances of non-compliance with government regulations. To address this risk factor, rule-based process mining can be used. It involves defining rules based on the specific regulations that the organisation needs to comply with. Process mining algorithms then evaluate the event log data against these defined rules to identify any deviations or violations [6]. For example, if legal requirements mandate that a specific set of tasks must be completed in a particular order by specifically trained personnel. Then rules can be established to enforce the sequential execution of activities, such as requiring that activity A must be followed by activity B. Additionally, rules can specify that activity A must be performed by employee A, who is trained to carry out that activity. Process mining can analyse the event log data and evaluate whether the established rules are being followed. It can detect any deviations from the defined rules, allowing auditors to identify instances where there are instances of non-compliance. This analysis helps to identify instances where the process deviates from the expected compliance standards, enabling auditors to detect instances of non-compliance [6]. However, the ability of process mining to detect non-compliance may vary depending on the type of regulation. A process

mining analysis may not be suitable for addressing regulations related to external factors such as employee training or environmental regulations as they cannot be captured through event logs. Overall, process mining empowers auditors to navigate the complexities of government regulations by providing insights into compliance and control effectiveness. By leveraging the capabilities of process mining, auditors can ensure that organisations meet regulatory requirements, mitigate risks and maintain a robust control environment.

Industry change cannot be directly addressed through a process mining analysis. However, it can still provide valuable insights into the impact of industry changes on business processes. By analysing event log data, auditors can detect patterns and deviations in process behaviour, helping them understand the consequences of industry changes. This allows auditors to identify potential areas of increased risk or potentially fraudulent activities and evaluate the effectiveness of controls in mitigating these risks. For example, during the COVID-19 pandemic, many organisations had to adapt to changing consumer behaviour by shifting to online sales. This required modifications or adaptations to their business processes. Auditors can utilise process mining to analyse the new processes and identify any deviations or inefficiencies in controls that may arise during the change. This helps ensure that the organisation remains compliant and effective in the face of industry changes. While process mining may not be the most direct tool for addressing the risk factor of industry changes, it can still provide valuable insights and support auditors in navigating the challenges brought about by industry change.

Due to the limited consideration of technological developments as a risk factor by auditors in practice, there is a lack of research focused specifically on addressing this risk factor through process mining. However, it is important to recognise the potential impact of technological developments on business processes. Process mining enables auditors to identify control failures, deviations from procedures and non-compliance stemming from technological advancements. By comparing observed process behaviour to predefined control rules, auditors can identify areas where controls may be compromised. This information empowers auditors to take appropriate measures to mitigate risks and propose control enhancements. Process mining equips auditors with the necessary tools and insights to navigate the influence of technological developments on business processes. By utilising process mining techniques, auditors can identify potential risks and evaluate the effectiveness of controls.

To conclude, process mining analysis is a valuable tool for detecting instances of non-compliance with government regulations. By defining rules based on specific regulations and evaluating event log data against these rules, process mining can identify deviations and violations, enabling auditors to detect instances of non-compliance. While its effectiveness may vary depending on the type of regulation, process mining can still provide valuable insights into compliance standards. For addressing technological developments and industry change, process mining may not be the most suitable tool. However, process mining can provide valuable insights into how a process is executed and identify deviations from expected behaviour. By analysing event logs and process data, auditors can assess control effectiveness and detect deviations or anomalies that may indicate risks or control deficiencies. While not directly addressing industry changes or technological developments, process mining can contribute to managing risks in this context.

4.3 operating characteristics

The operating characteristics category encompasses different aspects that pertain to the nature and complexity of an organisation's operations and transactions. The risk factors associated with business processes in this category primarily pertain to transactions. Auditors strive to identify and analyse transactions that deviate from the norm or display abnormal behaviour. Process mining facilitates the detection of transaction deviations through the analysis of event log data [30, 6].

Process mining serves as a valuable tool for auditors to identify transactions involving an unusual number of items purchased. By leveraging process mining techniques, auditors can apply filters and thresholds to detect such transactions [6]. Auditors can start by defining a threshold or expected range for the number of items purchased based on historical data, industry benchmarks or established policies. Process mining allows auditors to analyse transactional data and compare the number of items in each

transaction against the defined threshold or expected range. Transactions that significantly exceed the threshold or deviate from the expected pattern can be flagged for further investigation, as they may indicate potential control failures or fraudulent activities [3].

To detect transactions with unusual types of items purchased, auditors can employ filters based on the item categories or specific item identifiers in the process mining analysis [6]. By setting filters to identify transactions that involve rare or unexpected item types, auditors can flag instances where the purchased items deviate from the norm. This approach allows auditors to pinpoint transactions that may warrant further investigation due to the unusual nature of the items involved. By applying such filters in the process mining analysis, auditors can effectively identify and scrutinise transactions that involve uncommon or potentially suspicious item types. This allows auditors to trace the path of a transaction and identify the specific points where fraudulent activities or control failures may have occurred [30].

Duplicate transactions are another risk factor that can indicate an internal control issue [18]. These transactions can go unnoticed by ERP systems if they do not violate any specific rules or business logic [6]. In such cases, process mining can be a valuable tool for auditors to identify and investigate duplicate transactions. To address duplicate transactions, auditors can use process mining to analyse event logs and process data to identify patterns and repetitions in transactional activities. By comparing transactional attributes such as timestamps, customer details and transaction amounts, auditors can detect instances where identical or highly similar transactions have been processed multiple times. By applying filters and rule-based algorithms, auditors can flag transactions that exhibit characteristics indicative of duplication. For example, they can identify transactions with identical customer information and transaction amounts. These filters help auditors isolate potential instances of duplicate transactions for further investigation. This enables auditors to focus their attention on these transactions and trace their path within the process to pinpoint where the control failure or an error occurred.

Another risk factor is when payments occur without proper approval. By analysing event logs and process data, auditors can leverage process mining to detect deviations from the expected approval process and identify instances where payments have been made without the necessary authorisations. Using process mining, auditors can map out the payment process flow and compare it against predefined control rules to identify non-compliant transactions. By applying filters and rule-based algorithms, auditors can flag payments that bypassed the required approval steps. These filters can be designed to identify transactions lacking appropriate authorisation codes, signatures or supporting documentation. By setting thresholds and detecting deviations from the standard approval process, auditors can flag payments that warrant further investigation. By flagging these transactions, auditors can investigate further to determine the reasons behind the lack of approval and assess the effectiveness of the control measures in place [18].

For addressing the risk factor of outdated systems, process mining can aid the auditor in evaluating the effectiveness of internal controls. Outdated systems can pose risks as they may lead to inadequate or malfunctioning controls. Auditors can leverage process mining to analyse event log data and assess the execution of control activities within the system. This is achieved by comparing the event log data to predefined control rules or expected patterns. By doing so, auditors can identify any deviations or violations that occur in the actual execution of control activities. This enables them to assess the overall effectiveness of the controls. However, outdated systems may have limitations in accurately capturing and recording data, which can hinder the effectiveness of process mining. If the data captured by the outdated system is incomplete, inconsistent or of poor quality, it can impact the reliability and accuracy of the process mining analysis. In such cases, process mining may not be able to fully fulfil its intended purpose. Therefore, auditors need to consider the quality and reliability of the data before applying process mining.

In conclusion, process mining serves as a valuable tool for auditors to address various risk factors related to business processes. It enables auditors to detect transaction deviations, such as unusual numbers of items purchased and transactions involving unusual item types, by applying filters and thresholds in the analysis. Process mining also assists in identifying and investigating duplicate transactions by comparing transactional attributes and identifying patterns of repetition. Additionally, process mining helps auditors identify payments made without proper approval by analysing event logs and process data to detect

deviations from the expected approval process. In addition to identifying all these transactions, auditors can leverage the meta-data stored in the event log to determine the individuals or roles responsible for them [30]. Furthermore, process mining aids auditors in evaluating the effectiveness of internal controls in the context of outdated systems. It allows auditors to assess the execution of control activities by comparing event log data to predefined control rules or expected patterns. However, the reliability and accuracy of process mining may be impacted by the limitations of outdated systems, such as incomplete or poor-quality data. Overall, process mining provides auditors with valuable insights into the operating characteristics of an organisation and helps them address associated risk factors.

4.3.1 Controls

Controls are essential in minimising errors, maintaining compliance and ensuring the smooth functioning of business processes. Effective controls provide a framework to prevent, detect and correct errors, deviations and fraudulent activities. By employing process mining techniques, auditors can effectively address the risk factors associated with controls in this category.

To address the order of execution in a business process, auditors can use process mining to analyse event logs and process data to reconstruct the chronological sequence of activities and assess their compliance with predefined rules or expected patterns [2]. By visualising the process flow, auditors can identify instances where activities are performed out of sequence or where there are deviations from the expected order. By comparing the observed order of execution with the intended or prescribed order, auditors can detect control failures, non-compliant behaviour or potentially fraudulent activities. Process mining allows auditors to pinpoint the exact points in the process where deviations occur and to investigate the underlying causes. However, it is important to note that not all deviations indicate fraudulent activities or control failures. Some deviations may be considered normal and within acceptable limits. Hence, it is important for auditors to thoroughly examine the identified deviations [30].

Another important control is the segregation of duties. Process mining can identify instances where a single employee is responsible for performing two critical tasks within a process, by using the meta-data [18, 30]. auditors can use process mining to apply rules for the segregation of duties and identify violations. By analysing the event log data and associated meta-data, process mining can check if the defined rule for the segregation of duties is followed. For example, if activity A and activity B should be executed by two distinct persons, process mining can trace the execution paths and determine if any instances exist where the same person has performed both activities. In such cases, a violation of segregation of duties is identified and auditors can further investigate to determine the responsible individuals and assess if there are control failures or potential risks associated with the violation [32].

Authorisation is an important control mechanism designed to prevent potential misstatements and ensure the integrity of transactions. Authorisation can be represented by a sign activity or approval step within the business process [16]. For example, let's consider a business process where every transaction must be signed by a manager as an authorisation control. Process mining can be utilised to analyse the event log data and identify any deviations from this control. By examining the event log, process mining can detect instances where transactions are not signed or are signed by unauthorised personnel. These deviations can be flagged as potential control failures or risks within the process. Auditors can then delve deeper into these flagged cases to investigate the underlying causes and assess the effectiveness of the authorisation control. This enables them to identify potential control failures or risks that may compromise the integrity of the process [6].

Another important control mechanism to consider is access control. While process mining may not be able to directly address access control, it can still provide valuable insights into potential access control issues. By analysing event logs and process data, process mining can help auditors detect anomalies and assess the effectiveness of access control mechanisms. For example, if an organisation has a policy of restricting employee access to systems during weekends, process mining can help identify activities performed during that time. By analysing the event logs and associated meta-data, process mining can flag weekend activities that may indicate a violation of access control policies. Auditors can then investigate these activities to determine if there are valid reasons for the access or if there are control failures in place. Process mining can also help identify the individuals responsible for these activities [30], enabling

auditors to further investigate their actions and assess the effectiveness of access controls. Overall, while process mining cannot directly detect unauthorised access, it can indirectly uncover potential instances of access control failure through the analysis of event log data. By identifying deviations from access control policies, process mining helps auditors focus on potential cases of unauthorised access and take necessary actions to mitigate risks and strengthen access controls.

The last control to consider is security control systems. While process mining does not directly address security control systems, it can provide insights into the effectiveness of these systems by analysing event logs and process data. By examining the event logs, auditors can gain visibility into the sequence of security control activities, such as authentication, authorisation and monitoring. Process mining allows auditors to detect deviations from the expected security control processes, identify potential control failures and assess the overall effectiveness of the security control systems in place. For example, auditors can use process mining to analyse event logs and identify instances where security control activities were not properly executed or were bypassed. This could include unauthorised access attempts, violations of access restrictions or suspicious activities that may indicate security breaches. By comparing observed process behaviour to predefined control rules or security policies, auditors can identify anomalies and potential weaknesses in the security control systems. Furthermore, process mining can help auditors trace the path of security-related events and identify specific points where control failures or security breaches may have occurred. By analysing event logs, auditors can determine the individuals or roles involved in security-related activities, allowing for targeted investigations and follow-up actions.

It can be concluded that process mining can serve as a valuable tool for auditors to evaluate and assess the various controls implemented within a business process. By analysing event log data, process mining allows auditors to visualise and understand the actual flow of processes, detect deviations from expected patterns and investigate potential instances of fraudulent activities or control failures. Process mining aids auditors in identifying violations of predefined rules such as the order of execution, allowing them to flag these instances for further investigation. It also supports the enforcement of segregation of duties by tracing the execution paths of activities and identifying cases where a single employee performs two critical tasks, potentially indicating control deficiencies. Furthermore, process mining assists auditors in assessing the effectiveness of authorisation controls by detecting deviations from the required approval steps. Process mining also allows for identifying and investigating access control violations in business processes. It helps auditors flag any deviations from established rules and policies, allowing them to take necessary actions to enhance access controls. While process mining may not directly evaluate security control systems, it can help uncover deviations from established security protocols, highlighting potential security control weaknesses for auditors to address. Overall, process mining enhances the effectiveness of auditing by providing valuable information and insights into the execution and control of business processes.

5 ADDRESSING ADDITIONAL RISK FACTORS

In this section, I identify and address any additional risk factors that do not directly impact business processes. To ensure a structured and comprehensive analysis, the categorisation framework outlined in SAS No. 82, a widely recognised standard for risk assessment, is adopted. This framework facilitates the systematic organisation and analysis of the identified risk factors, enabling a holistic understanding of their implications [15]. I identify these additional risk factors using the collected articles from this research and address them by combining insights from the literature and my knowledge.

The risk factor of competition has been identified and can be classified under the category of industry conditions [27]. According to Fukukawa et al. (2011), the level of competition is rated as highly important. In highly competitive environments, organisations often face intense pressure to achieve results. This pressure can sometimes result in the bypassing of internal controls or employees skipping critical tasks, such as obtaining proper approvals. Auditors recognise the need to investigate the effectiveness of internal controls in such competitive environments to ensure their adequacy and mitigate associated risks [25]. Process mining is a valuable tool for auditors to detect potential control violations and deviations from standard processes. It enables auditors to compare observed process behaviour with predefined control rules. By analysing event logs and process data, auditors can pinpoint instances where these

rules have been breached. This allows for the identification of control failures, enabling auditors to take appropriate actions to mitigate risks [18]. Furthermore, process mining provides auditors with a comprehensive understanding of actual process execution, unveiling deviations that may otherwise go unnoticed using traditional audit methods [3]. This capability allows auditors to uncover instances of potential fraudulent activities. Ultimately, by evaluating the effectiveness of internal controls and identifying deviations from the normal process, process mining indirectly addresses the risk factor competition.

For the operating characteristics category, one additional risk factor is identified namely client size [25]. The size of a client can have implications for the complexity and volume of transactions, as well as the resources required to adequately control and monitor them. Larger clients may have more extensive operations, higher transaction volumes and more complex business processes, which can increase the risk of control failures or errors. On the other hand, smaller clients may have limited resources to implement and maintain effective internal controls. Therefore, auditors need to consider the client size as a risk factor and assess the adequacy of controls based on the specific characteristics and needs of each client [9]. Process mining is particularly beneficial for larger clients as it enables auditors to assess the entire data set rather than relying on sampling methods [31]. This comprehensive approach provides auditors with a more accurate understanding of the client's processes and controls. By analysing event logs and process data, process mining allows auditors to identify patterns, trends and anomalies within a large volume of data. It helps auditors visualise and analyse process flows, uncovering potential control failures or deviations from standard procedures. This enables auditors to evaluate the effectiveness of internal controls and identify instances of control violations, non-compliance or inefficiencies [30]. For smaller clients, process mining may have limited effectiveness due to their potentially limited data availability and resources. Smaller clients may not have the same level of structured data or sophisticated systems as larger organisations, making it challenging to gather the necessary information for a process mining analysis. As a result, auditors may need to rely on other audit procedures and techniques to evaluate the effectiveness of internal controls [19].

In summary, process mining proves to be a valuable tool for auditors in addressing risk factors. It helps detect control violations and deviations from standard processes, providing a comprehensive understanding of process execution. Process mining indirectly addresses the risk factor of competition by evaluating internal controls and identifying deviations. For client size, process mining benefits larger clients by assessing the entire data set and uncovering control failures. However, its effectiveness may be limited for smaller clients with limited data availability. Overall, process mining enhances auditors' ability to evaluate and mitigate risks, improving control effectiveness and risk management.

6 CONCLUSION

This paper aimed to identify and examine the risk factors that impact business processes and evaluate the effectiveness of process mining in addressing these factors. Through my exploration of the relationship between process mining and risk factors, I have shed light on the potential of process mining as a tool for mitigating and managing risks in business processes. The findings of this study have highlighted that various risk factors can significantly impact business processes, whether directly or indirectly. These risk factors include segregation of duty, unusual transactions, industry change, government regulations and system authorisation. It is crucial for organisations to identify and address these risk factors to ensure the effectiveness, efficiency and integrity of their operations. Process mining has emerged as a promising approach to tackle the risk factors that directly or indirectly impact business processes. This technique utilises event logs to map and analyse the intricacies of business processes. Unlike traditional auditing methods that rely on sampling, process mining leverages the entire data set, providing auditors with a more accurate and comprehensive understanding of the business processes and internal controls. Notably, process mining offers the advantage of visualising and analysing the actual flow of processes. By examining event logs and process data, auditors can identify deviations from expected patterns, uncover inefficiencies and evaluate the effectiveness of internal controls. This enables auditors to pinpoint potential control failures or instances of fraudulent activities within the business processes. The findings of this study emphasise the importance of incorporating process mining into risk management strategies. By utilising process mining, auditors gain the ability to detect and address potential risk factors effectively. Additionally, process mining facilitates the identification of hidden risks that may otherwise go unnoticed

with traditional audit approaches. However, it is essential to recognise that process mining should not be seen as a replacement for traditional audit techniques. Instead, it should be regarded as a complementary tool that enhances the effectiveness and efficiency of risk assessment. Auditors should exercise critical judgement and interpret the insights provided by process mining analysis in the context of their specific business environment. To summarise, process mining empowers auditors with a powerful tool to address risk factors that directly or indirectly impact business processes. By analysing event logs and process data, auditors can uncover deviations, control failures and potential instances of fraud. The visualisation and analysis of process flows enable auditors to identify inefficiencies, enhance the effectiveness of internal controls and provide a more comprehensive and accurate assessment of the business processes. Therefore, process mining adds significant value to the auditing industry by effectively addressing risk factors.

Further research is needed to explore the potential applications and benefits of process mining in the field of auditing. The application of process mining has the potential to provide significant value in addressing the risk of material misstatements and mitigating the risk factors associated with financial statements. Furthermore, it is essential to investigate the integration of process mining into auditing practices. This involves exploring how process mining techniques can be seamlessly incorporated into existing audit methodologies and frameworks. By focusing on these areas, future research can unlock the full potential of process mining, enabling auditors to proactively identify and mitigate risks while driving continuous improvement in business processes.

7 LIMITATIONS

The present study is not without its limitations, which should be taken into consideration when interpreting the findings. The present study acknowledges that there may exist additional risk factors that could influence business processes and could be addressed through process mining, but which have not been identified through the literature review or interviews conducted. The limitations of the study lie in the possibility of incomplete or limited information regarding all potential risk factors. Despite efforts to thoroughly explore the subject, it is possible that certain risk factors were overlooked or not sufficiently addressed.

Another limitation of the study is the limited availability of literature specifically focused on the application of process mining in addressing risk factors related to business processes in the field of auditing. Given that process mining is a relatively new and evolving discipline, its integration into auditing practices is still in the early stages. Consequently, there is a lack of comprehensive literature directly addressing the research questions and objectives of this study. The heavy reliance on existing literature can introduce potential implications for the validity and reliability of the findings. The limited availability of literature focused on process mining in auditing may restrict the ability to draw definitive conclusions or generalise the results with confidence.

The small sample size of the interviews conducted is another limitation of this study. With only three interviews conducted, the findings and conclusions may not fully capture the range of perspectives and experiences related to the risk factors associated with business processes. The limited number of interviews may restrict the depth and diversity of insights gained from different stakeholders or experts in the field. It is important to acknowledge that the perspectives and opinions expressed by the interviewees may not be representative of the broader population or may not capture the full complexity of the subject matter. Moreover, the findings from the interviews may be influenced by the specific characteristics of the individuals interviewed, such as their expertise, background or organisational context. This limited scope of perspectives may limit the generalisability of the findings and restrict their applicability to a wider range of contexts or industries. In conclusion, while the three interviews conducted in this study offer valuable insights, it is important to acknowledge the limitations associated with the small sample size. The findings should be interpreted with caution and further research with a larger and more diverse sample is recommended to validate and expand upon the results.

Overall, while the present study endeavours to provide valuable insights into the use of process mining to address risk factors in business processes, it acknowledges the possibility of limitations in terms of undiscovered risk factors, reliance on available literature and small sample size. These limitations

open avenues for future research to further explore and refine the application of process mining in risk management and mitigation.

REFERENCES

[1] Wil van der Aalst. "Process Mining: Overview and Opportunities". In: *ACM Transactions on Management Information Systems* 3.2 (July 1, 2012), 7:1–7:17.

[2] Wil van der Aalst, Arya Adriansyah, and Boudewijn van Dongen. "Replaying history on process models for conformance checking and performance analysis". In: *WIREs Data Mining and Knowledge Discovery* 2.2 (2012), pp. 182–192.

[3] Wil van der Aalst and Angelique Koopman. "Process mining: data analytics voor de accountant die wil weten hoe het nu echt zit". In: *Maandblad voor Accountancy en Bedrjjfseconomie* (Oct. 1, 2015), pp. 359–368.

[4] Modar Abdullatif. "Fraud Risk Factors and Audit Programme Modifications: Evidence from Jordan". In: *Australasian Accounting, Business and Finance Journal* 7.1 (Apr. 1, 2013), pp. 59–77.

[5] Modar Abdullatif and Husam Aldeen Al-Khadash. "Putting Audit Approaches in Context: The Case of Business Risk Audits in Jordan". In: *International Journal of Auditing* 14.1 (2010), pp. 1–24.

[6] Abdulrahman Alrefai. "Audit focused process mining: the evolution of process mining and internal control". PhD thesis. Rutgers University - Graduate School - Newark, 2019.

[7] Barbara Apostolou, John M. Hassell, and Sally A. Webber. "Management fraud risk factors: Ratings by forensic experts". In: *The CPA Journal* 71.10 (Oct. 2001), pp. 48–52.

[8] Jean C. Bedard and Lynford E. Graham. "The Effects of Decision Aid Orientation on Risk Factor Identification and Audit Test Planning". In: *Auditing: A Journal of Practice & Theory* 21.2 (Sept. 1, 2002), pp. 39–56.

[9] Jean C. Bedard, Lynford E. Graham, and Cynthia Jackson. "Information Systems Risk and Audit Planning". In: *International Journal of Auditing* 9.2 (2005), pp. 147–163.

[10] Jean C. Bédard, Nadine Glaudemans, Mieke Jans, and Mathijs van Peteghem. *Litarature review: current knowledge on internal control.* 2017.

[11] Allen Blay, Tim Kizirian, and L. Dwight Sneathen. "Evidential Effort and Risk Assessment in Auditing". In: *Journal of Business and Economics Research* 6.9 (Jan. 1, 2008), pp. 39–52.

[12] Helen Brown-Liburd, Hussein Issa, and Danielle Lombardi. "Behavioral Implications of Big Data's Impact on Audit Judgment and Decision Making and Future Research Directions". In: *Accounting Horizons* 29.2 (June 1, 2015), pp. 451–468.

[13] Joost van Buuren, Christopher Koch, Niels van Nieuw Amerongen, and Arnold M. Wright. "The Use of Business Risk Audit Perspectives by Non-Big 4 Audit Firms". In: *Auditing: A Journal of Practice & Theory* 33.3 (Aug. 1, 2014), pp. 105–128.

[14] Carla Carnaghan. "Business process modeling approaches in the context of process level audit risk assessment: An analysis and comparison". In: *International Journal of Accounting Information Systems*. 2005 Research Symposium on Integrity, Privacy, Security & Trust in an IT Context 7.2 (June 1, 2006), pp. 170–204.

[15] American Institute of Certified Accountants (AICPA). *Consideration of Fraud in a Financial Statement Audit. SAS No.82.* 1997.

[16] Tiffany Chiu. "Exploring new audit evidence: the application of process mining in auditing". PhD thesis. Rutgers University - Graduate School - Newark, 2018.

[17] Tiffany Chiu, Helen Brown-Liburd, and Miklos A. Vasarhelyi. "Performing Tests of Internal Controls Using Process Mining: What Could Go Wrong?" In: *The CPA Journal* 89.6 (June 2019), pp. 54–57.

[18] Tiffany Chiu and Mieke Jans. "Process Mining of Event Logs: A Case Study Evaluating Internal Control Effectiveness". In: *Accounting Horizons* 33.3 (Sept. 1, 2019), pp. 141–156.

[19] Lina Dagilienė and Lina Klovienė. "Motivation to use big data and big data analytics in external auditing". In: *Managerial Auditing Journal* 34.7 (Jan. 1, 2019), pp. 750–782.

[20] Jefferson T. Davis. "Experience and Auditors' Selection of Relevant Information for Preliminary Control Risk Assessments". In: *accounting, auditing and financial reporting* (1996), pp. 16–32, 35–37.

[21] Christine E. Earley. "Data analytics in auditing: Opportunities and challenges". In: *Business Horizons* 58.5 (Sept. 1, 2015), pp. 493–500.

[22] Peter Eimers and Oscar van Leeuwen. "De typologie als basis voor een effectieve en efficiënte data-analyse". In: *Maandblad voor Accountancy en Bedrijfseconomie* 89.10 (Sept. 10, 2015). Number: 10 Publisher: Amsterdam University Press, pp. 348–358.

[23] Peter Eimers and Remco ter Steege. "Data-analyse in de controlestandaarden; uitdagingen en ontwikkelingen". In: *Maandblad voor Accountancy en Bedrijfseconomie* 96.1 (Mar. 14, 2022), pp. 5–13.

[24] Faudziah Fadzil, Hasnah Haron, and Muhamad Jantan. "Internal auditing practices and internal control system". In: *Managerial Auditing Journal* 20.8 (Jan. 1, 2005), pp. 844–866.

[25] Hironori Fukukawa, Theodore J. Mock, and Arnold Wright. "Client Risk Factors and Audit Resource Allocation Decisions". In: *Abacus* 47.1 (2011), pp. 85–108.

[26] Audrey A. Gramling, Edward F. O'Donnell, and Scott D. Vandervelde. "An Experimental Examination of Factors That Influence Auditor Assessments of a Deficiency in Internal Control over Financial Reporting". In: *Accounting Horizons* 27.2 (Jan. 1, 2013), pp. 249–269.

[27] Jacqueline S. Hammersley, Karla M. Johnstone, and Kathryn Kadous. "How Do Audit Seniors Respond to Heightened Fraud Risk?" In: *Auditing: A Journal of Practice & Theory* 30.3 (Aug. 1, 2011), pp. 81–101.

[28] Chris E. Hogan and Michael S. Wilkins. "Evidence on the Audit Risk Model: Do Auditors Increase Audit Fees in the Presence of Internal Control Deficiencies?*". In: *Contemporary Accounting Research* 25.1 (2008), pp. 219–242.

[29] IAASB. *ISA 315 revised, Identifying and Assessing the Risks of Material Misstatement Though Understanding the Entity and Its Environment*. 2019.

[30] Mieke Jans, Michael G. Alles, and Miklos A. Vasarhelyi. "A Field Study on the Use of Process Mining of Event Logs as an Analytical Procedure in Auditing". In: *The Accounting Review* 89.5 (Sept. 1, 2014), pp. 1751–1773.

[31] Mieke Jans, Michael G. Alles, and Miklos A. Vasarhelyi. "The case for process mining in auditing: Sources of value added and areas of application". In: *International Journal of Accounting Information Systems* 14.1 (Mar. 1, 2013), pp. 1–20.

[32] Mieke Jans, Jan M. van der Werf, Nadine Lybaert, and Koen Vanhoof. "A business process mining application for internal transaction fraud mitigation". In: *Expert Systems with Applications* 38.10 (Sept. 15, 2011), pp. 13351–13359.

[33] Mieke Julie Jans, Michael Alles, and Miklos A. Vasarhelyi. *Process Mining of Event Logs in Auditing: Opportunities and Challenges*. Rochester, NY, Feb. 15, 2010.

[34] Timothy G. Kizirian, Brian W. Mayhew, and L. Dwight Sneathen Jr. "The Impact of Management Integrity on Audit Planning and Evidence". In: *Auditing: A Journal of Practice & Theory* 24.2 (Nov. 1, 2005), pp. 49–67.

[35] Robert W. Knechel, Steven E. Salterio, and Natalia Kochetova-Kozloski. "The effect of benchmarked performance measures and strategic analysis on auditors' risk assessments and mental models". In: *Accounting, Organizations and Society* 35.3 (Apr. 1, 2010), pp. 316–333. (Visited on 11/29/2022).

[36] Natalia Kochetova-Kozloski, Thomas M. Kozloski, and William F. Messier Jr. "Auditor Business Process Analysis and Linkages among Auditor Risk Judgments". In: *Auditing: A Journal of Practice & Theory* 32.3 (Aug. 2013), pp. 123–139.

[37]   Natalia Kochetova-Kozloski and William F. Messier. "Strategic Analysis and Auditor Risk Judgments". In: *Auditing: A Journal of Practice & Theory* 30.4 (Nov. 2011), pp. 149–171.

[38]   Theodore J. Mock and Jerry L. Turner. "Auditor Identification of Fraud Risk Factors and their Impact on Audit Programs". In: *International Journal of Auditing* 9.1 (2005), pp. 59–77.

[39]   Theodore J. Mock and Arnold Wright. "An exploratory study of auditors' evidential planning judgments". In: *Auditing; Sarasota* 12.2 (1993), p. 39.

[40]   Theodore J. Mock and Arnold M. Wright. "Are audit program plans risk-adjusted?" In: *Auditing: A Journal of Practice & Theory* 18.1 (1999), pp. 55–74.

[41]   Luc Quadackers, Theodore J. Mock, and Steven Maijoor. "Audit risk and audit programmes: archival evidence from four Dutch audit firms". In: *European Accounting Review* 5.2 (Jan. 1, 1996), pp. 217–237.

[42]   Sridhar Ramamoorti, Andrew D. Bailey Jr, and Richard O. Traver. "Risk assessment in internal auditing: a neural network approach". In: *Intelligent Systems in Accounting, Finance and Management* 8.3 (1999), pp. 159–180.

[43]   Nitin Singh, Kee-hung Lai, Markus Vejvar, and T. C. Edwin Cheng. "Data-driven auditing: A predictive modeling approach to fraud detection and classification". In: *Journal of Corporate Accounting & Finance* 30.3 (2019), pp. 64–82.

[44]   Carolyn A. Strand, Sandra T. Welch, Sarah A. Holmes, and Steven L. Judd. "Developing Student Abilities to Recognize Risk Factors: A Series of Scenarios". In: *Issues in Accounting Education* 17.1 (Feb. 1, 2002), pp. 57–67.

[45]   Adam M. Vitalis. "Business risk and audit risk: An integrated model with experimental boundary test". PhD thesis. United States – Wisconsin: The University of Wisconsin - Madison, 2012. 162 pp.

[46]   Michael Werner and Nick Gehrke. "Identifying the Absence of Effective Internal Controls: An Alternative Approach for Internal Control Audits". In: *Journal of Information Systems* 33.2 (June 1, 2019), pp. 205–222.

[47]   Arnold M. Wright and Jean C. Bedard. "Decision Processes in Audit Evidential Planning: A Multistage Investigation". In: *Auditing: A Journal of Practice & Theory* 19.1 (Mar. 1, 2000), pp. 123–143.

[48]   William F. Wright. "Client business models, process business risks and the risk of material misstatement of revenue". In: *Accounting Organizations and Society* 48 (Jan. 2016), pp. 43–55.

[49]   Shen Yin, Steven X. Ding, Xiaochen Xie, and Hao Luo. "A Review on Basic Data-Driven Approaches for Industrial Process Monitoring". In: *IEEE Transactions on Industrial Electronics* 61.11 (Nov. 2014), pp. 6418–6428.