Leiden University

ICT in Business & Public Sector

Continuous Financial Monitoring using Data Analytics in SMEs

Name: Dominic Jahangier
Student-no: S2118548

Date: 5/9/2020
Status: 1.0 Final

1st supervisor: drs. J.B. Kruiswijk
2nd supervisor: dr. W. Heijstek

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

PREFACE

The thesis before you, Continuous Financial Monitoring using Data Analytics in SMEs, is written to fulfill the graduation requirements for the degree of Master of Science in ICT in Business at Leiden University. It was made under the supervision of drs. Bas Kruiswijk and dr. Werner Heijstek. Baker Tilly, the company where I have been granted a temporary position, provided me with the insights and data to write this thesis. This thesis was written during a turbulent time where the COVID-19 caused a lockdown and made it hard to gather the appropriate data, and more importantly, keep the necessary focus. I find this thesis an appropriate conclusion to the ICT in Business master's program.

I would like to take this opportunity to express my deepest gratitude to everyone who has helped me through this process. Foremost, my first supervisor, Bas Kruiswijk, who has helped me from the very beginning. His inspiring lectures and guidance helped me to get from loose and empty ideas to a practical research topic, approach, and result. I would also like to thank Werner Heijstek, my second supervisor, for his feedback near the end of the process, which allowed me to sharpen up the research even more and allowed me to think more out of the box. My gratitude goes out to the research participants who took time out of their busy schedules to help me gather the necessary data. Also, my supervisors from Baker Tilly, Jan-Willem van Essen, Michiel Boers, and last but not the least, Remco Jansen, have gone to great lengths to guide and support me throughout this process. Finally, I thank my best friends Irfan Yuta, Rajesh Lale and Malik Samnani, my favorite study-partner and girlfriend Manju Patil, and my family, who helped me to stay focused throughout the entire masters program and supported me to finish this thesis. We did this together.

Dominic Jahangier
Den Haag, September 5th, 2020

ABSTRACT

Introduction

Although much research has been done on the theory of applying Continuous Financial Monitoring, concrete implementations have never been researched and described. Also, approaches of where to start, with which processes, and what to test in terms of data have not been researched.

This research is focused on developing a practical implementation model for Continuous Financial Monitoring using data analytics within small to medium-sized enterprises. The research question is: How can continuous financial monitoring using data analytics be implemented in small to medium-sized enterprises?
As a result, a reference enterprise architecture is created that describes the layers that are required for continuous financial monitoring using data analytics: processes, matching controls, data, the applications where this data is coming from, and the systems that hold the data and perform the analytics.
The scope of this research is trade organizations and especially the processes procurement and sales, as well as general conditional processes regarding IT management.

Methods

Firstly, a literature study regarding financial monitoring and data analytics was performed to create a basic understanding of the topics and their components. Additionally, a literature study on reference architectures was performed in order to specify which components are required and what tools can be used to develop one.

Secondly, interviews have been held with Accountants and IT auditors in order to retrieve processes, matching controls, required data, and applications. Also, an interview with a data analytics expert was done to gather additional information regarding data analytics setups.

Thirdly, a reference architecture is developed based on the gathered information from the interviews and literature.

Finally, a multiple case-study was performed to test the possibility of implementing the reference architecture in two small to medium-sized enterprises with various IT systems.

Results

The interview results have shown to be very consistent, and a reference architecture was developed. All architectural components have been implemented as required from the literature review.

Validation & Conclusions

The validation showed that the reference architecture is accurate and is implementable within the two out of three cases. In contrast, one case cannot use the architecture due to infrastructural limitations. It can be concluded that Continuous Financial Monitoring using Data Analytics can be implemented in SMEs using the developed reference architecture.

TABLE OF CONTENTS

1. INTRODUCTION

The operating environment of organizations is becoming more complicated because of social and technological developments. The environment is described as VUCA: volatile, uncertain, complex, and ambiguous (Bennett & Lemoine, 2014). Also, technological developments have created a data-intensive environment in combination with a real-time-economy; decisions have to be made rapidly (M. G. Alles, Kogan, & Vasarhelyi, 2008; Chan & Vasarhelyi, 2011). These developments have caused management and stakeholders to prefer real-time information, and especially real-time financial statements, which are necessary to make responsible, high-quality, and timely business-critical decisions that improve the organizational resilience in the VUCA environment. Organizational resilience considers the ability to detect, anticipate, adapt, and learn from environmental changes (Lee, Vargo, & Seville, 2013). Concluded can be that management and stakeholders operate their business in a changing environment, in which decisions are made more rapidly and based on real-time financial statements.

The information that directors, managers, employees, and other stakeholders within a company base their decisions on must have its integrity assured (Flowerday & Von Solms, 2005). Companies operate in increasingly competitive environments where their information resources play a crucial role in achieving their strategies and objectives (Flowerday & Von Solms, 2005). Information resources should continuously, near real-time, be monitored in order to be assured (have a certified certainty) that the information is correct (Ezzamouri & Hulstijn, 2018).

Financial Monitoring (FM), continuous monitoring, and continuous auditing are techniques that were initially developed for financial auditing. However, we are more often starting to see the use of those techniques for conformance checking (Elgammal, Turetken, van den Heuvel, & Papazoglou, 2016), contract management (Christiaanse & Hulstijn, 2013), and business process improvements (Sonnenberg & Brocke, 2014). In order for FM to work, essentially, the data on which FM is being performed needs to be valid, and this needs to be tested on continuous bases as well. There is a need for continuous IT assurance: ensuring the availability, integrity, authentication, confidentiality, and nonrepudiation of data and the IT environment (Sosin, 2018).

In the world of financial auditing, an audit is performed by an auditor that provides assurance to the board, management, and investors of an organization regarding the extent to which business operations are managed (Flowerday & Von Solms, 2005). This includes the adequacy of risk management systems and information (financial) systems (IS). IT auditing is mostly used during financial statement auditing. The purpose of a financial audit is to enhance the degree of confidence of intended users in the financial statements (IFAC, 2009). During an audit, financial statements and transactions are being tested on whether they represent the current state of the organization correctly. These days, most financial information is being managed using integrated financial solutions such as Enterprise Resource Planning (ERP) systems and accounting software suites (Barta, 2018; Chan & Vasarhelyi, 2018). An auditor will base conclusions on data (evidence), which often comes from IT systems. In order for an auditor to rely on this data, he needs to be sure that it is valid, authentic, and not tampered with. Therefore, IT assurance is crucial. Information Technology audits are being performed since

1977 (Ruthberg & McKenzie, 1977). IT audits involve examining all IT business processes and data that integrate with an organization's financial systems (Carlin & Gallegos, 2007).

The audit of IT systems can be divided into two fields of IT controls: IT general controls and IT application controls (Palmas, 2011). IT controls can be tested by analyzing the data that impacts the control and validate whether it matches the standard or not; Data Analytics is the modern way to do this (Ghasemaghaei, Hassanein, & Turel, 2017).

Zakir and his associates defined data analytics as a way of extracting value from massive volumes of information (Big Data) (Zakir, Seymour, & Berg, 2015). The data to be analyzed is not just database-driven data anymore. Instead, it includes documents, images, audio, video, and many other contents from various sources. These large sets of unstructured data are being referred to as big data (Zakir et al., 2015). Big data is also described as data that includes the three V's; high-volume, high-velocity, and high-variety data (Gandomi & Haider, 2015). Therefore, Big data will enhance the result of analytics, "the general rule is that the larger the data sample, the more accurate are the statistics" (Russom, 2011).

By combining data analytics and the financial systems used in an organization, financial monitoring (FM) can be achieved (Bănărescu, 2015; Cao, Chychyla, & Stewart, 2015; P. Yudowati & Alamsyah, 2018). The added value of FM has extensively been researched (Chan & Vasarhelyi, 2011; Rezaee, Elam, & Sharbatoghlie, 2001); however, concrete implementations have not, since existing research is focusing on implementation frameworks only and has never actually tested those. An implementation of FM would be based on the specific architecture of an organization. Because FM would mainly test the processes, data, applications, and technology within an organization's financial administration department, these elements would need to be defined and mapped. A concrete implementation of financial monitoring would contain a combination of processes and matching controls, data entities to test the controls and IT systems to enable the actual monitoring. Performing this test of the processes, data, applications, and technology automated and continuously would result in continuous financial monitoring (CFM).

For defining relationships between processes, data, application, and technology within an enterprise, enterprise architecture is a common tool. For the development of a model that represents an entire class of organizations, this can be done in the form of the more abstract reference architecture, which combines multiple enterprise architectures. (D. Chen, Doumeingts, & Vernadat, 2008) Also, reference architectures are widely used for solutions to general multi-organization problems as it can be used to define a generalized approach. Or where a general problem is at hand over multiple companies, a reference architecture can be used to deduct a generalized version of that problem.

1.1. Significance

The topic of financial monitoring (FM) has been researched, and theoretical approaches have been described as stated in the introduction. However, research regarding the actual application of FM has never been done. Also, the existing financial monitoring research focuses on large enterprises solely (Chan & Vasarhelyi, 2011). This research will focus on the practical application of FM in a controllable but significant group of organizations (SMEs). No research regarding the application of FM, nor theoretical nor practical, has been done within

SMEs. Also, little research has been done where data analytics is being considered as an approach to perform continuous financial monitoring (Cao et al., 2015). A gap in previous research is also the lack of a thorough description of what the components in a financial monitoring environment would consist of.

1.2. Research Question

This research will try to describe the combination of Financial monitoring and Data Analytics in small to medium enterprises. And this should be performed in a continuous and automatic manner. The research question is:

> **RQ: How can continuous financial monitoring using data analytics be implemented in small to medium-sized enterprises?**

In order to answer the research question, certain research steps are required. Those are described in the methods section.

1.3. Research Scope

Financial monitoring (FM) is mostly related to accounting standards and complying with regulations accordingly, as described in the previous chapters. This research will not focus on complying with standards; however, it will use the methodology and controls of auditing as a basis for financial monitoring. In order for continuous financial monitoring to comply with audit standards, future research regarding the requirements for auditing in combination with the proposed solution in this research should be done. Therefore, the proposed solution should be adapted to comply.

Organizations can have similar core business processes and are therefore grouped in typologies. As financial monitoring regards business processes, logically, organizations with a similar set of processes should be taken into account for this research. As the scope for this research, a specific type of organizations will be researched: trade organizations. This type is chosen because of the simplicity of the process and also because the process is represented in a substantial amount of organizations in The Netherlands (Kamer van Koophandel, 2019). When researching more different organizations from other typologies, those processes would be more complex and different. The topology will be researched within SMEs. Larger enterprises have often business processes which are far more detailed and more complex than the ones within SMEs. Within SMEs the core processes are often defined more clearly. Also, SMEs represent the biggest segment of roughly 20% of the businesses in The Netherlands (Kamer van Koophandel, 2019) which allows this research to define a broad applicable conclusion.

A reference architecture is a tool to define multiple organizations and their general outline, also regarding business and IT integration. When talking about multiple organizations in general, a reference architecture is a means to do this. This research will try to define a reference architecture, with a specific focus on gathering and combining all components on a high level. Specific designs within components will not be made throughout the design as they might be subjective to the studied cases. Examples may be defined. A reference architecture is a helpful tool to answer the research question because it is a model which can be tested in other studies.

1.4. Research Setting

This research was conducted in collaboration with experts from accounting firm Baker Tilly. The research set-up is meant to be generic, but most respondents, as well as studied cases, will be supplied by Baker Tilly. Since the interviews will not regard Baker Tilly employees, but more their clients whom are very different, this does not limit the research. The business processes, as well as applications, are mostly different per organization. Nevertheless, this point will be mentioned in the limitations as well.

1.5. Research Method

A research method is a strategy of inquiry that moves from the underlying physiological assumptions to research design and data collection (Myers, 1997). Financial monitoring could be described as the process of testing the financial state of an organization. Automating that process by using IT (applications) would allow it to be executed continuously. Therefore, the implementation of FM can be defined as a process and a description of matching (software) components to technically implement the process.

This research will define a reference architecture for a proposed implementation of continuous financial monitoring. The definition and validation of the implementation of a continuous financial monitoring approach will fill a gap in the existing literature.

1.5.1. Research Steps

To enable the correct development of a Reference Architecture, this topic needs to be researched first (1). The results of this research step will define what information needs to be gathered from the research step regarding financial monitoring and data analytics in order to develop a Reference Architecture. The first step is to define the components that a Reference Architecture consists of.

The second step (2) is to gain insight into the working of a financial department and the controls that are typically used to monitor a financial department. Therefore, first, the organizational structure of SMEs in terms of processes, data, and infrastructure that regard the financial department should be researched. Secondly, the controls that are used to monitor the processes in a financial department should be defined.

The third step (3) is defining what a data analytics infrastructure looks like and what components are required in order to set up one. Also, the processes that are involved should be defined.

The data that was gathered during the first three steps should be analyzed and combined. The fourth step (4) is to combine the information about financial departments and processes, controls and data, and data analytics into a Reference Architecture.

The developed Reference Architecture should be tested. Therefore, the fifth (5) step is to validate if the architecture can actually be implemented within SMEs.

1.5.2. Methods

In this research, multiple methods are being used. The method per step is stated in the table below.

Table 1-1 Steps and corresponding methods in research

Step	Method
1: Define reference architecture components	Systematic Literature Review
2: Research financial department structure in SMEs, processes, controls, data, and infrastructure	Systematic Literature Review Expert Interview(s)
3: Research required components for data analytics	Systematic Literature Review Expert Interviews
4: Develop a Reference Architecture	Combining the results of steps 1, 2, and 3.
5: Validate the developed architecture	Qualitative multiple-case study through interviews

The purpose of collecting data using multiple methods and from various data sources is to cross-verify the findings (triangulation) (Myers, 1997).

The research methods to answer the research questions will be executed in the order are shown in figure 1-1. A more detailed description per item is given in the next sections.

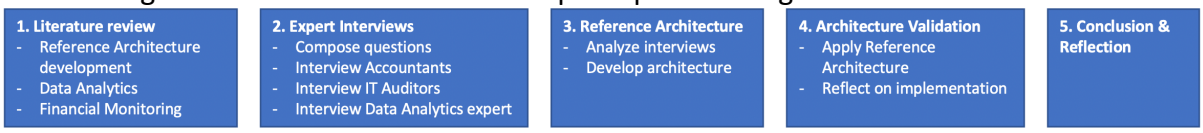


Figure 1-1 Research methods order

1.5.3. Literature review

The objective of the literature review is to give an insight into the three topics: reference architecture development, continuous financial monitoring, and data analytics. The literature review will be performed using a systematic approach.

The literature review will fully finish step 1 and will partly contribute to steps 2 and 3. It will provide insight into what information is missing regarding steps 2 and 3 and allow the development of a set of interview questions in order to discover the missing information.

1.5.4. Expert interviews

The objective of the expert interviews is to validate the data gathered during the literature review as well as discovering a practical approach and undiscovered details about the topics of financial monitoring and data analytics. The expert interviews will help to finish steps 2 and 3.

1.5.5. Reference Architecture development

The reference architecture will be structured as discovered in step 1. The results from step 2 and step 3 will be used to develop the reference architecture. The Reference Architecture should be a generally applicable blueprint.

1.5.6. Validation

The developed reference architecture will be validated using a multiple-case study. Meyers described that a case study is a well-suited mechanism for studying information systems in organizations as interests have shifted from organizational (process) rather than technical issues (Myers, 1997). That is true here as we validate the process in the proposed system. During the validation phase, three client cases will be selected based on the IT systems used. To validate as broadly as possible, the IT systems used should be different per case.

The validation will prove whether the reference architecture can be used in an organization. It will show if and how data can be accessed. More importantly, it will show what components are missing within the organizations to enable continuous financial monitoring.

1.5.7. Conclusion

The conclusion will discuss the developed reference architecture and the results of the model validation. Also, the limitations of the research and feature research possibilities will be discussed, and a reflection will be done.

1.6. Research Structure

This thesis consists of seven chapters:

1. The first chapter will outline the introduction of this research that consists of the background of the research, the significance and issue that it is trying to solve, the research questions, the specified scope and setting, and the approach for executing the research.

2. In the second chapter, the related literature in this research area and regarding those topics will be reviewed. The topics financial monitoring, data analytics, and reference architecture development will be discussed.

3. The third chapter describes the used methodology in order to gather the required data to answer the research question.

4. The fourth chapter summarizes and analyzes the gathered data using the methodologies from chapter three.

5. In the fifth chapter, the reference architecture will be developed.

6. The sixth chapter describes the validation of the developed reference architecture.

7. Finally, the seventh chapter discusses the conclusion of the research, the limitations and the recommendations for further research, and the reflection.

2. LITERATURE REVIEW

This chapter contains a review of relevant literature in the field in order to provide insights into the covered topics in this thesis. Also, it will provide the relevant body of knowledge for this research.

2.1. Approach

The objective of the literature review is to create insight into three topics:

- financial monitoring
- data analytics
- reference architecture development

The topic of financial monitoring will be reviewed in order to create a basic understanding of the topic. The topics data analytics and Reference architecture development will be thoroughly discussed.

A systematic review will be conducted using the libraries of Leiden University, Gartner, Research Gate, and Google Scholar. Also, the libraries containing previous Baker Tilly and Leiden University theses will be used to find relevant theses. There will be no scope limit in terms of age; the topic relevance does not degrade over time. A list of search terms will be defined, but as the search elopes, more terms can be used if references in papers are found.

2.1.1. Financial Monitoring

The field of financial monitoring consists of various topics. The directly linked topics will be covered in this study. The search terms that are used are:

- Financial Monitoring in SMEs
- Audit IT Controls
- Audit IT General Controls
- Audit Application Controls
- Continuous Monitoring
- Financial Monitoring
- Business Typologies
- Testing Application Controls
- Testing IT General Controls
- Continuous Auditing

2.1.2. Data Analytics

The field of Data Analytics is broad and consists of various components. For this study, the most-uses components will be covered. The search terms that are used are:

- Data Analytics definition
- Data Analytics components
- Big Data
- Business Intelligence
- Big Data Dashboarding
- Machine Learning
- Data Warehousing

2.1.3. Reference Architectures

For the topic of reference architectures, only peer-reviewed papers, and articles will be used. Also, practical approaches to architecture development and previously developed reference architectures will be covered. The search terms to be used are:

- Reference Architectures
- Enterprise Reference Architectures
- Reference Architecture model
- Reference Architecture development
- Reference Architecture model development

In addition to the named libraries, a separate Google search will be conducted to find practical Reference Architecture models.

2.2. Continuous Financial Monitoring

The objective of financial reporting is to provide information to management and stakeholders for resource allocation decisions (FASB, 2006). The usefulness of financial information relies on it to be on-time and free from material errors, omissions, and fraud. As described in the introduction, the real-time economy requires timely and reliable (financial) information for day-to-day business decisions.

Traditional auditing as a practice has not adapted to the demands from the real-time economy, which causes a lack of real-time assurance. This may be primarily attributed to the nature of the labor- and time-intensive manual (traditional) audit. These constraints limit audit frequency, an annual occurrence, which in turn could cause company management and stakeholders to make adverse decisions (Chan & Vasarhelyi, 2011).

This research uses the terms 'Financial Monitoring', 'Continuous Auditing', 'Continuous Monitoring', and 'Continuous Financial Monitoring'. The first step toward the understanding of these concepts is defining them.

2.2.1. Definitions

Continuous Auditing

The definition of an audit is: "the examination of the financial report of an organization - as presented in the annual report - by someone independent of that organization" (PWC, 2010). The purpose of an audit is "to form a view on whether the information presented in the financial report, taken as a whole, reflects the financial position of the organization at a given date" (PWC, 2010).

The concept of continuous auditing is developed by science, but there is no consistent definition defined. The most frequently cited definition is developed by a joint committee of the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA) (CICA & AICPA, 1999): "A continuous audit is a methodology that enables independent auditors to provide written assurance on a subject matter, for which an entity's management is responsible, using a series of auditors 'reports issued virtually simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter."

A few other definitions that are being used are described below.

Rezaee et al. (2002): "a comprehensive electronic audit process to provide continuous assurance, shortly after disclosure" (Rezaee, Sharbatoghlie, Elam, & McMickle, 2002).

Alles et al. (2008): "a concept to bring the audit process closer to the operational process, away from the backward-looking once-a-year examination of financial statements" (M. G. Alles et al., 2008).

Chan and Vasarhelyi (2011): "a technological innovation" (Chan & Vasarhelyi, 2011).

Vasarhelyi et al. (2012): "a progressive shift in audit process towards the maximum possible degree of audit automation as a way of taking advantage of the technological basis,

to reduce audit costs and increase audit automation" (Vasarhelyi, Alles, Kuenkaikaew, & Littley, 2012).

Rikhardson and Dull (2016): "the methodologies, processes, and technologies to enable continuous assurance on a specific subject matter" (Rikhardsson & Dull, 2016).

This results in a combined definition that will be used during this research:

> *"Continuous auditing is a concept to bring the audit process closer to the operational process by utilizing technology to the maximum and therefore enabling continuous 'audited' financial information."*

Continuous Monitoring

Continuous monitoring is defined as "a concept that ensures that policies, processes, business processes, and internal controls are operating effectively, in an automated manner" (Chiu, Liu, & Vasarhelyi, 2014; Vasarhelyi, Alles, & Kogan, 2004). It consists of the automated analysis of data on a continuous basis against a set of predetermined rules (controls) (Kuhn & Sutton, 2010). The demand for continuous monitoring is mostly driven by management and internal auditors in order to assess the effectiveness of internal controls (M. G. Alles et al., 2008; Chiu et al., 2014). And also by external audit, to detect errors, defalcations, and other breaches of the internal control system (Brown, Wong, & Baldwin, 2007).

Financial Monitoring & Continuous Financial Monitoring

The terms 'Financial Monitoring' and 'Continuous Financial Monitoring' are used interchangeably in research.

Financial monitoring is seen as a part of the general business monitoring systems used by management. Two definitions of financial monitoring in the context of this research are present.

Ezzamouri and Hulstijn (2018) describe financial monitoring as continuous auditing but without the auditing jargon and complexities in order to monitor and improve processes and procedures without providing formal assurance (Ezzamouri & Hulstijn, 2018).

Another weakly-supported article lists a definition of financial monitoring as "a systematic and continuous observation of financial activities and financial position of the object and their efficient assessment" (Oneshko & Ilchenko, 2017).

In this research, the definitions of continuous monitoring and financial monitoring will be combined, and the following definition will be used:

> *Financial Monitoring is the process of monitoring the financial processes and procedures within a company, based on testing defined controls resulting in the certainty of the financial information without providing formal assurance.*

In this research, a differentiation regarding the use of the word 'continuous' will be made. 'Continuous' will define Financial Monitoring on an event-driven or near real-time bases, whereas the frequency of analysis is daily (every 24 hours).

2.2.2. Current state of Continuous Auditing and Financial Monitoring

Theoretical implementations of Continuous Auditing (CA) have been described by various researchers (M. Alles, Brennan, Kogan, & Vasarhelyi, 2006; Ezzamouri & Hulstijn, 2018; Groomer & Murthy, 2018; Kuhn & Sutton, 2010; Sheldon, 2019). However, it was always kept theoretical and never practical in the sense that the full process was automated. The theoretical background of CA implementations can be divided into two parts: architecture and process.

Architectures

Early research regarding the implementation of Continuous Auditing (CA) suggested the implementation of Embedded Audit Modules (EAM's) into company systems such as ERP systems. These modules would be specially developed for systems and be implemented to respond to processes and transactions and alert when outliers were detected. Many research budgets have been spent on EAM's, but the approach was rarely used in practice in order to protect the company's ERP from excessive auditor interference. (Kuhn & Sutton, 2010)

Later research suggested another implementation for CA: EAM Ghosting. System "ghosting" essentially defines the creation of a copy of the company's ERP system. This copy would include all working data and system settings. On that copy (or ghost), queries could be executed in a separate environment without the risk of affecting ongoing transactions. It can be argued that the continuous creation of copies of the systems is very resource-intensive and not appealing for IT personnel/management to implement. (Kuhn & Sutton, 2010)

An alternative architecture, the Monitoring Control Layer (MCL), is viewed as the next stage of CA/CFM architectures. MCL connects the CA systems using middleware to company systems such as ERP or banking systems and extracts data. The main elements of the MCL architecture are: (1) data capture layer; (2) data filtering layer; (3) relational storage; (4) measurement standards layer; (5) inference engine; (6) analytic layer; (7) alarms and alerting layer; and (8 reporting platform. Essentially, the CA system would have a simple user interface and an underlying database and exist outside the company network (at the external auditors' facilities). The CA system receives periodical data as requested by the auditor and processes this against a predefined set of rules. Outliers and other alerts would be pushed to a dashboard and be visible to the external auditor and optionally the company management. This architecture was proven during a case study at a large enterprise. (Kuhn & Sutton, 2010; Vasarhelyi et al., 2004)

Continuous Auditing (CA) requires an IT infrastructure with data processing, data storage, and data visualization capabilities (Brown et al., 2007).

Process

The described process towards Continuous Auditing (CA) starts with the formalization of existing audit procedures (control testing) for automation. Procedures might have to be reengineered. Secondly, data that is necessary to test the controls has to be formalized and standardized. Data should be in a consistent format. Subsequently, data collection should be automated, and data transport should be arranged. Next, internal control policies should be formalized in order to support the testing of control violations. In essence, CA is the

continuous testing of process controls. (M. Alles et al., 2006; Chan & Vasarhelyi, 2011; Chiu et al., 2014; Vasarhelyi et al., 2012)

2.2.3. Application Controls and IT General Controls

As described in the introduction, an audit is performed by an auditor who provides assurance. This assurance is mostly based on information that comes from IT systems such as ERP systems, financial systems, and banking systems. In order to be able to rely on these systems, they have to be audited as well; this is mostly done by an IT auditor who has a technical background. (Barta, 2018; Chan & Vasarhelyi, 2018)

Carlin et al. (2007) describes the IT audit process as "the examination of the control structure of an organization's business processes, which may or may not be entirely computerized, to validate the organization's information assurance practices (Carlin & Gallegos, 2007). The audit of IT systems can be divided into two fields: IT general controls and IT application controls (Palmas, 2011).

1. IT general controls test the fundamental components of the IT organization: data center and network operation, system software acquisition and change management, program change, access security, application system acquisition and development, and maintenance. Those general controls are a fundamental part of the IT infrastructure (Barta, 2018).

2. IT application controls are controls that relate to specific information systems. These can be specific authorization rules for an Enterprise Resource Planning (ERP) system, for instance (Barta, 2018).

Organizational business processes have their individual controls that can be tested. The control is unique to each business process, and since every process functions differently, controls can differ per business or even per business unit. However, some process controls can be standardized. Processes such as sales and procurement operate roughly the same in every company.

2.2.4. Conclusion

To conclude, the definition of Continuous Financial Monitoring (CFM) that will be used within this research is:

> *Financial Monitoring is the process of monitoring the financial processes and procedures within a company, based on testing defined controls resulting in the certainty of the financial information without providing formal assurance.*

Therefore, the monitoring does not have to comply with formal auditing standards, as this will be a topic for further research. However, auditing techniques such as the testing of IT General Controls and Business Process Controls will be used within this research and the proposed solution. The focus will lay on CFM by an external organization. This research will not focus on Application controls since they are highly organization and application-specific.

Since the scope of the research is trade organizations with the processes procurement and sales, during the interviews, the Business Process Controls and IT General Controls, as well as the data that is needed in order to analyze and test the controls should be gathered.

2.3. Data Analytics

Analytic has been a term that is involved in almost all of the different business variety. It is the process of analyzing information using statistical and mathematical data analysis that clusters, categorize, and gives the prediction to the future trend of the business in a particular domain (Gartner, 2020). Zakir and his associates defined data analytics as a way of extracting value from massive volumes of information (Big Data) (Zakir et al., 2015). The data to be analyzed is not just database-driven data anymore. Instead, it included documents, images, audio, video, and many other contents from various sources. These large sets of unstructured data are being referred to as Big Data (Zakir et al., 2015). Big data is also described as data that includes the three V's; high-volume, high-velocity, and high-variety data (Gandomi & Haider, 2015). Therefore, Big Data will enhance the result of analytics, "the general rule is that the larger the data sample, the more accurate are the statistics" (Russom, 2011).

Data analytics can also be defined as 'techniques, technologies, systems, practices, methodologies, and applications that analyze critical business data' (H. Chen, Chiang, & Storey, 2012). It can help organizations to create a more thorough understanding of their business operations, market, and more. Also, the use of data analytics tools can help firms to sense changes in their operating market and, through this, improve their response speed and efficiency: increase their agility (Roberts & Grover, 2012). Additionally, data analytics can help to identify opportunities by analyzing abundant data (H. Chen et al., 2012). The use of data analytics has become essential for many organizations, as it is an important tool in modern competitive environments (Ghasemaghaei et al., 2017).

Data analytics can serve three purposes: descriptive – to understand what happened, predictive – to predict what may happen, and prescriptive – to simulate and test possible decision outcomes (Ghasemaghaei et al., 2017). Shao et al. add diagnostics – identifying why something happened or is currently happening – as a fourth purpose (Shao, Shin, & Jain, 2015).

2.3.1. Big Data Analytics adoption

As Louis Columbus reported, Big Data adoption in enterprises rose from 17% in 2015 to 59% in 2018 (Columbus, 2018). The report stated that the Telecommunications, advertising, and insurance is the industries that consider Big Data is critical for their businesses. Furthermore, the study showed that the Financial industry is eager to adopt Big Data architecture and technologies. Moreover, another research stated that visual analytics software is the Big Data technology that has the most frequently adopted by organizations. The adoption of visual analytics is supported by several data resources such as online portal content, RFID data, GPS data, POS data, and transactional data of the company (Raguseo, 2018).

2.3.2. Big Data analytic benefit and barriers

As Raguseo (2018) argued the benefit of big data analytics is to improve the data management in all of the industrial sectors. While, the risk that may appear in Big Data analytics adoption

is the privacy of the data that is stored in the Big Data infrastructure (Raguseo, 2018). Similar studies show that 325 respondents ensure the following benefit of the Big Data analytics adoption: Better targeted social influencer marketing; More numerous and accurate business insights; Segmentation of customer base; Recognition of sales and market opportunities; and Automated decisions for real-time processes. However, the study also reported the barriers that might be encountered of the Big Data analytics adoption such as: "Inadequate staffing or skills for big data analytics; Overall technology adoption cost; Overall Lack of business sponsorship; Difficulty of architecting big data analytic system; Current database software lacks in-database analytics" (Russom, 2011).

2.3.3. Data Warehouse

The need to store and manage data from multiple sources at a central location can be argued back to the exponential growth of available data, big data, over the past few years. Data warehouses emerged, and data from one or more separate sources were integrated into a central repository. A fundamental property of data warehouses is that it is highly structured (Campbell, 2015). Unstructured data has also been growing, which required a new form of storage, Data Lakes. Data lakes demand little to no structure, making them applicable for semi- and unstructured data (Campbell, 2015).

Data Warehouse

In a data warehouse, data is stored that is modeled and/or structured. Before data is loaded into the data warehouse, it must be transformed into the required structure. This is called schema-on-write (Campbell, 2015).

In data warehouses, the term data marts cannot be missed. Data marts are 'retail outlets' of the data warehouse, which provide data in a specific format for analysis by end-users (or data consumers). Data marts are mostly tailored to the needs of a specific user group or decision-making task. Data marts can be stored in tables or views on the central data warehouse. (Moody & Kortink, 2000)

Generally spoken, there are two approaches for data warehousing: top-down and bottom-up. In the case of the bottom-up approach, data marts are created first, and afterward, these data marts are combined to a single data warehouse. The top-down approach works the other way around: first, a data warehouse is created, and afterward, data marts are extracted for specific groups of users. (Rouse, 2015)

Data Lake

Data lakes contain all data from systems, whereas in data warehouses, only data with predefined use is stored. Data can be stored in (nearly) untransformed state, and all data types are supported. Data lakes store all data that might not have a purpose today but can be used tomorrow or in the future. (Campbell, 2015)

2.3.4. Data Management

At the foundation of data analytics lies data management. Data management entails the extraction, cleaning, transformation on, and storage of data. Data essentially comes from a source-system and should be transferred in a proper format to the destination system. The destination system is often a data warehouse. A data warehouse (DW) is a collection of

multiple tools and technologies that are aimed at enabling faster decision making. A data warehouse differs from traditional databases in the subjects of size – can store much data, volatility – content can rapidly change, normalization – can store data in various formats, and subject orientation – data from various types can be stored. (El-Sappagh, Hendawi, & El Bastawissy, 2011)

The data source can vary a lot, and data from those sources can have various formats. In order to perform analysis on this data or gain structural insights from the data, it should be conforming to the needed format. In order to transform data from source to needed format (in the data warehouse), ETL is needed. The process of ETL consists of three steps: where (1) data is extracted from various data sources in various formats, (2) moved to the data staging area(operational data storage DSA) where it can be transformed and cleansed, and then loaded into the data warehouse. The ETL process is displayed in figure 2-1. A more thorough description of the ETL steps is described below. (El-Sappagh et al., 2011)

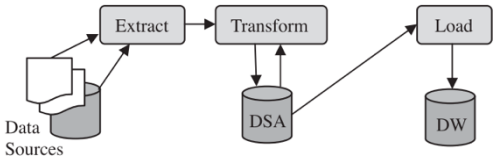


Figure 2-1 ETL schema

Extraction
The goal of the ETL extraction step is to connect to the different data sources, understand the data structures of the sources, and knows how to transfer the data from the sources to the operational data store (DSA).

The extraction step also defines the interval at which data is extracted. Possible is that data is only extracted at full during the initial extraction from the data source. After that, only incremental extraction can be performed if the data source supports this. Incremental data extraction is called changed data capture (CDC).

Transformation
The goal of the ETL transformation step is transforming data by cleaning and conforming it to ensure the data from the sources is correct, complete, consistent, and unambiguous. This may also include combining data from different sources. The transformed data is then again stored in the DSA.

Loading
The goal of the ETL loading step is to input the data (which should already have the correct format) into the data warehouse. No logic should be needed during this step.

In order for data to be processed, it should be transferred to the data storage first. If the data storage and data warehouse are on a different location than the data sources, this may be a time-consuming task when data volumes increase. A proposed solution for this is to bring the analytics (code) to the data and only transport processed data. (Kaisler, Armour, Espinosa, & Money, 2013)

2.3.5. Data Privacy

Privacy is a multi-faceted concept, and the term itself has been the subject of various definitions and refinements. The term Data Privacy is used increasingly in the Data Analytics industry. It can be defined as ‘all aspects of access to data’ (Chaudhuri, 2012). In the scope of

this research, data privacy will be a very important aspect. Data will entail users with their roles and rights, financial transactions, financial statements, and more classified and business-critical data.

2.3.6. Data Visualization

Data visualization has become very important nowadays. In order to be able to understand and interpret data and data analytics outcomes, these need to be visualized in an understandable format. This is mostly done by using dashboards which compile key metrics in an easy to interpret interface (West, 2012).
Gartner (2020) has redefined their Magic Quadrant for Analytics and Business Intelligence Platforms. The top three ranking platforms are Microsoft PowerBI, Tableau, and Qlik. The choice for the platform is dependent on organizational contracts rather than platform capabilities, as most key capabilities are equal. (Richardson, Sallam, Schlegel, Kronz, & Sun, 2020)

2.3.7. Conclusion

To conclude, data should be extracted from the source systems, and ETL should be performed in order to store the data in a useful format in the data warehouse. Therefore, data transport from the source system to the data warehouse is essential. Tooling that can be recognized as essential to perform data analytics is data extraction, data transportation, data transformation, data loading, data warehouse, and data visualization tooling. The tools can be defined as applications.

When data sizes increase, data could be preprocessed before transportation to the data source.

2.4. Reference Architectures

The most widely used definition of architecture is the one of ISO/IEC 1471:2000: “The fundamental organization of a system embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution”. This standard was overruled by ISO/IEC 42010:2011, in which it is slightly modified: “(system) fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution”. Those definitions are mostly the same.

A Reference Architecture (RA) is an abstract solution for the design of systems in a specific domain (The Open Group, 2016). A U.S. Department of Defense paper defined the concept of reference architectures as “an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions” (Office of the DoD CIO, 2010). The architecture defines the infrastructure as well as the skills and procedures needed for the implementation of the respective systems (Niemann, 2008). Additionally, the Reference Architecture can contain heuristics to determine timelines, risks, and development costs, which are based on previous experiences (Niemann, 2008). It is a more high-level model of what it references, used as a basis for education and explaining standards to non-specialists (The Open Group, 2018).
A Reference model is different from a Reference Architecture; it constitutes organization-specific configurations (The Open Group, 2011). Reference Architectures often target specific groups of organizations (use-cases) such as the Dutch government (NORA) or for municipalities (GEMMA). Reference Architectures are not prescriptive; organizations can choose whether to (partially) implement them.

A possible pitfall of Reference Architectures could be that they are too high-level. On the other hand, being too specific while looking at a broad scope might also cause problems. The chance of organizations not willing to use the architecture because it is too specific then increases. Being non-prescriptive does not have to be a bad thing but leaves the possibility for organizations to only partly adopting an architecture (or not even at all), decreasing the aimed result. Therefore, Reference Architectures are mostly used to guide the design of a more focused and specific architecture by a smaller group of organizations or even a single one.

2.4.1. Structure and Components

A fair amount of literature regarding Reference Architectures is available; however, most of it regards software engineering. The lack of maturity of the term “Reference Architecture” can be seen by the small number of articles and books regarding the topic from a system engineering perspective. A result of the small amount of research is that there is no standardized way of developing or even structuring a Reference.

Cloutier et al. (2011) defined that a Reference Architecture (RA) captures the essence of existing architectures, and the vision of future needs and evolution to provide guidance to assist in developing new system architectures. This definition tries to enforce an RA to be based on existing architectures; however, in practice, this is not always possible. For certain applications of RA, it should be the starting point for the implementation of a system and the foundation for improvements to the RA. (Cloutier et al., 2010)

The actual content of a Reference Architecture may differ a lot between architectures. Some only consist of sets of principles to follow and terminology to be used, thus focusing primarily on conceptual integration. Others also include standards for messaging and communication, and even reference models for specific types of organizations or sectors. Applicative integration is also a focus in that case. Technical descriptions or application descriptions as part of a technical integration should not be part of a RA. (Greefhorst, Grefen, Saaman, Bergman, & Beek, 2008) Cloutier et al. (2011) described that a Reference Architecture should address the technical architecture, business architecture, and customer context. (Cloutier et al., 2010)

Greefhorst et al. (2008) has reviewed multiple existing architectures and concludes that an RA mainly describes a product, so a blueprint of a piece of the information architecture. Distinguishable parts are (Greefhorst et al., 2008):

- Data – description of relevant data (corporate data model).
- Process – description of relevant processes (workflow model).
- Communication – a structure of interfaces between and systems and with external systems.
- Platform – description of abstract technology classes used for the implementation of the system.
- Organization – description of the organizational structure used to implement system usage.

One of the reviewed architectures, for implementation of a specific enterprise portal, consists of a few leading principles, a blueprint of relevant layers and components including a description of each layer and component, and a translation of the reference architecture towards the implementation of an actual portal which makes a selection of relevant layers and components. (Greefhorst et al., 2008)

The Open Group Architecture Framework (TOGAF) is a widely used Enterprise Architecture framework, originally developed in 1995 by The Open Group. The most current version of it is TOGAF 9.2, which was released in 2018. TOGAF describes three architectural layers (combining Data and Application Architecture) (The Open Group, 2018):

- Business Architecture – the business strategy, governance, organizational structure, and key processes.
- Data Architecture – the structure of an organization's logical and physical data assets and data management resources.
- Application Architecture – the individual applications, their functions, interactions, and relationships to the core business processes.
- Technology Architecture – the software and hardware capabilities that are required to support the deployment of business, data, and application services.

Research by Boer et al. (2011) describes that a Reference Architecture consists of principles and models. Principles are general rules and guidelines which are intended to be maintained for a long time and rarely change. These direct the way an organization fulfills its mission and support. Each principle consists of at least a name, theorem, rationale (motivation), and implications it has. The models are complementary to the principles and can be developed using the ArchiMate modeling language. ArchiMate can be used to describe the architectural components of an enterprise architecture. It describes the information, behavioral and

structural aspects over three layers: the business layer, application layer, and technology layer. (Boer, Schijvenaars, & Oord, 2011)

Remarkable is that a layer that is described by The Open Group (2018) and Boer et al. (2011) is missing in the research by Greefhorst et al. (2008). This regards the application layer, which describes application components and functions. Combining the works of three researchers, the architectural layers would be:

- Business Architecture – a description of the organizational structure and key business processes.
- Data Architecture – a description of relevant data required for the key processes.
- Application Architecture – a description of the individual applications with their functions and relationships to the key business processes.
- Technology Architecture – the technology classes, components, and capabilities that are required to support the applications, data, and business processes.

Summarizing the existing research, one could conclude the following definition:

> *"A Reference Architecture is an abstract description of a product that describes the customer context, business architecture, data and application architecture, and technical architecture in which it can be implemented. Therefore, a set of leading principles and models are defined that describe the organization, process, data, communications, and platform(s)."*

2.4.2. Architecture Modeling

Lankhorst (2004) introduced a modeling language specifically designed for reference (enterprise) architectures named ArchiMate (Lankhorst, 2004). It was adopted by The Open Group and introduced in 2016 (The Open Group, 2016). ArchiMate is still under development; the current version is 3.1. Both ArchiMate and TOGAF are maintained by The Open Group but not explicitly developed for each other. However, they are naturally compatible because they both use business-, application- and technology layers.

Modeling a Reference Architecture with different layers and components can become a large and complex whole of models and principles (Lankhorst, 2009). Therefore, the concept of views and viewpoints were developed. The IEEE 1471 standard (Maier, Emery, & Hilliard, 2001) defines a view as "a representation of a system from the perspective of a related set of concerns" and a viewpoint as "a specification of the conventions for constructing and using a view; a pattern or template from which to develop individual views by establishing the purposes and audience for a view and the techniques for its creation and analysis". So, to summarize, a viewpoint is an angle, and a view is what you see from that angle.

A viewpoint is defined by describing the intended stakeholder(s), his concerns, and the content metamodel. A (content) metamodel is an abstraction of the model that defines the characteristics of the model, and it describes the collection of used elements and relations within a model to improve model understanding (Gerber, Kotzé, & Van Der Merwe, 2010).

2.4.3. Conclusion

A Reference Architecture (RA) is mostly described as a generally applicable architecture that is applicable to multiple organizations or even industries. It should be based on proven implementations and architectures. For this research, a Reference Architecture will be developed but not based on proven implementations. It will be the first Reference Architecture for the implementation of continuous financial monitoring. The architecture will be validated during the multiple-case study, and it will be a first version which has to be adapted as new insights are gained.

The definition, as stated in chapter 2.4.1, will be used throughout this research.

The Reference Architecture will distinguish the four layers; Business-, Data, Application, and Technology Architecture, and will be modeled using the ArchiMate language.

3. RESEARCH APPROACH

This chapter describes the used research methodology for the interviews, for the development of the reference architecture, and for the validation of the architecture.

Based on the financial monitoring literature review, extra information regarding financial monitoring is needed since the literature cannot directly be used for the development of the architecture. The literature review is used to develop specific interview questions. The results for those questions will be used for the model development.

Based on the data analytics literature review, interview questions can be formulated to gather missing information. Both the literature and the interview results will be used for model development.

The reference architecture literature review presents a method of developing the reference architecture, which can directly be used for model development.

An overview of the abovementioned approach is displayed in Figure 3-1 where blue block represent literature, yellow. Blocks represent interview questions, white blocks represent interview results and green blocks represent viewpoints (parts of the final reference architecture) that are being developed.

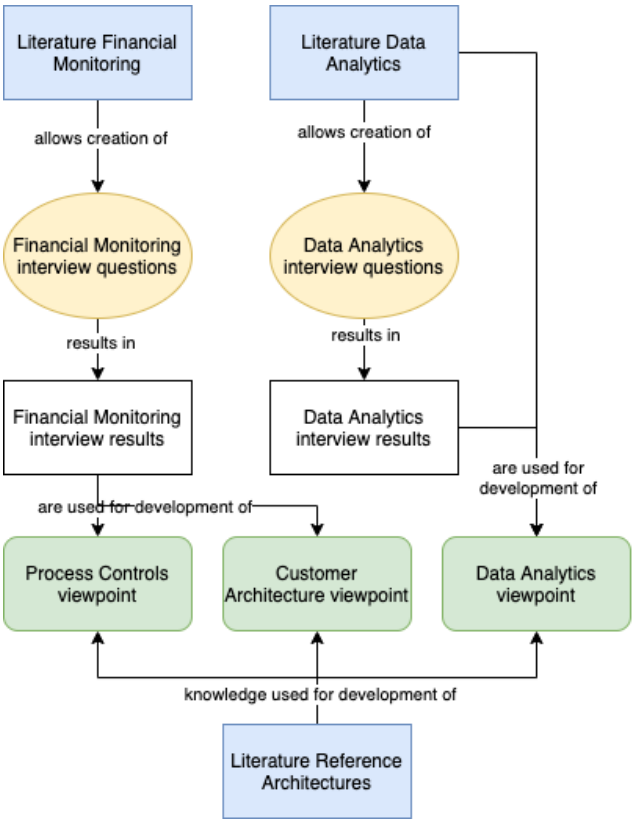


Figure 3-1 Research approach for model development

3.1. Interviews

The expert interviews regarding financial departments and process controls (steps 2 and 3) will be with three registered accountants (RA) and two IT auditors (ITA) from Baker Tilly. The participants represent the working field of accountancy. Also, an accountant from the Professional Competence Center (VAL) within Baker Tilly will be interviewed as a form of validation. He is chosen because he works independently from the three registered accountants.

The expert interview regarding Data Analytics (step 4) will be with a data analytics expert (DA) with experience regarding data-management, and technical implementation. The interviewee will be from within Baker Tilly. Because this study does not specifically focus on the best way of implementing data analytics, but more on how to implement it, only one approach will be researched.

The literature review regarding reference architectures concluded that the layers business, data, applications, and technology are distinguished in the model. Therefore, these layers should be modeled using data from the literature reviews as well as from the interviews.

The literature review regarding continuous financial monitoring concluded that it is necessary to gather an overview of processes, IT general controls, and business process controls as well as the data that is needed in order to analyze and test the controls. Since the processes are already defined in the research scope, only the departments, controls, data, applications, and technology should come from the interviews.

The literature review regarding data analytics defined the processes (steps) and certain data to perform DA but does not define applications, and technology. Therefore, these will have to come from the interviews in order to complete the reference architecture.

3.1.1. Interview Questions – Accountants

The interview questions with the accountants are the broadest since accountants keep the overview of the entire process at the customers. The accountant will be asked to keep in mind a customer case and answer questions, where necessary, based upon that customer. The interviews are with interviewees from the same firm but the customer cases (topics) are completely different.

First, general questions regarding the background, current role, and experience with the topics and scope will be asked. These will define the reliability of the answers. Also, a question towards the actual topic will be asked (q5), in order to gain a better general understanding of the topic and to identify possible items that are missing during the literature review. The remaining questions regard controls, data, applications, and general information. The questions to be asked are:

1. What is your background regarding education?
2. What is your current role within Baker Tilly?

3. What is your experience regarding continuous financial monitoring / automated controls?

4. Do you have customers of the type of trade organization? How many?
5. What is your approach to testing the purchasing and sales processes within a company?
    a. What controls do you use?
    b. How do you get to these controls?
    c. Are these controls unambiguous across your different customers?
6. What data is required to test each control? Which systems does this data come from?
7. Is there any added value to test these controls more than once a year (e.g., on continuous bases)?

3.1.2. Interview Questions – IT auditors

The interview questions for the IT auditors are partially based on the results from the interviews with the accountants. The interviews with the accountants should result in several controls with matching data entities. First, general questions regarding the background, current role, and experience with the topics and scope will be asked. Then, IT auditors will be asked what the IT General Controls and processes are, with the matching data and applications where the data comes from. Lastly, they will be asked from what applications the data for the controls that the accountants named come since they have a better understanding of the application landscape at customers.

1. What is your background regarding education?
2. What is your current role within Baker Tilly?

3. Do you have experience with continuous financial monitoring / automated controls?

IT General Controls

4. What are the IT general controls that you test during an audit?

5. Which sets of data do you ideally need per control to test it fully automatically?
6. From which systems does that data come? Type or specific systems per data entity.

Application Controls

7. The accountants have listed a number of controls that are used to test the purchasing and sales process, as well as data entities. From which specific systems do the following data entities come?
    1. Purchase orders
    2. Receipt receipts
    3. Invoices
    4. Accounts payable master data
    5. Payment lists
    6. Payment Powers
    7. Product prices

3.1.3. Interview Questions – Data Analytics expert

The interview questions for the data analytics expert are based on the literature review and are related to the experience of the expert, ways of executing the processes that came from the literature review, technical and legal limits regarding the process, and used tools. First, general questions regarding the background, current role, and experience with the topics and scope will be asked.

1. What is your background regarding education?
2. What is your current role within Baker Tilly?

3. Do you currently extract data automatically from customer systems and load it into a data warehouse?

Data Extraction

4. What are the common ways of extracting data from the customer environment? What is the process?
5. Are there any limits to this?

Types of data & privacy

6. Is it allowed to extract data from customer systems?
7. What data can be extracted to the internal Baker Tilly DWH?
8. Should the data be anonymized?
9. How long can the data be stored at the Baker Tilly data warehouse?

Current tools

10. What tools are currently in use at Baker Tilly for Data Analytics and relates tasks?
    8. Source systems
    9. ETL tooling
    10. Data Warehouse system

3.1.4. Interview Questions – Validating accountant

The questions for the validating accountant will be a combination of the questions for Accountants and the questions for IT auditors. The notes from the interviews with those will be added during the interview in order to validate what was said before.

1. What is your background regarding education?
2. What is your current role within Baker Tilly?

3. Do you have experience with continuous financial monitoring / automated controls?

Accountants

4. The accountants have noted a certain approach [add-in audit approach step], what is your view on this?
    a. The controls that have been listed are [add-in controls], do you agree with those? Are they all relevant?
    b. Are there any controls missing in the list?
5. Do you see the added value to test these controls more than once a year?

IT auditors

6. The most important controls, named by the IT auditors were [add in controls], what is your few on this?
    a. Did I miss any controls?

3.1.5. Interview processing

All interviews will be held in the native language of the interviewee and transcribed in that language. In the transcript, the interviewer will be labeled as SP1, and the interviewee as SP2. The transcript will be translated to English using the Google document translator. All English transcripts will be added as Appendix A in this research. The interviews will be coded by adding unique keys (#-tags) to relevant answers that regard any of the components as described in chapter 2 or that regard the research questions. This will allow traceability from the processed results to the original interview transcripts.

The interviews with Accountants and IT auditors will lead to specific information. Therefore, a structured format will be used to describe the interview results. The format will mainly be a table that describes the control with their respective process, required data, and system.

The interview with the data analytics expert will be unstructured as there is no expectation of results. Therefore, the answers will be summarized in the structure of the interview questions.

The validation interview will be ordered per control where the response from the validator per control is captured. Additional notes will be unstructured.

Finally, the results of the interviews with the Accountants, IT auditors, and the validator will be combined. Controls that are 'IT General', or were named by multiple interviewees, or by the validating interviewee will be used. Combining the results will also fill in gaps in the interviews. Because gaps can be filled, extra information that was missed during a specific interview will not be asked again, unless it was not mentioned by any of the other interviewees.

3.1.6. Interviewees

In order to preserve privacy, only a brief profile of each interviewee is described, and each interviewee has a unique identifier. This is described in Table 3-1.

Table 3-1 Interviewee profiles

Interviewee ID	Interviewee	Profile
RA1	Registered Accountant 1	Economics and post-master Accountancy at Tilburg University. A senior manager in the audit practice at Baker Tilly.
RA2	Registered Accountant 1	Post-master AA and RE training. Manager in the audit practice at Baker Tilly.
RA3	Registered Accountant 1	Master in Business Administration and Tax Law at Erasmus University, RA post-master. Manager in the audit practice at Baker Tilly.
ITA1	IT auditor 1	Master Accountancy at the University of Amsterdam, RE post-master. Manager and IT auditor at the IT Advisory department at Baker Tilly.
ITA2	IT auditor 2	Bachelor in Business IT and master IT audit, RE.

		Senior IT auditor and consultant Data Analytics at the IT Advisory department at Baker Tilly.
DA1	Data Analytics 1	Bachelor in Business IT Manager Data Analytics solutions at the IT Advisory department at Baker Tilly.
VAL1	Professional Competence Center 1	Post-master RE. Director at Professional Competence Center at Baker Tilly

3.2. Reference Architecture development

As described in chapter 2.4, a Reference Architecture describes the customer context, business architecture, and technical architecture of a system. Therefore, principles and models will be defined that describe:

1. the organizational structure – the organizational components that are involved in financial monitoring,
2. processes – the processes within a typical financial department,
3. controls – the controls that are used to test a process,
4. data structure – the data that is needed to test the controls,
5. application functions – the functions that various applications perform to handle the data and execute the processes,
6. and infrastructure – the systems that contain the data and the systems that will analyze the data to test the controls.

Based on the interview results, three viewpoints will be defined and modeled using the ArchiMate modeling language.

The first viewpoint describes the customer architecture, which entails the organizational structure (1), business processes (2), supporting data (4) and applications (5), and technology (6). This will be modeled for the processes as defined in the research scope and for the processes that come from the interviews.

The second viewpoint describes the process controls, which again entails the processes (2) and the matching controls (3). In addition, the data that is required to test the controls (4) and the applications where the controls come from (5) are described.

The third viewpoint describes the data analytics architecture, which allows the automated testing of the controls.

This results in a reference architecture that enables continuous financial monitoring.

3.3. Validation

To verify and test whether the reference architecture can be implemented, the researcher will apply the architecture to three cases. The architecture should be implementable for the enterprises, as stated in the scope. Therefore, three company cases were selected that represent a variety of technologies and systems used. Even though three case studies cannot represent the entire scope, it will provide valuable insights on whether the architecture can actually be implemented. The study per-case will consist of two steps.

The IT auditor responsible for the case will be interviewed. Questions will be based on the components of the reference architecture, where the IT auditor will be asked to help to fill the blueprint with the IT components from the case. The main purpose of this interview is to retrieve if and where the necessary data can be found in the client infrastructure and if it is possible to extract this data using data analytics techniques. Also, questions are asked to test if data can be continuously accessed and how this data should be accessed.

The specific validation questions are defined in the validation chapter itself as they are highly dependent on the reference architecture.

3.3.1. Validation Cases

In order to preserve the privacy, the cases and corresponding interviewee are described, and each case and interviewee has its unique identifier. The cases have been selected based on the company data analytics maturity, interviewee availability, and use of technology. The cases are described below.

The first case, CS01, regards a company that uses a Navision Business Central ERP system. An IT auditor (ITA03) with much practical knowledge is interviewed for this case. This company has no experience with data analytics.

The second case, CS02, regards a company that uses an SAP ERP system. On top of that, also, data analytics is being performed at this client. A manager, IT auditor (ITA04), who works closely with the company, is interviewed.

The second case, CS03, regards a company that uses a Proteus ERP system. An employee of that company, EMP01, with a lot of knowledge regarding the infrastructure, is interviewed for this case.

4. INTERVIEW RESULTS

This chapter describes the results of the interviews based on the transcripts and notes (#-tags) that have been added. This is based on the topics that are being covered in the interviews. This chapter concludes with an aggregate of the interviews with RA1, RA2, RA3, ITA1, ITA2, and VAL1.

As described in chapter 3.1.5, all interviews are transcribed, and answers that match the questions are labeled with #-tags. Per interview, a summary table describes the interviewee, general notes were added for data that came from the interviews but was not directly an answer to a question, a structured format was used for the analysis of the answers to the interviewed questions, and a list of used #-tags was added for reuse and traceability. All detailed results can be found in 'Appendix A Detailed Interview Results'.

The interviews with accountants (RA1, RA2, RA3), IT-auditors (ITA1, ITA2), and the validating accountant (VAL1) are formatted per control in a structured table. The interview with the data analytics expert (DA1) is summarized.

The next chapters describe the interviews per set of interviewees. Chapter 4.5 contains the conclusion, which is an aggregated table of structured data from the interviews with the accountants, IT auditors, and validating accountant.

4.1. Interviews with Accountants

The interviews with the accountants gave a broader understanding of their clients' company structure, processes, and more. All accountants agreed that controls could only be properly automatically tested if the IT general controls are sufficiently functioning (RA1 note 1, RA2 note 3, RA3 note 2). Continuous financial monitoring will save a lot of time during the audit and is the next step in auditing (RA2 note 4). It will also allow benchmarking to be done over multiple companies to spot trends (RA3 note 4).

The processes, controls, data, applications, and technology, as described by the accountants, can be found in chapter 4.5.

4.2. Interviews with IT auditors

The interviews with the IT auditors added more in-dept information on top of the broader information the came from the accountants. Both auditors named the exact same controls and data that was required. Also, more information was given regarding applications where the data that was named by the accountants comes from.

Companies often have a mix of various systems where data comes from. These can be any combination of ERP and financial systems (ITA1 note 4). Each system has its own user list. Users can be stored in multiple systems as well, which makes them hard to trace manually (ITA2 note 4). Also, since data in systems may be labeled differently, it can be hard to match (ITA2 note 6).

The processes, controls, data, applications, and technology, as described by the IT auditors, can be found in chapter 4.5.

4.3. Interviews with Validating accountant

The validating accountant was asked to review the answers as given by the accountants and the IT auditors. He could recognize the named controls and also didn't miss controls. Additions to fill in gaps were done and included in the aggregated results table. The list of controls was complete, according to him. The control VAT was not found useful by him since it tests something that never goes wrong.

The processes, controls, data, applications, and technology, as described by the validating interviewee, can be found in chapter 4.5.

4.4. Interview with Data Analytics expert

The data analytics expert described how data should be exported, the tooling that is being used, and some technicalities and privacy points of concern.

The needed data, tables, and fields for data analytics are defined based on the controls that will be tested. The way of data extraction is defined based on the system manuals and is always done manually by the customer. The data should be uploaded to a secure file share and from there is loaded into the data warehouse before being displayed on a Qlik Sense data analytics dashboard. This can be done with large amounts, such as 45 GB of data.

Only data that serves the purpose (predefined goal), data such as personal identification numbers, can be extracted. Mostly, a data retention policy of 365 days is being used.

It is important that the integrity of the data from the system to the data warehouse is maintained. The data has to come directly from the system, has to be recent, and cannot be tampered with.

For the tooling, Baker Tilly uses SmartExporter to export data from SAP, Huddle as a secure file share for data transfer, TimeXtender as a data warehouse, and Qlik Sense as a dashboarding tool.

A detailed analysis of this interview can be found in appendix A.

4.5. Aggregated Processes, Controls, Data and Applications

Since the results from the interviews with accountants, IT auditors, and the validating accountant have a structured format, these can be combined and put together. First, the lists of approaches and department structures have been combined.

A company mostly has the following departments that are linked to the financial department (RA1, RA2, RA3, VAL1):

- Finance department
- Warehouse department
- IT
- HR
- Procurement and Sales

Per business type (typology), there is a pretty standard list of controls that manage risks (RA3 note 1). However, some processes may be very organization dependent and specific, and it can be hard to define standardized controls, for example, the sales process (RA1 note 1).

As an approach to start an audit and define the controls, the following steps are executed (RA1, RA2, RA3, VAL1):

1. What is the business revenue model.
2. Define risks based on the revenue model.
3. Define the business processes.
4. Define relevant IT systems / IT landscape.
5. Define controls.

Secondly, the structured tables containing the controls, processes, data, and applications have been combined. Only processes and controls that were named by multiple interviewees or specifically highlighted by the validation interviewee will be listed. Also, the processes and controls have been assigned an identified in the format of Pxx and Cxx; they have been ordered by the process. The control General access protection did not receive an identifier because it is a category and not a separate control. The descriptions of controls that are used in this chapter will be used as leading throughout the rest of this research. The detailed table of controls, including traceability to the interviews, can be found in Appendix B. A simplified version is shown in table 4-1.

Table 4-1 Simplified table of Processes, controls, and descriptions

Process	Control	Control Description
P01 Procurement	C01 Three-way-match	A purchase order should have a receiving receipt and invoice. Those three items should match and be tested by different people (segregation of duty).
	C02 Product pricing	The price of products on the receipt should match the price, as stated in the overlapping contract.
P02 Sales	C03 Turnover	The number of sales (Q) can be tested by the inventory at the end of the year, minus the inventory at the start of the year. In between, the number of sales and failure can be seen.
P03 Invoice payment	C04 Payment segregation of duty	Making a payment requires segregation of duties and has to be checked by at least ‘four eyes’.
P04 Update creditor master data	C05 Change creditor master data	Changing the data of a creditor (person or organization who receives money) requires segregation of duties and has to be checked by at least ‘four eyes.
P05 New employee	C06 New Employee	When a new employee joins the company, an account has to be set up. How is it ensured that he gets the right access (authorization).
P06 Employee new role	C07 Employee new role	When an existing employee gets a new function, his roles and rights should change as well. How is it ensured that his access is proper (authorization).
P07 Employee leaves	C08 Employee leaves	When an employee leaves the company, his access should be revoked (authorization)
P08 Manage general authentication	General access protection	Identification, Authentication, and Authorization

	C09 Identification	Which person does a user in the system represent. When you log in with a username, does that represent a person.
	C10 Authentication	How do you prove that you have that identity. Are password requirements proper.
	C11 Authorization	What can you do in the system. Roles and rights within the system.
P09 Update system	C12 Change Management	What changes in system configuration have been made and what software upgrades have been performed. What was the impact of those changes and how have they been tested to ensure the correct functioning of the system(s) and business processes.
P10 Manage backup and recovery	C13 Business Continuity	For businesses where IT is crucial in day-to-day operations, the continuity of these systems should be guaranteed by having proper backup and recovery measurements in place.

5. REFERENCE ARCHITECTURE

This chapter describes a reference architecture to implement continuous financial monitoring using data analytics. Therefore, the information from the interviews will be analyzed and translated into ArchiMate models. The approach for the development of the reference architecture is described in chapter 3.2.

Each section in this chapter represents a different viewpoint that addresses certain concerns for a specific stakeholder. These concerns and the viewpoint definition including the viewpoint metamodel are described in the chapters itself.

Chapter 5.1 describes the architecture of the customer. This viewpoint addresses the stakeholder Customer IT Architect.

Chapter 5.2 describes the process controls, required data, and applications where the data comes from. The viewpoint addresses the stakeholder Accountant.

Chapter 5.3 describes the proposed data analytics architecture at the accountant and addresses the stakeholder data analytics consultant. This proposed architecture is a result that allows the automated execution of testing of the controls that are defined in chapter 5.2 in order to achieve continuous financial monitoring.

The architectures will not contain any organization-specific information since the final result will be an abstract reference architecture. Also, detailed descriptions of elements such as processes will be minimized as much as possible.

5.1. Customer Architecture

This chapter models the viewpoint of the Customer IT architect.

First, the viewpoint and content metamodel are described (ch. 5.1.1). Next, the organizational departments and their interrelations are described and modeled, which will be used throughout the architecture (ch. 5.1.2). Then, the various processes are modeled in separate chapters (ch. 5.1.3 t/m 5.1.7). Finally, the general application interfaces and technology are modeled for the completeness of the viewpoint.

For the processes, the business and application layers are modeled per process. The interview results (ch. 4.5) describe several processes that are being tested. Some are named explicitly, and some are interpreted. Also, the matching systems are named. Those systems will be defined more abstractly and extracted into functions and grouped as application components.

5.1.1. Viewpoint description

The Customer IT architect is the stakeholder whose concerns are applications and their relation to the business (processes) and also the data that is going on and forth in and between those layers in order to execute the process.

The used objects in the ArchiMate models are described below.

Business layer elements

The group object represents an organizational department. The groups contain business actors who can execute various business roles.
An actor executing a business role can trigger (be assigned to) a business function (a group of business processes) or a single business process. A group of processes of a specific process can have multiple business (data) objects that are being used for reading and/or writing data. A business process can realize a business service that can be consumed by an actor in a specific role.

The interviews disclose the actors that are involved in the processes and the data that is important in order to test the associated process controls. To execute the controls, the process should at least work with several data entities. The population of some of these data entities happens inside of the process, by other actors. For this, services are defined.

The metamodel for this layer is displayed in Figure 5-1.

Application layer elements

A business process uses one or more services that are realized by an application function. Multiple application functions can be grouped into an application component. Those application functions (or entire application components) read and/or write to the application (data) objects that store data. When two or more applications (components) have to work together, an interface between those systems is defined.

Application functions are abstracted from the application descriptions by the interviewees. Those functions may, in turn, be grouped into application components again.

The metamodel for this layer is displayed in Figure 5-2.

Technology layer elements

An application node is placed at a specific location, either on-premise or in the cloud. In a node, multiple devices can be hosted, which expose technology services that can be used by application components for hosting.

The metamodel for this layer is displayed in Figure 5-3.

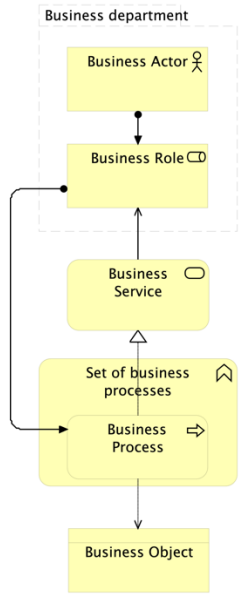


Figure 5-1 Business layer metamodel

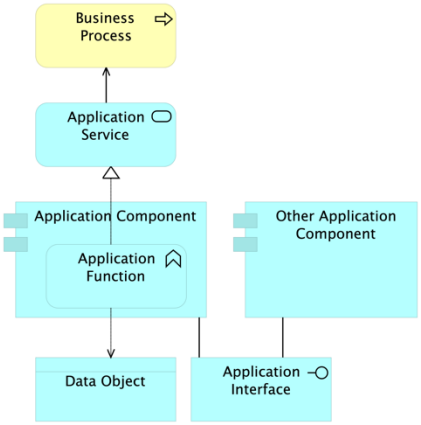


Figure 5-2 Application layer metamodel

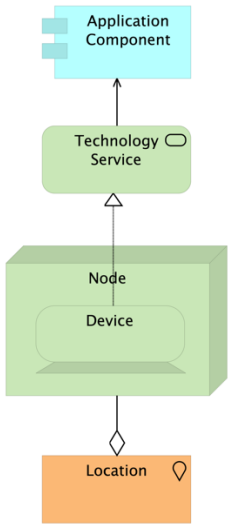


Figure 5-3 Technology layer metamodel

5.1.2. Organizational departments

The aggregated interview result (ch. 4.5) describes a few organizational departments:

- Financial department
- HR
- IT
- Warehouse department
- Procurement and Sales

These are modeled in Figure 5-4.

Administrative department

As per convention, HR and Financial administration are mostly part of the Administrative department. Therefore, an HR worker and Financial worker are defined as roles of an Administrative employee within the Administrative department.

Within controls, certain roles of departments are mentioned. The 'Change creditor master data' control states that at least two people are required to perform a payment data change. Therefore, two authorized to pay roles will be introduced.

IT department

The interviews with ITA1 and ITA2 described three IT General controls and, therefore, roles and responsibilities that should be present to manage those controls. We can distinguish a system administrator who maintains and updates systems such as the ERP system. Also, a change manager who approves the work of the system administrator as a 'second pair of eyes' is necessary. There is a responsibility to manage user accounts, roles, and rights in the system. This is defined in the access manager role. Lastly, the business continuity should be managed, and backups should be made and tested; this responsibility lies at the employee with the business continuity manager role.

Warehouse department

The control three-way-match requires a separate employee to register received goods; this is described by RA2. Therefore, the role of a goods receiver is defined as the role of a warehouse employee. This importance of this role can be seen by RA3 who mentioned it separately from the three-way-match.

Procurement and Sales department

The control product pricing is executed by a procurement worker, as stated by RA1, RA2, and RA3. Both RA2 and RA3 stated that the turnover (amount of sales) depends on the sales workers; this is defined as a role as well.

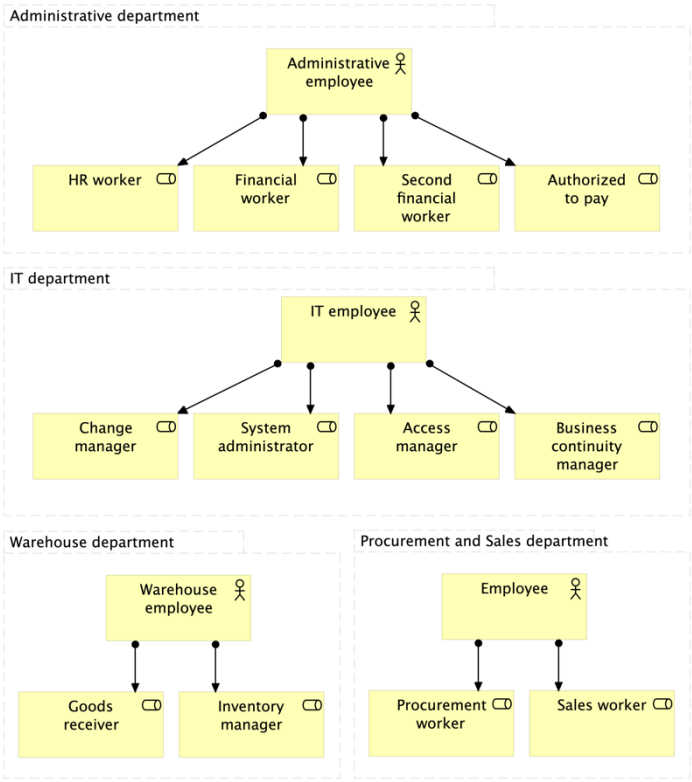


Figure 5-4 Organizational departments

5.1.3. Procurement process

The P01 procurement process can be described as the process of buying goods within an organization. The interviews (RA1, RA2, RA3) disclosed the people that are involved in the process and the data that is important in order to test the associated process controls. To execute the controls C01 and C02, the process should at least work with several data entities. The population of some of these data entities happens inside of the process, by other actors. For this, services have been defined. The procurement process with roles, services, and data is modeled in Figure 5-5. Note that the data entity 'invoice' is modeled as 'Purchase invoice' in order to avoid conflicts with the data entity 'invoice' in the sales process.

Appendix B and the interviews describe several specific systems for the procurement process. Those application functions with their services are modeled in Figure 5-6.

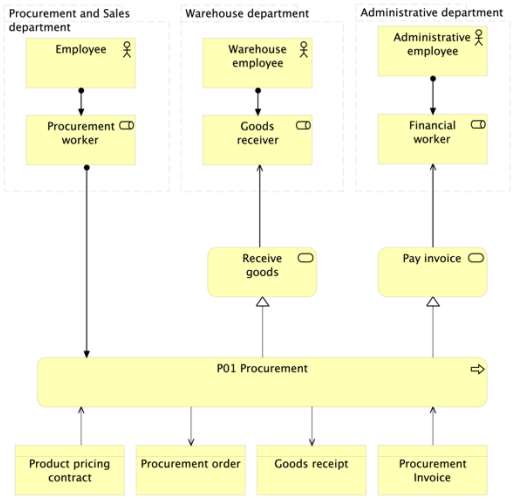


Figure 5-5 Procurement process - business layer

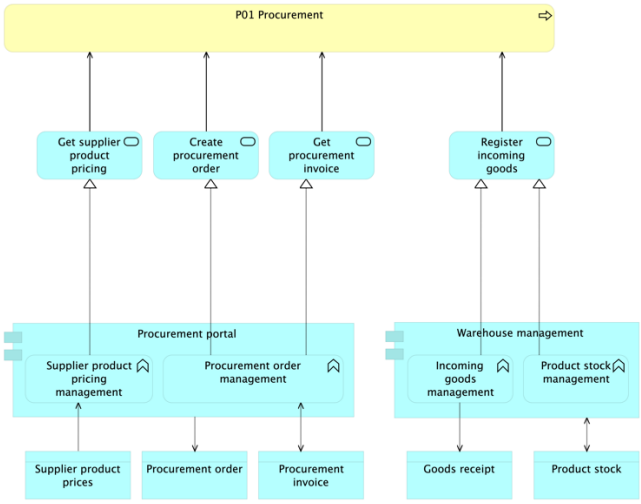


Figure 5-6 Procurements process - application layer

5.1.4. Sales process

The P02 sales process can be described as the process of selling goods to a customer. RA1 described this process as highly variable and depending on the organizational business model and sales strategy. Therefore, it was hard to generalize and define controls. RA2 and RA3 defined control C03 Turnover as a very helpful control. Because this process is hardly generalizable, it isn't modeled in detail, and only parts that support the control are modeled. The sales process with roles, services, and data is modeled in Figure 5-7. Figure 5-7 describes the application functions with services. Also, an interface between the two application components is modeled because bases on the application descriptions, they rely heavily on each other and have to work together.

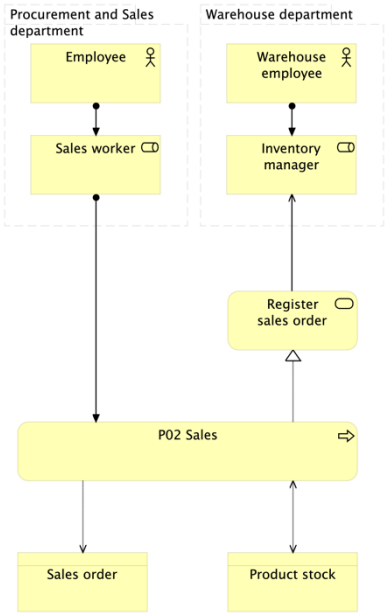


Figure 5-7 Sales process - business layer

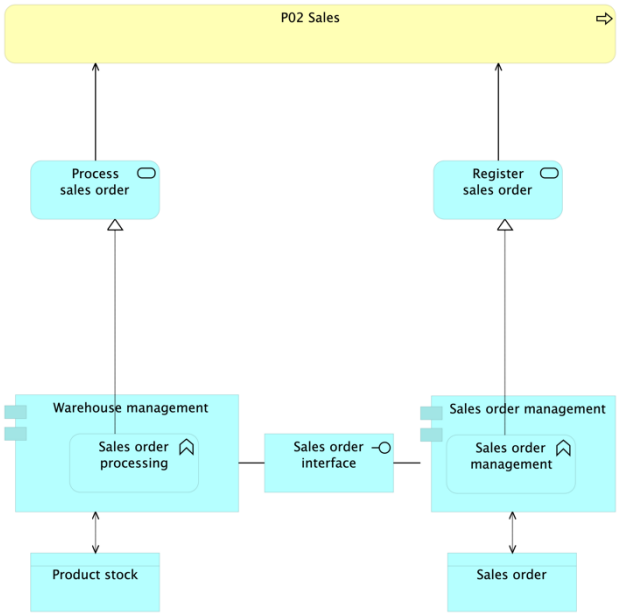


Figure 5-8 Sales process - application layer

5.1.5. Payment processes

The payment processes are two important processes, as stated by RA1, RA3, and VAL1. The P03 invoice payment process and the P04 update creditor master data process.

The invoice payment process can be described as the payment of an invoice. This process can be tested using control C04 payment segregation of duty as defined by RA1, RA3, and VAL1. This control tests that every payment is approved by at least two people and that the payment is linked to an invoice. Necessary data entities that should be matched are the purchase invoice and the bank transaction (payments), and also the involved employees in a transaction (invoice approval).

The update creditor master data process can be described as the alteration of creditor bank account numbers and making sure that no errors or fraud are involved. The control to test this process is C05 change creditor master data, as defined by RA1 and VAL1. The control tests that every change in creditor master data is approved by at least two people. Necessary data entities that should be matched are the creditor database and the data changes and approvals.

The payment processes with roles, services, and data are modeled in Figure 5-9. The application functions and services are modeled in Figure 5-10.

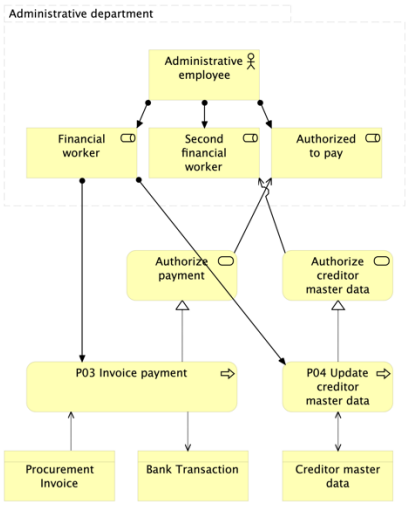


Figure 5-9 Payment processes - business layer

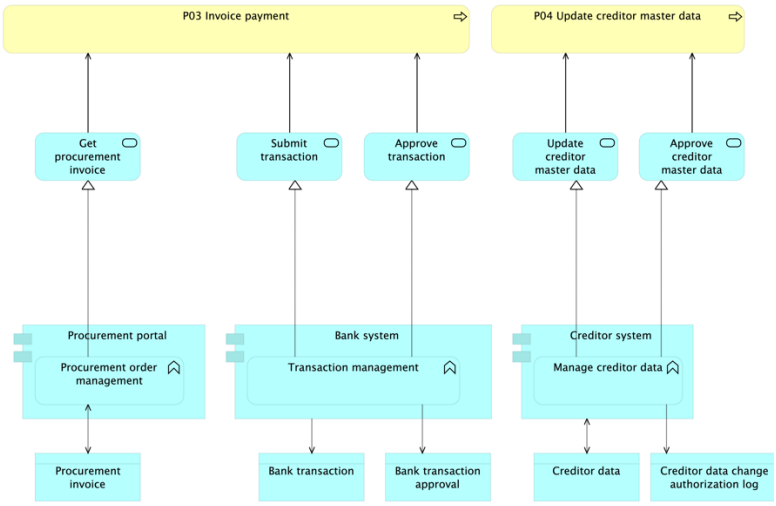


Figure 5-10 Payment processes - application layer

5.1.6. HR Employee Mutation

The HR process consists of three employee mutation processes. The process P05 is mentioned by both ITA1 and ITA2 as an important precondition of the General Access Protection controls. The additional processes P06 Employee new role and P07 Employee leaves were only mentioned by ITA1, as ITA2 expected these to be included in P05.

The P05 new employee process regards the onboarding of a new employee. The employee should get an IT account, and certain roles and rights should be assigned. What is important is how it is determined which roles should be assigned to this new employee and how this is authorized.

The P06 employee new role process regards an employee that gets a new role within the organization. The roles and rights of the IT account should be altered accordingly to the change.

The P07 employee leaves regards an employee leaving the organization. The IT accounts should be suspended correctly.

Necessary data entities that should be matched to test the controls are the HR employee directory, User changelogs, and IT user directory.

The Employee mutation processes with roles, services, and data are modeled in Figure 5-11. The applications and services are modeled in Figure 5-12.

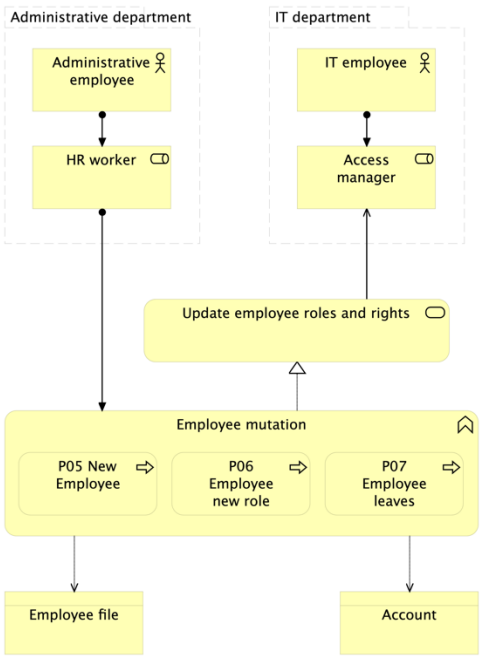


Figure 5-11 Employee mutation processes - business layer

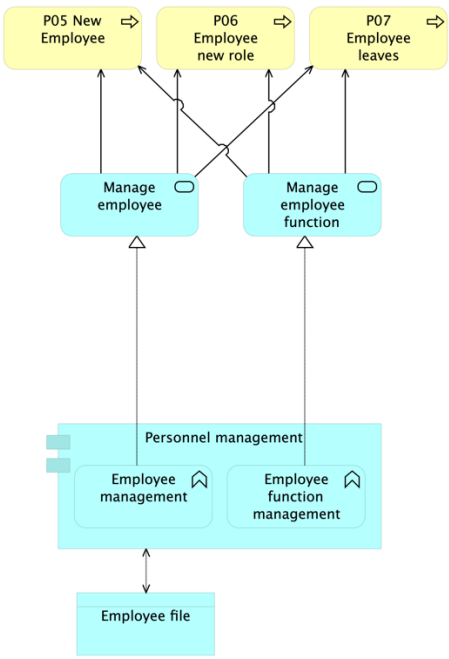


Figure 5-12 Employee mutation processes - application layer

5.1.7. IT General processes

The IT General processes are P08 Manage general authentication, P09 Update system, and P10 Manage backup and recovery.

The process P08 manage general authentication was mentioned by RA1, RA2, ITA1, ITA2, and VAL1. It regards the general management of accounts, roles and rights, and authentication policies. Creating, updating, and deleting user accounts and assigning the proper rights and roles to them. Also, ensuring that accounts have proper passwords set-up and, if possible, two-factor authentication. This process is modeled in Figure 5-13 and the application functions and services are modeled in Figure 5-14.

The process P09 Update system regards changing company systems. This can be updating a system to a newer release or changing system configuration parameters. Every system change should be tested properly and also be checked by a second person, in order to assure no errors have been made.

The process P10 Manage backup and recovery was mentioned by ITA1, ITA2, and VAL1 and regards assuring that all systems are properly back-upped and that possible recovery scenario's have been tested. This process has been noted as essential.

The General IT processes P09 and P10 with roles, services, and data are modeled in Figure 5-15. Not all data entities that are needed to test the controls are used within the processes. Therefore, those data entities have been modeled but are not linked to the processes. The applications and services are modeled in Figure 5-16.

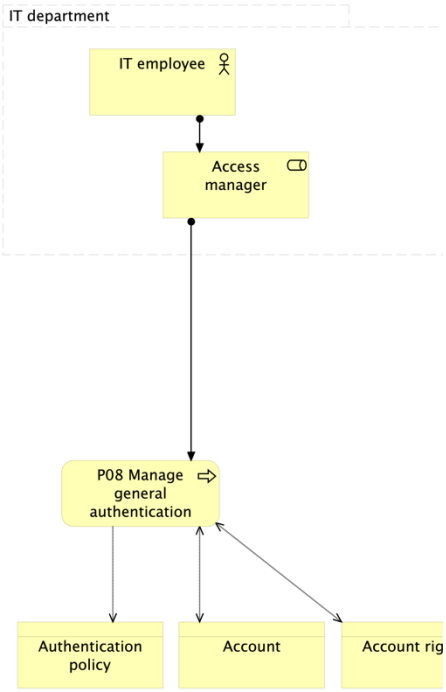


Figure 5-13 Manage general authentication process -business layer

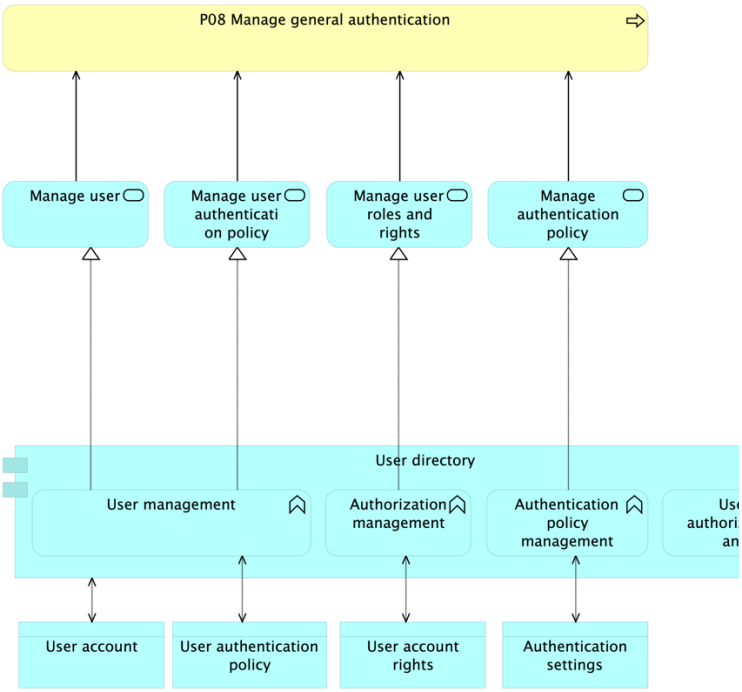


Figure 5-14 Manage general authentication process - application layer

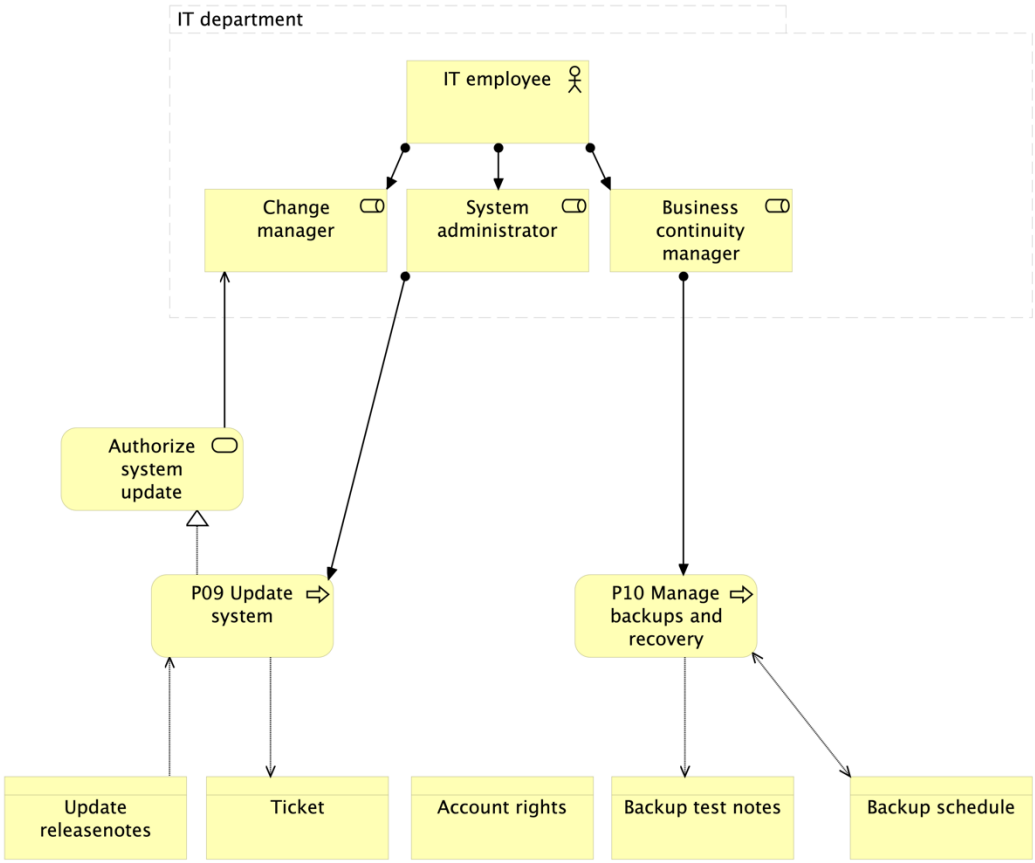


Figure 5-15 IT general processes - business layer

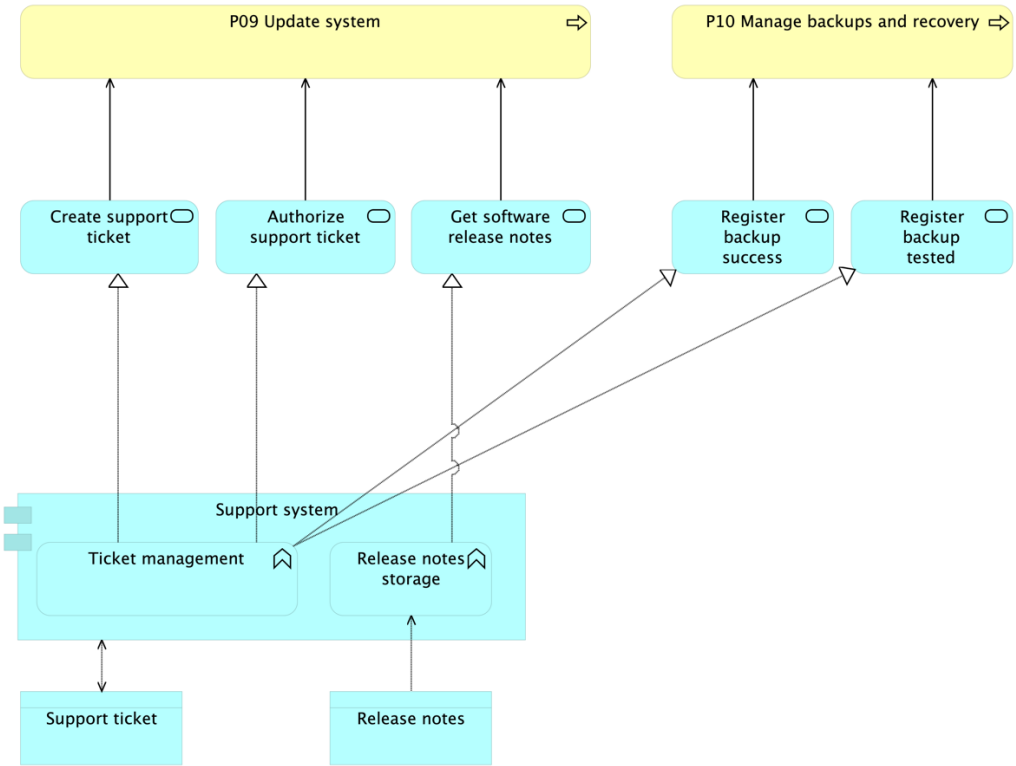


Figure 5-16 IT general processes - application layer

5.1.8. Application interfaces and Technology

All application components in the application landscape interface with the User directory application for authentication and authorization. Therefore, an interface is defined that can be used by other applications. This is modeled in Figure 5-17.

As intended for completeness, Figure 5-18 shows the technology layer. It is not relevant since the infrastructure is a service, and its functioning is irrelevant. What may be relevant, though, is where the infrastructure is hosted, either on-premise or in the cloud.

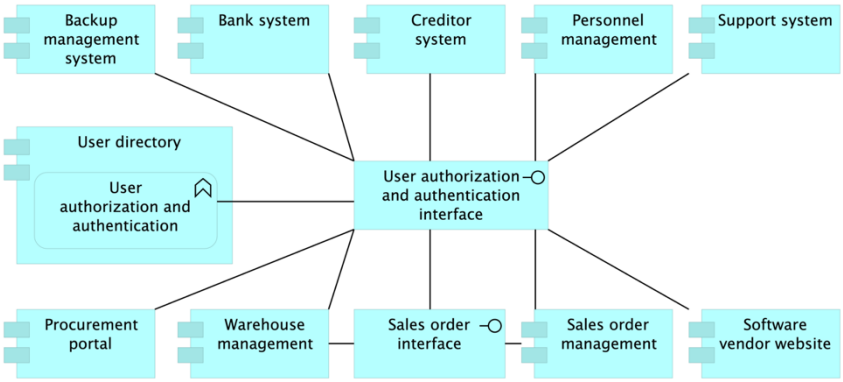


Figure 5-17 Authentication and authorization interface

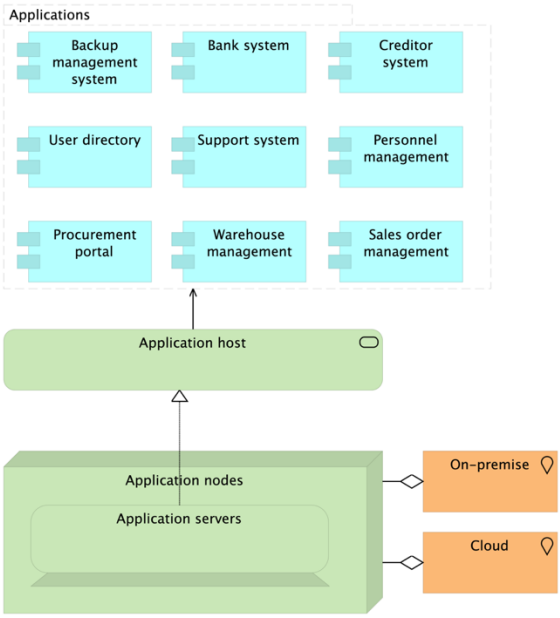


Figure 5-18 Technology layer

5.2. Process Controls Architecture

This chapter models the viewpoint of the Accountant.

First, the viewpoint and content metamodel are described (ch. 5.2.1). Second, the processes with their controls and required data and applications are described and modeled per process (ch. 5.2.2 t/m 5.2.7).

5.2.1. Viewpoint description

The Accountant is the stakeholder whose concerns are business processes and the matching controls that are necessary to test those processes. Additionally, the business objects and the applications that use those objects (linked to application objects) are essential as well. This is a newly defined viewpoint that shows data that is required to test a control.

The used objects in the ArchiMate models are described below.

Business layer elements

This viewpoint models processes as defined in chapter 5.1 as business processes. Those processes consist of one or multiple controls, which are modeled as business processes as well, with an aggregation relationship to the matching process. For each control, the business objects that are required to test the control are modeled.

Application layer elements

The business objects that are required for testing the controls have to come from applications. Therefore, the business objects are linked to application data objects. The application objects are, in turn, linked to application functions where the objects can be retrieved from.

The business and application layer elements are modeled in Figure 5-19. This viewpoint shows only static elements. Active elements such as services are out of scope.

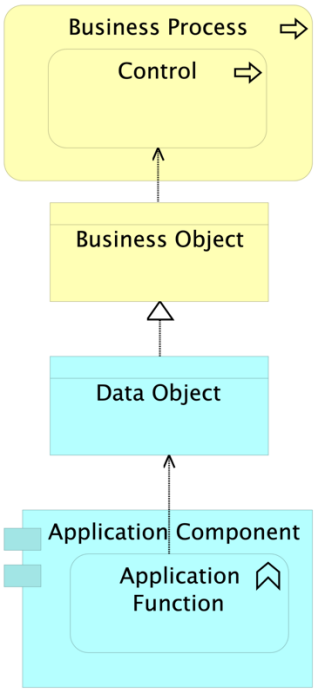


Figure 5-19 Process controls viewpoint metamodel

5.2.2. Procurement process controls

All interviewees, RA1, RA2, RA3, and VAL1, mentioned the control C01 Three-way-match as most important to test the procurement process. Also, RA1, RA3, and VAL1 mentioned the control C02 Product pricing as essential.

The aggregated interview results describe the Three-way-match as a control that tests if the steps in the procurement process are all aligned and executed by separate people (separation of concerns). A purchase order should have a receiving goods receipt and an invoice. Those three items should match and be tested by different people (segregation of duty). So essentially, those three data points should match and should be created or entered by three separate people. Necessary data entities that should be matched are the purchase order, the receipt that goods are received, and the received invoice that is paid.

The Product pricing control tests whether the price of goods that are purchased are as agreed in overlapping contracts. This ensures that no mistakes can be made, and no fraud can be committed by employees. Necessary data entities that should be matched are the received invoice and the contract that states the product prices.

Figure 5-20 shows the model of the process with controls and data entities.

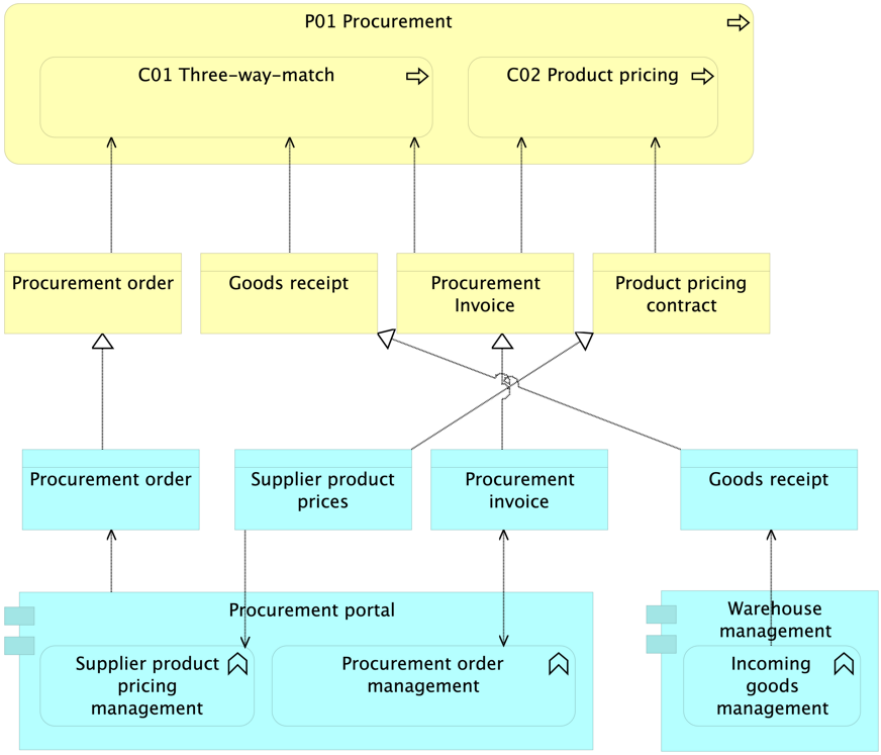


Figure 5-20 Procurement process controls

5.2.3. Sales process control

The Turnover control is based on the product inventory. The aggregated interview results describe that the number of sales (Q) can be tested by the inventory at the end of the year minus the inventory at the beginning of the year. In between, the number of sales and failure can be seen. This number (amount of sales) should be relatable to the amount of sales orders in a year. This can also be done throughout the year, as long as the inventory is managed properly. Necessary data entities that should be matched are the stock of products at the beginning and end of the period, and the sales orders during that period.

Figure 5-21 shows the model of the process with controls and data entities.

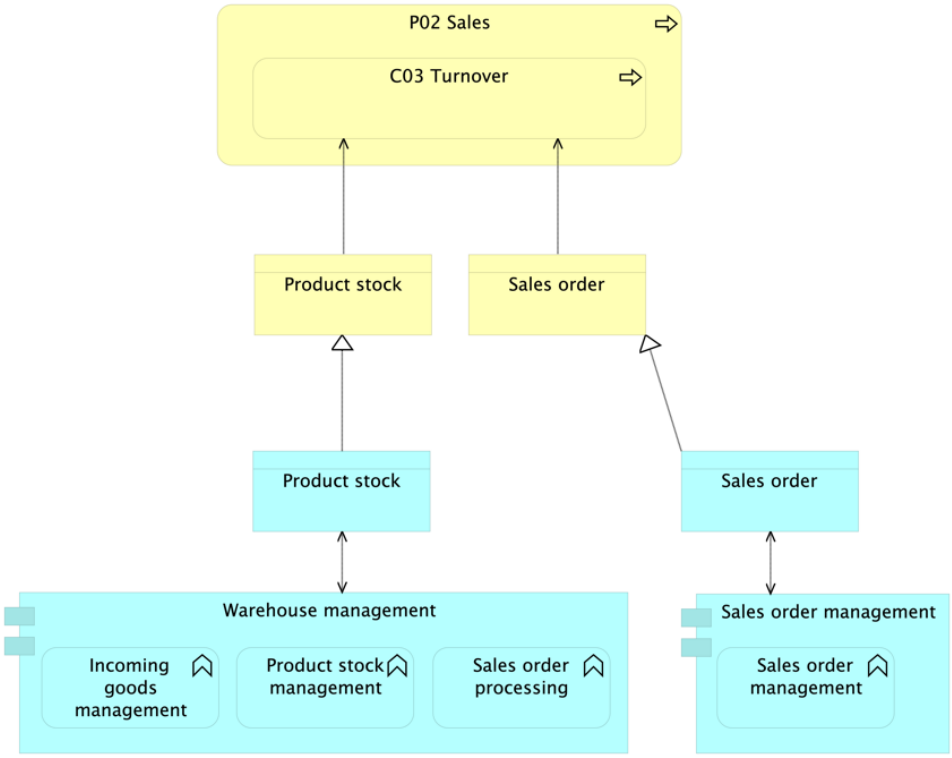


Figure 5-21 Sales process control

5.2.4. Payment processes and controls

The payment processes each have their own control.

The invoice payment process can be tested using control C04 payment segregation of duty as defined by RA1, RA3, and VAL1. This control tests that every payment is approved by at least two people and that the payment is linked to an invoice. Necessary data entities that should be matched are the purchase invoice and the bank transaction (payments), and also the involved employees in a transaction (invoice approval).

The update creditor master data process can be tested by control C05 change creditor master data, as defined by RA1 and VAL1. The control tests that every change in creditor master data is approved by at least two people. Necessary data entities that should be matched are the creditor database and the data changes and approvals.

Figure 5-22 shows the model of the process with controls and data entities.

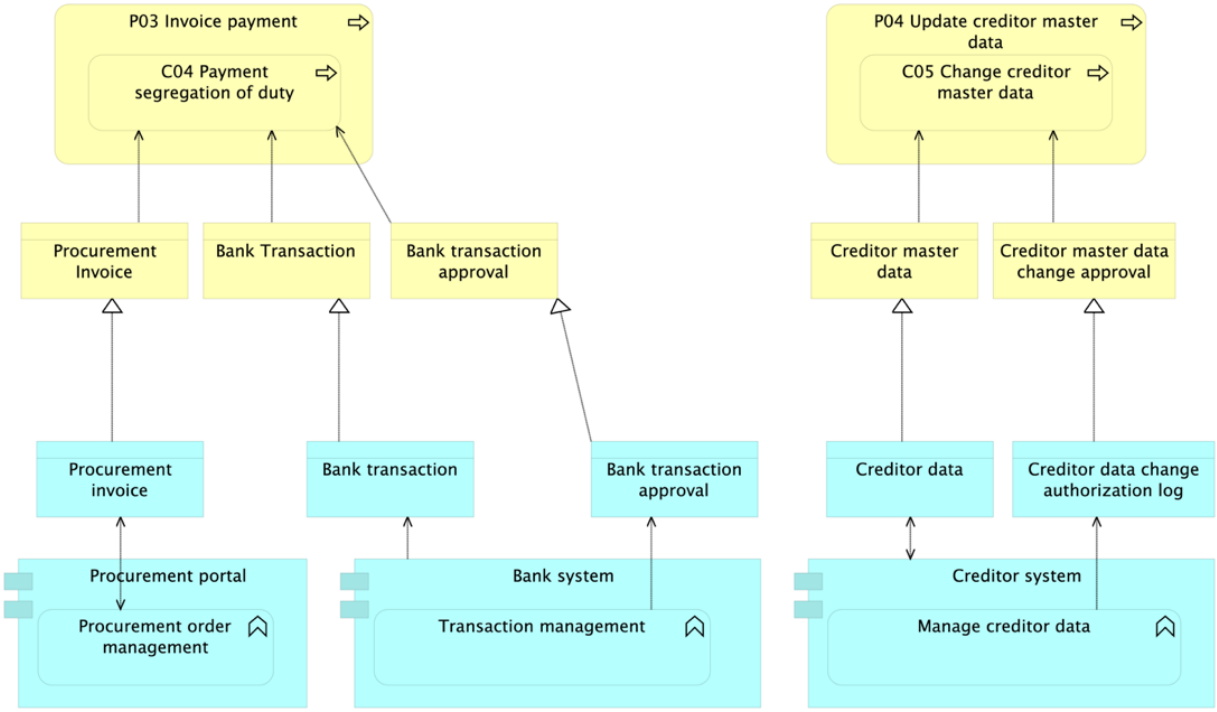


Figure 5-22 Payment processes and controls

5.2.5. HR Employee Mutation process controls

The Employee mutation processes have been mentioned as important preconditions for the General Access Protection control (C09, C10, and C11) by ITA1 and ITA2.

For the P05 New employee process, the control C07 New employee was mentioned, which checks how an account has was set up and how it is ensured that he got the right access (authorization).

For the P06 Employee new role process, the control C08 Employee new role tests how it is ensured that his access is proper (authorization) after the change.

The P07 Employee leaves can be tested by the control C09 Employee leaves, which tests that roles and rights are revoked in a correct and timely manner.

Figure 5-23 shows the model of the process with controls and data entities.

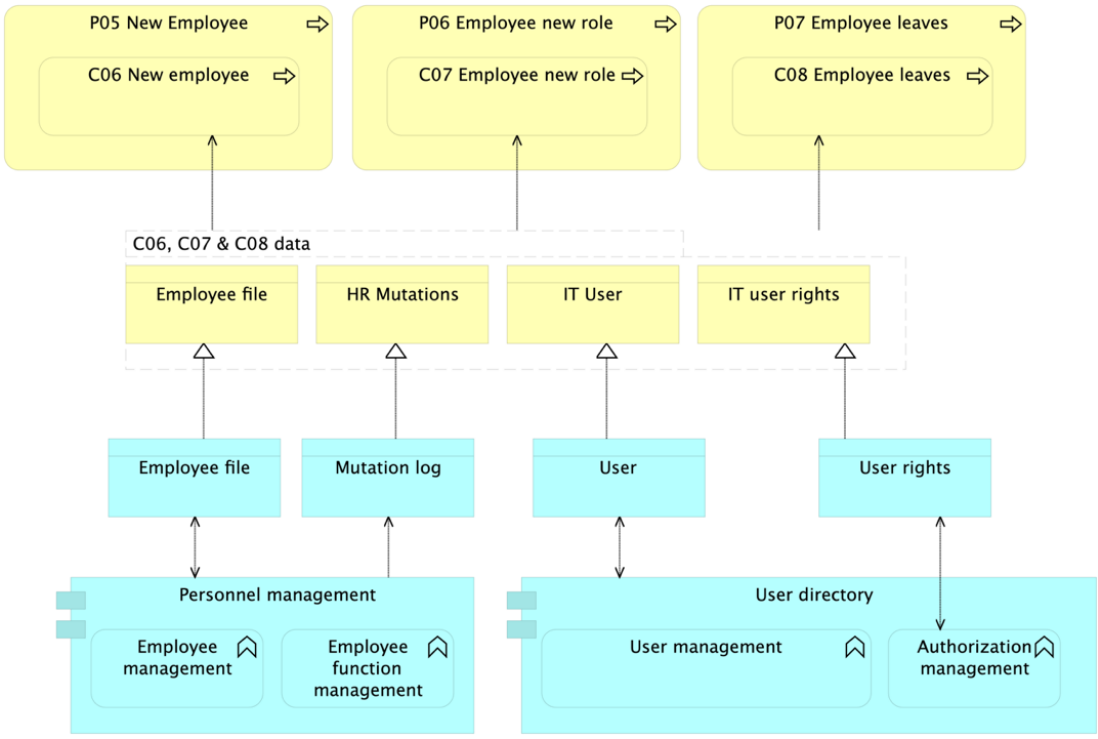


Figure 5-23 HR Employee mutation process controls

5.2.6. IT General process controls

To test this process, three controls were defined by the interviewees: C09 General access protection identification (Identification), C10 General access protection authentication (Authentication), and C11 General access protection authorization (Authorization).
Control C09 Identification tests whether a user in the system actually represents which real person. A user in the system should be identifiable and traceable to an actual person. Necessary data entities that should be matched to test the control are the users in the system, the username mapping, and the list of employees from HR.
Control C10 Authentication tests whether a user in the system is logged in himself using a proper username and password. The logged-in user is the actual person that it represents and not someone else. Necessary data entities that should be matched are the password policy (how should it be) and the actual password policy per user.
Control C11 Authorization tests whether a user in the system has the appropriate rights and roles and can only do within the system what he should do. Necessary data entities that should be matched to test this control are the roles and rights per user in the system and the roles that a user should have (from HR).
Figure 5-24 shows the model of this process with controls and data entities.

The process P09 Update system is being tested by control C12 Change management, which checks changes in system configuration have been made and what software upgrades have been performed. What was the impact of those changes and how have they been tested to ensure the correct functioning of the system(s) and business processes. Necessary data entities that should be matched are an overview of all system changes and updated over a period, the changelogs per update, the approval of a second person per change, and the change ticket from the ticketing system.

Of the processes, P10 Manage backup and recovery is an essential process, the testing of it is not. The control to test this process is C13 Business continuity, which checks whether proper backup and recovery measurements are in place. Necessary data entities to test this control are backup schedules, backup tests, and an overview of the IT landscape to assure that all systems are back-upped properly.

The model for C12 and C13 is shown in Figure 5-25.

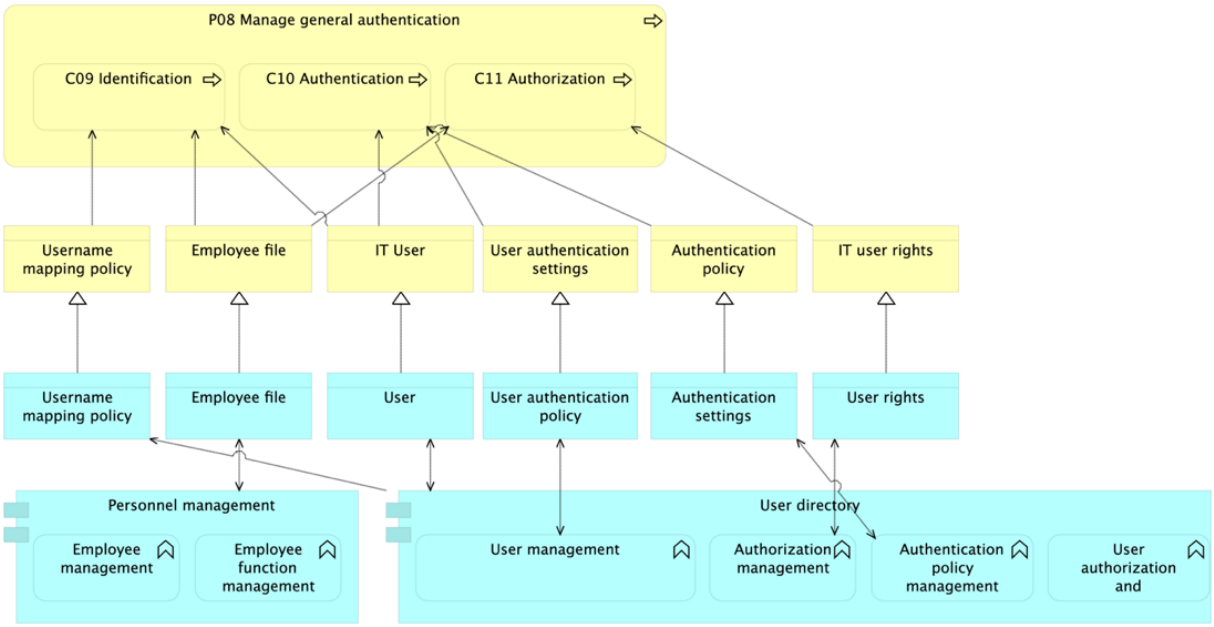


Figure 5-24 Manage general authentication process controls

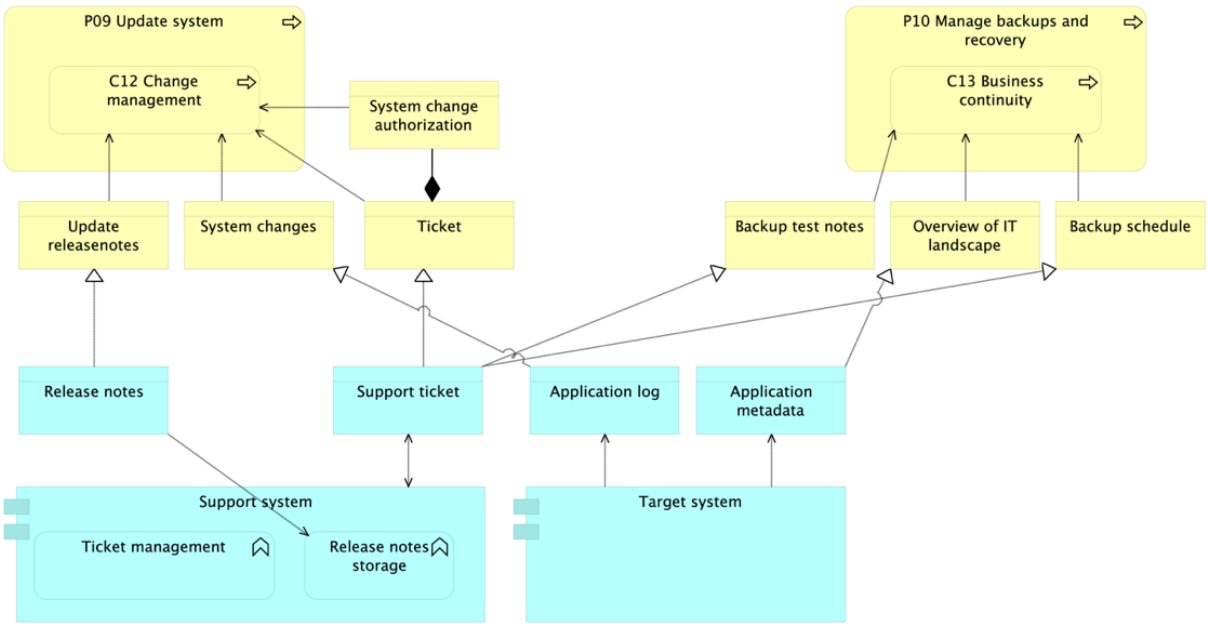


Figure 5-25 IT General process controls

5.3. Data Analytics Architecture

This chapter models the viewpoint of the Data Analytics architect and describes the business processes, application components and functions, and systems and infrastructure that are required for a data analytics architecture. Also, their relations will be described. This is based on the literature review (ch. 2.3) and the interview with DA1.

The views in this chapter show how the testing of controls could be automated by using data analytics.

5.3.1. Viewpoint description

The Data Analytics architect is the stakeholder whose concerns regard the entire data analytics infrastructure (processes, applications, and technology) and touching every step of the data analytics process (Table 5-1).

The used objects in the ArchiMate models are described below.

Business layer elements

The business layer consists of business actors who have one or multiple business roles. Those business roles execute business processes or groups of business processes, called business functions. Business processes and functions require or deliver data that is modeled as business objects. A business process can also be executed at a separate location (customer), which means that the business object is also available at this separate location. This is modeled using the location element and a composition relation.

The metamodel for this layer is displayed in Figure 5-26.

Application layer elements

The application layer consists of application functions that are grouped into application components. Those functions and components work with application data objects. Business functions implement application services that are used by business processes. Application functions and components can work with multiple application (data) objects.

Application components can be at the customer (source) location. In order for data to be transferred from this source location to the other location, an interface is modeled.

The metamodel for this layer is displayed in Figure 5-27.

Technology layer elements

Multiple application nodes are defined containing various devices in order to implement services that application components can be hosted on. An interface is modeled to describe how nodes communicate in order to pass data. Also, technology collaboration can be modeled to describe the use of a single resource by multiple nodes.

The metamodel for this layer is displayed in Figure 5-28.

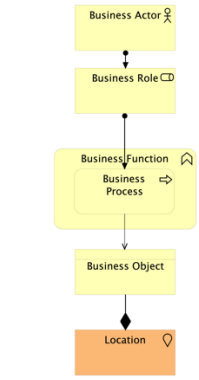


Figure 5-26 Metamodel business layer

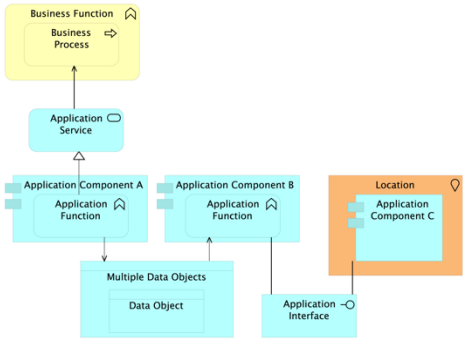


Figure 5-27 Metamodel application layer

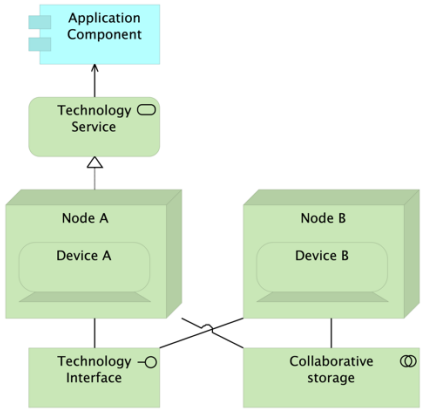


Figure 5-28 Metamodel technology layer

5.3.2. Processes and data

The literature describes that the essential steps towards data analytics are: (1) data extraction from the source systems, (2) data transport to the temporary data storage, (3) data transformation to a uniform format, and (4) data loading into the data warehouse. When the data is transformed in a uniform format in the data warehouse, (5) standardized analysis can be performed on that data and (6) published to a data visualization system.

The interview with DA1 describes the steps towards data analytics as (1) defining the data required from the source (customer) systems, (2) extract the data from the source (customer) systems, and (3) upload it to a secure file share. From the file share, the data is (4) manually loaded into the data warehouse, and (5) displayed using a data visualization dashboard. Additionally, data can be loaded in a system that supports data analysis.

Combining these processes, results in the process steps as displayed in Table 5-1.

Table 5-1 Data analytics process steps

#	ID	Name	Description
1	DAP01	Data definition	Defining the required data and source systems.
2	DAP02	Data extraction	Extracting data from the source systems.
3	DAP03	Data transport	Uploading data to the temporary data storage.
4	DAP04	Data transformation	Transforming data into a uniform format.
5	DAP05	Data loading	Loading data into the data warehouse.
6	DAP06	Data analysis	Analyzing the data and performing tests such as controls.
7	DAP07	Data visualisation	Visualizing the data analysis results.

Since data analysis will be performed at a different site, by different actors than the data source site, multiple actors and roles are required. The actors and data analytics process steps are modeled in Figure 5-29. The source location in this represents all applications in chapter 5.2 where data comes from that is required to test the controls.

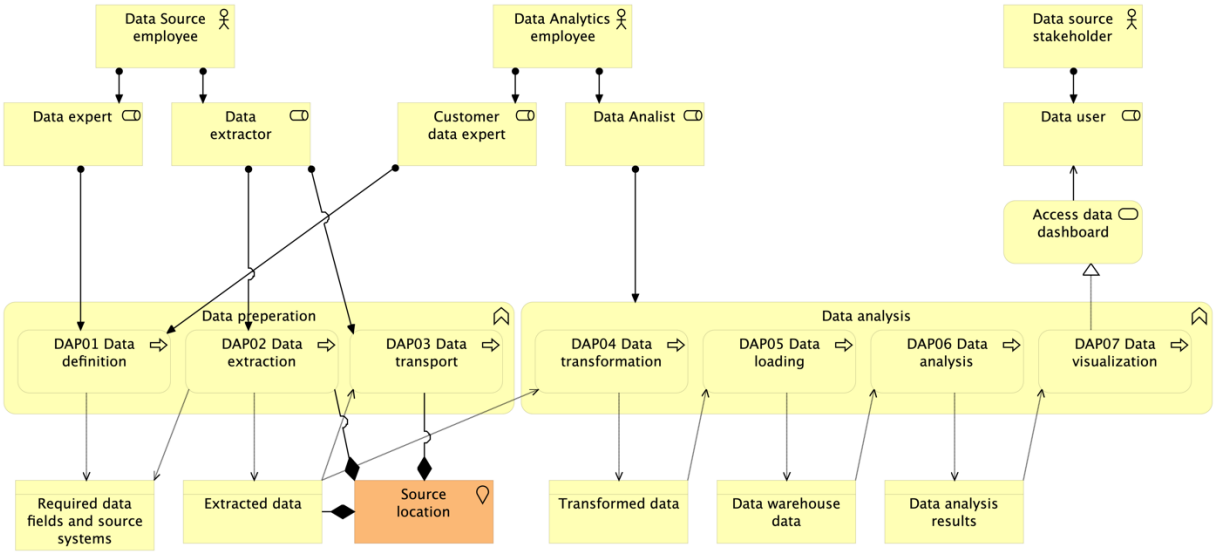


Figure 5-29 Data analytics process

5.3.3. Application components and functions

The interview results define multiple specific applications that are used to support the processes. These specific applications are translated into application components, based on the description from the literature and interview. This is shown in Table 5-2. Those applications and the data that they require are modeled in Figure 5-30 and Figure 5-31. The file share is the link between the application components.

Table 5-2 Data analytics applications mapping

Process	Specific application	Application components	Description
DAP01	Word / Excel	Data modeling - Data definition	A tool for defining the data that needs to be extracted.
	Source systems		The source applications that are modeled in chapter 5.1, where the data that analysis is performed on come from.
DAP02 DAP03	Smart Exporter	Data management - Data extraction - Data upload	An application that extracts data from the source systems and transports the data to another system.
	Huddle	Fileshare - Data storage	A system where data can be stored on to share.
DAP04 DAP05	TimeXtender	Data warehouse - Temporary data storage - Data transformation - Data storage	A centralized system where various sets and types of data can be stored for further processing, such as transformation.
DAP06	Data Analysis	Data analysis - Data analysis processing	A data analysis engine that can execute queries on the data and store the results.
DAP07	Qlik Sense	Data visualization dashboard - Data visualization	A user interface to display data and analysis reports on.

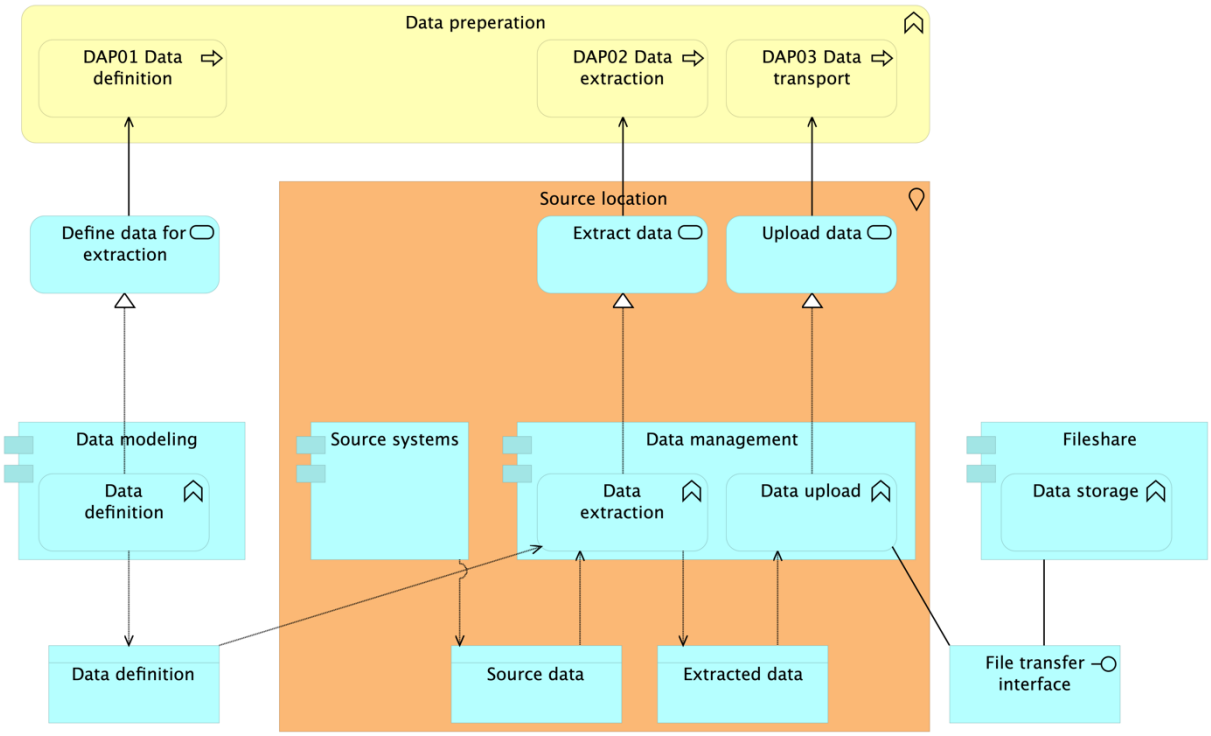


Figure 5-30 Data analytics application components, functions, and data part 1

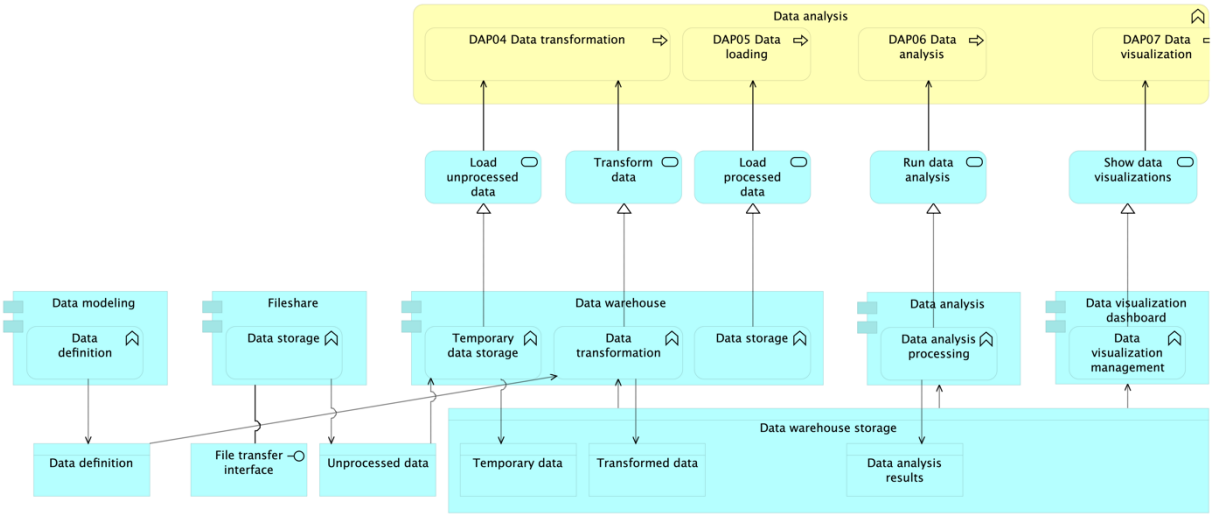


Figure 5-31 Data analytics application components, functions, and data part 2

5.3.4. Systems and infrastructure

The literature describes that data analytics requires a specific infrastructure. Several applications use the same resources, such as data storage (the data warehouse) and more. This view is defined to complete the viewpoint and is based on the described infrastructure during the interview with DAL1. This is described in Figure 5-32.

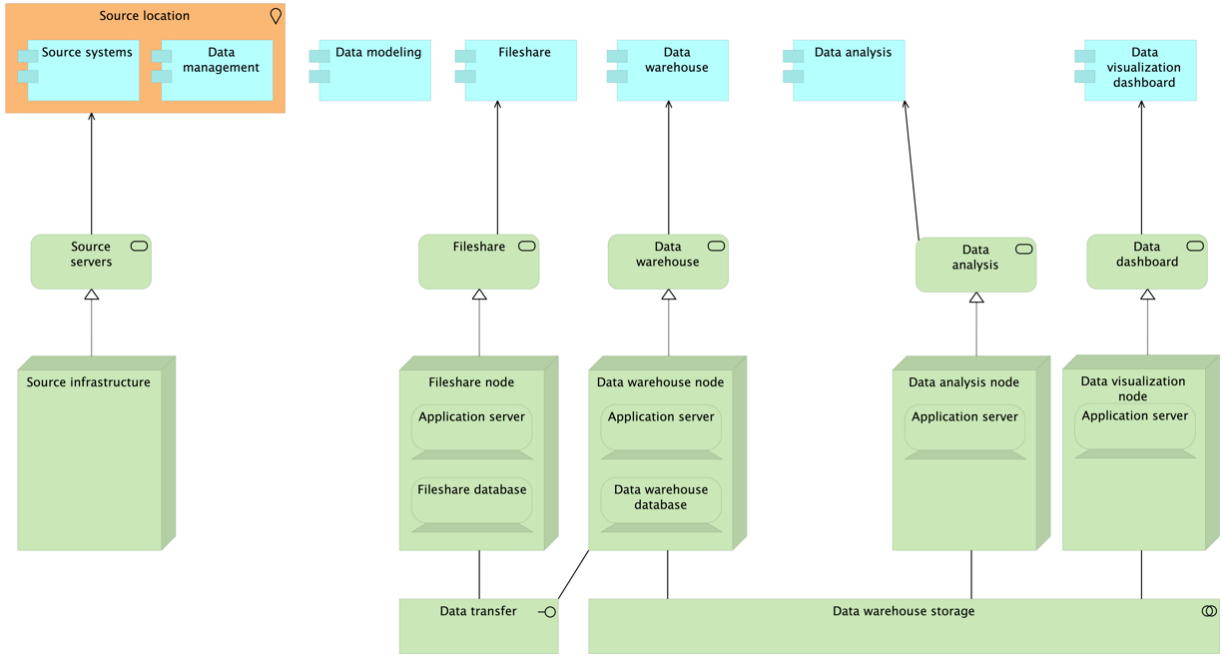


Figure 5-32 Data analytic systems, and communications

6. VALIDATION

This chapter describes the validation of the reference architecture that was developed in chapter 5, as described in chapter 3.3. The architecture should be implementable in the cases, and all required components in order to test the controls and to implement data analytics should be available.

First, the questions that will be asked to validate the model are defined (ch. 6.1). Secondly, the cases are discussed (ch. 6.2, 6.3, and 6.4), starting with a case description, second, the results from the validation questions, and last a discussion of those results.

6.1. Validation Interviews

The goals of the validation interview are, firstly, to test whether the modeled application and data objects in the reference architecture can be mapped to actual company elements. And secondly, if the data can actually be extracted from the source systems in an automatic and continuous manner. This results in which controls can or cannot be implemented if certain elements are not available or mappings are not possible. In essence, the interviewee will be asked to (1) name the actual application for each application component in the reference architecture, (2) confirm whether the data is available in the applications, and (3) explain if the described integration can be implemented.

The questions are asked in an open manner, but the results will be noted in structured tables in order to optimize interview processing. The result tables can be found in Appendix C: Validation Result Tables. The interview questions are defined below.

Interview questions

1. Figure 6-1, Figure 6-2 and Figure 6-3 show application components that have been defined. These application components can be implemented in one or more applications. Can you please name the actual applications where these components are embedded in? *Fill in the data in* Appendix Table 2*.*

2. Are those applications hosted in the cloud or on-premise? *Fill in the data in* Appendix Table 2*.*

3. In order to test the controls, data entities have been defined as shown in Figure 6-1, Figure 6-2 and Figure 6-3. This data was mapped to application components that should produce it. How do these data entities relate to data entities in the applications? *Fill in the data in* Appendix Table 3*.*

4. How can the data be accessed? E.g., by using separate tooling, getting it directly from the database, accessing the API, or making exports through the application interface? And where are they located, e.g., database table? *Fill in the data in* Appendix Table 3*.*

5. How often can this data be fetched from the systems? (e.g., every hour, trigger, daily) *Fill in the data in* Appendix Table 3*.*

6. In order for data to be extracted from the systems, a data management system at the customer-site is required, as shown in Figure 6-4. That system extracts all data from

the systems and uploads it to the secure file share. Is there already such a system at your client? Does that system support continuous uploading? If not, do you have an idea of what kind of system could be used for this data management?

7. How would data transfer from the customer environment to the accountant's environment be performed? (e.g. file share / dropbox / API)

Procurement, warehouse, Sales orders

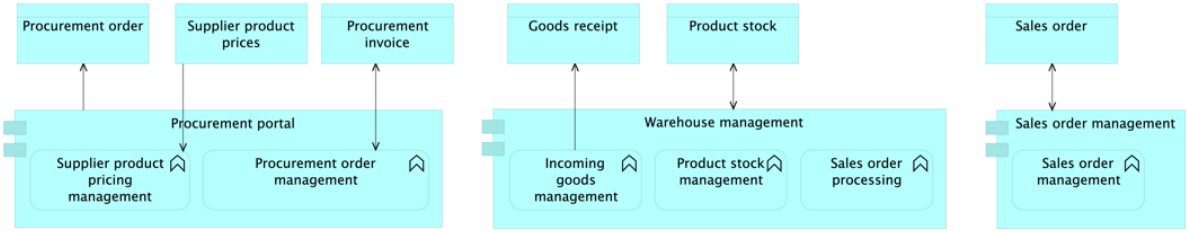


Figure 6-1 Procurement, Warehouse, and Sales order application components

Bank, Creditor, and Personnel management

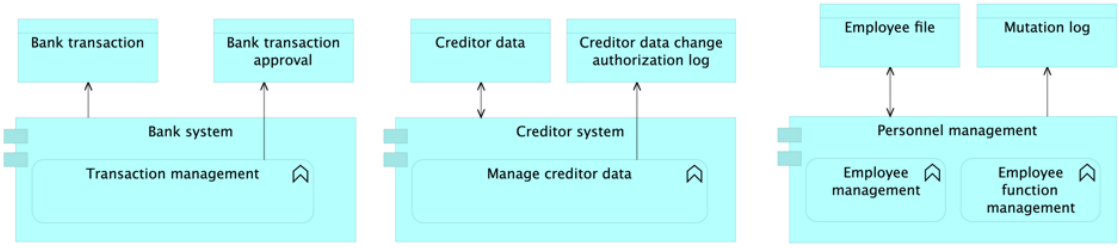


Figure 6-2 Bank, Creditor, and Personnel management application components

User directory, Support, and Target system

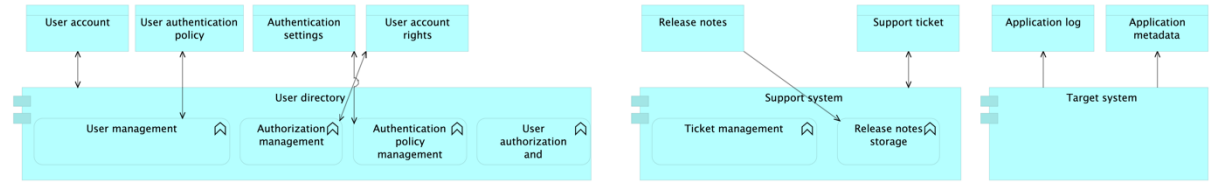


Figure 6-3 User directory, Support, and Target application components

Data management and File transfer interface

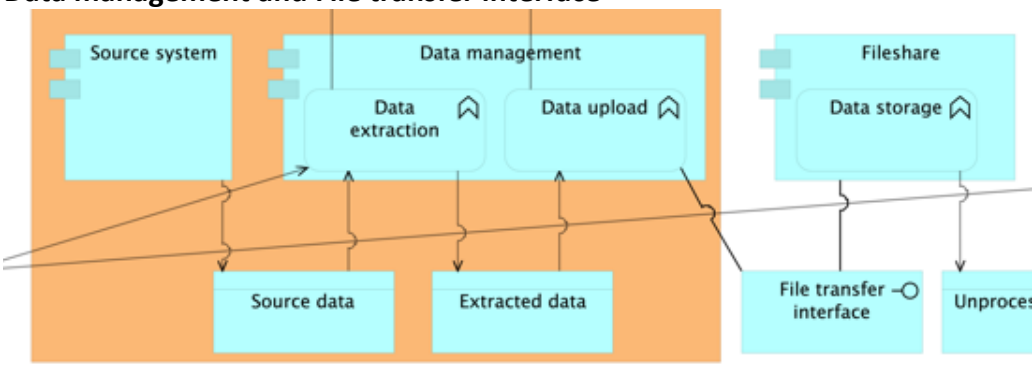


Figure 6-4 Data management and File transfer interface

6.2. Case 1

The first case regards an SME (ComA) that is founded in 1999 and has 130 employees. ComA imports skirting boards and window profiles and resells them. They take care of the entire process, from procurement, to order, to delivery themselves. For their processes, ComA relies heavily on IT systems with at the heart an ERP system, Navision Business Central.

IT auditor ITA03 has been performing the IT audits for ComA for three years and knows the business processes and IT systems that are relevant for the audit. He is interviewed in order to test whether the company could implement the reference architecture.

6.2.1. Interview results

ComA uses six applications that are in the scope of this study. Navision ERP, an enterprise resource planning system with a standard structure, is used for the management of procurement, sales, and creditor management. WICS, an inventory management tool that was developed internally is used for inventory management. Delta, a software-as-a-service application, is used for personnel management. For account management, they use Microsoft Active Directory. A separate support ticketing system is being used for ticket management. Finally, Rabo Telebankieren is being used for bank transaction management. This is described in detail in Appendix Table 4.

All data entities, as described in the architecture, are available in the applications of ComA. Some data, however, cannot be extracted in an automatic manner as manual exports should be made, or even requests for exports have to be done to third-party suppliers. The data access frequency for most data is unlimited since it can be accessed on-demand directly. This is described in detail in Appendix Table 5. The data can be extracted and pushed to the data analytics environment using Robotic Process Automation (RPA) and storage of the data onto a file share. RPA is already in place.

For gathering the exact data tables where Navision data was located, ITA03 consulted the Navision database manual. A note hereby was that modeled data entity names do not always match database table names.

6.2.2. Discussion

ComA has all applications available in order to implement the reference architecture financial monitoring. The continuous part, however, is not possible yet since the bank system data, personnel management data, and support system data have to be manually exported. The possibility exists that those integrations can still be made, but ITA03 does not have this knowledge, and it would require a more thorough investigation into the specific applications.

The comment that data entity names do not match the database tables names can be important. The business object names in the architecture are based on the interview results and on how the accountants name these. The application data objects are based on those interviews as well but might be altered if more cases result in the same mismatch.

Data from the application components Bank system, Personnel management, Support system, and Target system are not available for continuous automated extraction. Therefore, based on the reference architecture, 9 out of 13 controls for the processes P03 Invoice payment, P05

New Employee, P06 Employee new Role, P07 Employee leaves, P08 Manage general authentication, P09 Update system, and P10 Manage backups and recovery cannot be automatically tested. This data could be added manually though.

6.2.3. Conclusion

The reference architecture describes the Continuous Financial Monitoring properly and can be applied properly. All mentioned application components and data objects are available, but not all data objects are automatically accessible. Therefore, CFM can not yet be implemented for this case due to infrastructural limitations. Only 4 out of 13 controls can be tested. Further study of this case might result in solutions that would allow integration with the missing systems.

6.3. Case 2

The second case regards an SME (ComB) that is founded in 1979 and has 85 employees. ComB develops and produces emulsified beverages for customers around the world. They are the global leader in the B2B cream liqueur segment. They handle the entire process from buying products (procurement), to production, to sales, to delivery themselves. As a world-class production company, ComB relies heavily on the ERP system, especially for supply-chain management.

ComB has a modern IT infrastructure and already performs data analytics for their production process. IT auditor ITA04 has helped with setting up the current data analytics environment and will be interviewed.

6.3.1. Results

ComB uses three different applications in the scope of this study. The most important is SAP ERP, which is involved in all business processes. ING Banking is a software-as-a-service application that is provided by their bank for making transactions. Lastly, Microsoft Active Directory is being used for user management. This is described in more detail in Appendix Table 6.

The data entities, as described in the reference architecture, are available in the applications. All data can be extracted automatically and continuously at an unlimited frequency. The data from SAP is already being extracted and loaded into the on-site data warehouse. The exact table names were found in the SAP manual since ComB has a standard implementation. To extract data from the banking application, the API has to be used, which is well-documented. The customer data mapping is described in detail in Appendix Table 7.

ComB already has a data warehouse in which they can load all data. From there, the data can be uploaded onto a secure file share on demand.

6.3.2. Discussion

Since ComB is already using data analytics, continuous financial monitoring can be implemented relatively easily. Only integrations with the banking application and the Active Directory would have to be made.

ITA04 noted that the ComB is very willing to implement continuous financial monitoring but would like to have access to the information as well.

The same table names mismatch that occurred in case 1 was seen in this case as well. However, table names are very inconsistent and are not descriptive. The tables for procurement orders are named EKKO and EKPO, while the data object in SAP was named procurement.

6.3.3. Conclusion

The reference architecture describes the Continuous Financial Monitoring properly for case 2 as well. All mentioned application components and data objects are available, and all data objects are automatically accessible. Therefore, CFM can be implemented in this case and all controls can be automatically tested.

6.4. Case 3

The third case regards an SME (ComC) that is founded in 1999 and has 65 employees. ComC is a wooden interior manufacturing company. They are active in the retail industry and can manufacture entire shop interiors within days. ComC handles the entire process from sales to procurement to delivery to installation themselves. ComC has an old-fashioned ERP system, Proteus ERP, on which they rely heavily.

ComC is currently working on upgrading its IT infrastructure. They will soon start to use data analytics to measure and optimize their business processes. EMP01

6.4.1. Results

ComC uses four applications that are in the scope of this study. Proteus ERP, an enterprise resource planning system, which is used throughout all business processes. Rabobank Telebankieren is a software-as-a-service application that is used to execute bank transactions and to view incoming transactions. For account management, Microsoft Active Directory is being used. And as a support system, the ticketing system from the IT supplier is used. This is described in detail in Appendix Table 8.

All data entities, as described in the architecture, are also available in the applications. All data can be automatically extracted on demand, except for the support system, which can do automated CSV exports on a daily bases. ComC is currently working on the implementation of a data management solution in order to perform its own analysis. This system would be capable of extracting data from the source systems and pushing it to a secure file share.

In addition to the interviews with EMP01, a Proteus consultant was asked to provide the table names where the specific data could be found.

6.4.2. Discussion

ComC has modern systems and will be able to perform its own data analytics soon. This makes the implementation of continuous financial monitoring relatively simple. Integrations with the banking application API and with the Active directory would have to be made in addition to the ERP integration.

Because of the support system that provides daily reports, the financial monitoring would not be 100% continuous. However, the support system data does not have a big impact when testing the controls, so continuous financial monitoring would still be possible.

A table name mismatch occurred here as well, but only for some tables. The table for sales orders is named SALESORDER, which is the same as the data entity Sales order. But procurement was called purchase in Proteus.

6.4.3. Conclusion

The reference architecture describes Continuous Financial Monitoring properly for case 3 as well. All mentioned application components and data objects are available, and all data objects are automatically accessible. Therefore, CFM can be implemented in this case, when the data analytics environment is finished. All controls can be automatically tested.

7. CONCLUSION

The research question throughout this research is: How can continuous financial monitoring using data analytics be implemented in small to medium-sized enterprises?

In the literature review, we have taken an extensive look at what (continuous) financial monitoring entails: the process of monitoring the financial processes and procedures within a company, based on testing defined controls. And also, at the procedures and components that data analytics consists of. Through the interviews with accountants and IT auditors we have learned what those controls actually are for the business processes procurement, sales, payment, HR, and general IT, how they can be tested, what data is needed to test them, and from what applications and systems this data can come from. A total of 13 controls were named and validated. The interview with a data analytics expert resulted in additional information on what components are required to use data analytics and how this can be performed. The literature regarding reference architectures, combined with the gathered data about financial monitoring and data analytics, allowed for the development of a proposed reference architecture for the implementation of continuous financial monitoring.

The developed reference architecture consists of three viewpoints: Customer Architecture, Process Controls, Data Analytics Architecture, which respectively address the concerns of the customer IT architect, the Accountant, and the data analytics consultant. The viewpoints portray the organizational structure and business processes with the required data, applications and technology infrastructure. Also, the controls per business process with the required data in order to test it are modeled, as well as a manner to implement continuous financial monitoring using the data analytics infrastructure. For the data analytics infrastructure, the process and several core IT components were defined.

The reference architecture was validated by performing a multiple-case study to test whether the architecture could be implemented in three different SMEs. We were able to implement the architecture in two out of three cases completely. One company could implement the architecture but was not able to automatically test all controls due to infrastructural limitations but might be able to after further research on the functioning of certain systems. The validation has shown how the reference architecture is also applicable for defining which controls could be (automatically) tested using the systems available.

Since the architecture could be implemented in two out of three cases fully, and only cannot be implemented in the third case because of their own limitation, we can conclude that the answer to the research question is:

> Continuous financial monitoring using data analytics can be implemented in small to medium-sized enterprises by implementing the reference architecture as proposed in this research.

7.1. Limitations and Further Research

This research took place within a specific research setting. The interviewed accountants and IT auditors all came from different branches of the same firm; this might be a bias, although the interviews mostly regarded the actual organizations which differed a lot. Also, all accountants in the Netherlands have to comply to the same standards. Further research on controls by means of a quantitative survey and sending it out to accountants and IT auditors

of more different firms could further strengthen this research. Also, a limited amount of business processes was tested, which should be extended further as well. This was not necessary for this research since it lays a ground for researching other processes.

The case study only researched three cases which all used an ERP system for most business processes. This should be extended to also incorporate businesses that use other systems. This can be performed by developing a quantitative survey, as well.

Finally, continuous financial monitoring is portrayed as a black and white image in this research. A company could either implement it fully or not implement it at all. A certain approach of implementation could come in handy where steps, stages or maturity levels can be defined. Maturity levels could be developed which are grouped per set of controls. For instance, testing the general controls is fundamental, so controls C06/C13 should be the at the first maturity level. In the next layer, a set of controls could be defined that tests general business processes such as the payment processes P03 and P04. Other general business processes should be defined and added as well. Next levels could be defined per process again. For organizations that have, for instance, the sales process, what controls should generally be tested? And, in a next level for that process, what controls are less often found in organizations? Further research on whether these various maturity levels of implementations could be defined and what they would entail might be valuable. This would allow smaller companies to benefit from CFM as well, as they could only implement it up until a certain level.

7.2. Reflection

Looking back at this research and writing my thesis, I can say a few things that I didn't anticipate when planning the research and developing the approach.

Firstly, it was very interesting to see that the interview results were quite the same. Interviewees were from different branches and locations within Baker Tilly but still produced the same results. This is mostly caused by the Accountancy branch being highly standardized and the same procedures that have to be followed. I couldn't anticipate this because of my lack of knowledge of the branch.

Secondly, the lack of IT maturity within SMEs was very unexpected. I first noticed this during the interviews with accountants and IT auditors when they made certain statements regarding their clients. The lack of their clients' IT management and maturity, where essential parts such as passwords were not managed properly, surprised me a lot. Especially because my initial thought was that IT integrations within SMEs would be quite easy since they were small, this came back as well during the case study. Case 1 regarded a company that did not have an IT strategy. Case 2 and 3 regarded bigger organizations that relied more on IT and therefore spent more time on developing a strategy.

Thirdly, my own bias during the development of the reference architecture was big. I had a strong idea regarding how the reference architecture should look like. I noticed this quickly during the early stages of development. Therefore I chose for an extended reference method where I made sure that traceability of elements in my architecture could be traced back to

literature or interviews by using proper annotations in the interviews and multiple tables containing summaries of information.

Fourthly, looking back at my chosen methods and with the knowledge regarding the branch that I have now, I would have chosen a more quantitative research method. The questions to retrieve controls, data, and applications could be asked in a survey as well since the result is formatted into structured data anyways. Also, the multiple-case study as validation could have been in the form of a quantitative survey. Choosing for a quantitative approach would have increaded the reliability of this research a lot. During the validation I actually switched from two to three cases because of the easy format that I could use for analysis.

Finally, because of the outbreak of the COVID-19 pandemic, my progress got slowed down a lot. More important things than this research came up, and also research participants had other tasks to focus on. Therefore, it became harder to plan the interviews. Also, interviewees had less time to spent on the interviews.

8. REFERENCES

Alles, M., Brennan, G., Kogan, A., & Vasarhelyi, M. A. (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems*, *7*(2), 137–161. https://doi.org/10.1016/j.accinf.2005.10.004

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting Continuous Auditing Theory into Practice: Lessons from Two Pilot Implementations. *Journal of Information Systems*, *22*(2), 195–214. https://doi.org/10.2308/jis.2008.22.2.195

Bănărescu, A. (2015). Detecting and Preventing Fraud with Data Analytics. *Procedia Economics and Finance*, *32*(15), 1827–1836. https://doi.org/10.1016/s2212-5671(15)01485-9

Barta, G. (2018). The increasing Role of It Auditors in Financial Audit: Risks and intelligent answers. *Business, Management and Education*, *16*(1), 81–93.

Bennett, N., & Lemoine, G. J. (2014). What a difference a word makes: Understanding threats to performance in a VUCA world. *Business Horizons*, *57*(3), 311–317. https://doi.org/10.1016/j.bushor.2014.01.001

Boer, R. de, Schijvenaars, T., & Oord, E. (2011). Referentiearchitecturen in de praktijk. Delen van architectuurkennis in een stelsel van semantische wiki's (in Dutch). *NOVA ARCHITECTURA*, (October), 1–14. Retrieved from http://www.archixl.nl/files/vna_wiki.pdf

Brown, C. E., Wong, J., & Baldwin, A. A. (2007). A Review and Analysis of the Existing Research Streams in Continuous Auditing. *Journal of Emerging Technologies in Accounting 4*.

Campbell, C. (2015). Top Five Differences between Data Lakes and Data Warehouses. Retrieved April 22, 2020, from https://www.blue-granite.com/blog/bid/402596/top-five-differences-between-data-lakes-and-data-warehouses

Cao, M., Chychyla, R., & Stewart, T. (2015). Big data analytics in financial statement audits. *Accounting Horizons*, *29*(2), 423–429. https://doi.org/10.2308/acch-51068

Carlin, A., & Gallegos, F. (2007). IT audit: A critical business process. *Computer*, *40*(7), 87–89. https://doi.org/10.1109/MC.2007.246

Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems*, *12*(2), 152–160. https://doi.org/10.1016/j.accinf.2011.01.001

Chan, D. Y., & Vasarhelyi, M. A. (2018). Innovation and Practice of Continuous Auditing. *Continuous Auditing*, 271–283. https://doi.org/10.1108/978-1-78743-413-420181013

Chaudhuri, S. (2012). What next? A half-dozen data management research goals for big data and the cloud. *Proceedings of the ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, 1–4. https://doi.org/10.1145/2213556.2213558

Chen, D., Doumeingts, G., & Vernadat, F. (2008). Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry*, *59*(7), 647–659. https://doi.org/10.1016/j.compind.2007.12.016

Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, *36*(4), 1165–1188.

Chiu, V., Liu, Q., & Vasarhelyi, M. A. (2014). The development and intellectual structure of continuous auditing research. *Journal of Accounting Literature*, *33*(1–2), 37–57. https://doi.org/10.1016/j.acclit.2014.08.001

Christiaanse, R., & Hulstijn, J. (2013). Control automation to reduce costs of control.

International Journal of Information System Modeling and Design, *4*(4), 27–47. https://doi.org/10.4018/ijismd.2013100102
CICA, & AICPA. (1999). *Continuous Auditing*.
Cloutier, R., Muller, G., Verma, D., Nilchiani, R., Hole, E., & Bone, M. (2010). The Concept of Reference Architectures. *Systems Engineering*, *13*(1). https://doi.org/10.1002/sys
Columbus, L. (2018). Big Data Analytics Adoption Soared In The Enterprise In 2018. Retrieved February 17, 2020, from Forbes website: https://www.forbes.com/sites/louiscolumbus/2018/12/23/big-data-analytics-adoption-soared-in-the-enterprise-in-2018/#172d659b332f
El-Sappagh, S. H. A., Hendawi, A. M. A., & El Bastawissy, A. H. (2011). A proposed model for data warehouse ETL processes. *Journal of King Saud University - Computer and Information Sciences*, *23*(2), 91–104. https://doi.org/10.1016/j.jksuci.2011.05.005
Elgammal, A., Turetken, O., van den Heuvel, W. J., & Papazoglou, M. (2016). Formalizing and appling compliance patterns for business process compliance. *Software and Systems Modeling*, *15*(1), 119–146. https://doi.org/10.1007/s10270-014-0395-3
Ezzamouri, N., & Hulstijn, J. (2018). Continuous monitoring and auditing in municipalities. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3209281.3209301
FASB. (2006). Conceptual Framework for Financial Reporting: Objective of Financial Reporting and Qualitative Characteristics of Decision-Useful Financial Reporting Information. *Financial Accounting Standards Board - FASB*, (1260), 69.
Flowerday, S., & Von Solms, R. (2005). Real-time information integrity = system integrity + data integrity + continuous assurances. *Computers and Security*, *24*(8), 604–613. https://doi.org/10.1016/j.cose.2005.08.004
Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, *35*(2), 137–144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007
Gerber, A., Kotzé, P., & Van Der Merwe, A. (2010). Towards the formalisation of the TOGAF content metamodel using ontologies. *ICEIS 2010 - Proceedings of the 12th International Conference on Enterprise Information Systems*, *2 AIDSS*, 54–64.
Ghasemaghaei, M., Hassanein, K., & Turel, O. (2017). Increasing firm agility through the use of data analytics: The role of fit. *Decision Support Systems*, *101*, 95–105. https://doi.org/10.1016/j.dss.2017.06.004
Greefhorst, D., Grefen, P., Saaman, E., Bergman, P., & Beek, W. Van. (2008). *Referentie-architectuur*. 1–12.
Groomer, S. M., & Murthy, U. S. (2018). Continuous Auditing of Database Applications: An Embedded Audit Module Approach. *Continuous Auditing*, 105–124. https://doi.org/10.1108/978-1-78743-413-420181005
IFAC. (2009). Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing. In *Studies and Scientific Researches. Economics Edition*. https://doi.org/10.29358/sceco.v0i14.26
Kaisler, S., Armour, F., Espinosa, J. A., & Money, W. (2013). Big data: Issues and challenges moving forward. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 995–1004. https://doi.org/10.1109/HICSS.2013.645
Kamer van Koophandel. (2019). *KVK Data over de bedrijvendynamiek*. Retrieved from https://www.kvk.nl/download/KVK-Bedrijvendynamiek-Q3-2019_tcm109-482993.pdf
Kuhn, J. R., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The

current state and future directions. *Journal of Information Systems*, *24*(1), 91–112. https://doi.org/10.2308/jis.2010.24.1.91
Lankhorst, M. (2004). Enterprise architecture modelling - The issue of integration. *Advanced Engineering Informatics*, *18*(4), 205–216. https://doi.org/10.1016/j.aei.2005.01.005
Lankhorst, M. (2009). *Enterprise Architecture at Work: Modelling, Communication and Analysis* (3th ed.). https://doi.org/10.1016/s1573-4285(08)10010-2
Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a tool to measure and compare organizations' resilience. *Natural Hazards Review*, *14*(1), 29–41. https://doi.org/10.1061/(ASCE)NH.1527-6996.0000075
Maier, M. W., Emery, D., & Hilliard, R. (2001). Software architecture: Introducing IEEE standard 1471. *Computer*, *34*(4), 107–109. https://doi.org/10.1109/2.917550
Moody, D., & Kortink, M. A. . (2000). From Enterprise Models to Dimensional Models: A Methodology for Data Warehouse and Data Mart Design. *Proceedings of the International Workshop on Design and Management of Data Warehouses (DMDW'2000)*, *2000*, 1–12.
Myers, M. D. (1997). Qualitative research in information systems. *MIS Quarterly: Management Information Systems*, *21*(2), 241–242. https://doi.org/10.4018/978-1-59140-144-5.ch016
Niemann, K. D. (2008). Enterprise architecture management and its role in IT governance and IT investment planning. *Advances in Government Enterprise Architecture*, *49*(0), 208–228. https://doi.org/10.4018/978-1-60566-068-4.ch010
Office of the DoD CIO. (2010). *DoD Reference Architecture Description*. (June), 22. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf
Oneshko, S., & Ilchenko, S. (2017). Financial monitoring of the port industry companies on the basis of risk-oriented approach. *Investment Management and Financial Innovations*, *14*(1), 191–199. https://doi.org/10.21511/imfi.14(1-1).2017.05
P. Yudowati, S., & Alamsyah, A. (2018). Big Data Framework for Auditing Process. *International Journal of Engineering & Technology*, *7*(4.38), 908. https://doi.org/10.14419/ijet.v7i4.38.27606
Palmas, E. (2011). IT General and Application Controls: The Model of Internalization. *ISACA Journal*, *12*(5), 23–26. Retrieved from http://www.isaca.org/Journal/Past-Issues/2011/Volume-5/Pages/IT-General-and-Application-Controls-The-Model-of-Internalization.aspx
PWC. (2010). What is an audit? Retrieved April 1, 2020, from https://www.pwc.com/m1/en/services/assurance/what-is-an-audit.html
Raguseo, E. (2018). Big data technologies: An empirical investigation on their adoption, benefits and risks for companies. *International Journal of Information Management*, *38*(1), 187–195. https://doi.org/10.1016/j.ijinfomgt.2017.07.008
Rezaee, Z., Elam, R., & Sharbatoghlie, A. (2001). Continuous auditing: The audit of the future. *Managerial Auditing Journal*, *16*(3), 150–158. https://doi.org/10.1108/02686900110385605
Rezaee, Z., Sharbatoghlie, A., Elam, R., & McMickle, P. L. (2002). Continuous auditing: Building automated auditing capability. *Auditing*, *21*(1), 147–163. https://doi.org/10.2308/aud.2002.21.1.147
Richardson, J., Sallam, R., Schlegel, K., Kronz, A., & Sun, J. (2020). Magic quadrant for

analytics and business intelligence platforms. *Gartner*, *ID G003866*(February), 1–60. Retrieved from https://www.gartner.com/doc/reprints?id=1-68720FP&ct=190213&st=sb

Rikhardsson, P., & Dull, R. (2016). An exploratory study of the adoption, application and impacts of continuous auditing technologies in small businesses. *International Journal of Accounting Information Systems*, *20*, 26–37. https://doi.org/10.1016/j.accinf.2016.01.003

Roberts, N., & Grover, V. (2012). Leveraging information technology infrastructure to facilitate a firm's customer agility and competitive activity: An empirical investigation. *Journal of Management Information Systems*, *28*(4), 231–270. https://doi.org/10.2753/MIS0742-1222280409

Rouse, M. (2015). What is extract, transform, load (ETL)? - Definition from WhatIs.com. Retrieved April 22, 2020, from http://searchdatamanagement.techtarget.com/definition/extract-transform-%0Aload

Russom, P. (2011). BIG DATA ANALYTICS - TDWI BEST PRACTICES REPORT Introduction to Big Data Analytics. *TDWI Best Practices Report, Fourth Quarter*, *19*(4), 1–34. Retrieved from https://vivomente.com/wp-content/uploads/2016/04/big-data-analytics-white-paper.pdf

Ruthberg, Z. G., & McKenzie, R. G. (1977). *Audit and Evaluation of Computer Security*.

Shao, G., Shin, S. J., & Jain, S. (2015). Data analytics using simulation for smart manufacturing. *Proceedings - Winter Simulation Conference*, *2015-Janua*(Smlc 2012), 2192–2203. https://doi.org/10.1109/WSC.2014.7020063

Sheldon, M. D. (2019). A primer for information technology general control considerations on a private and permissioned blockchain audit. *Current Issues in Auditing*, *13*(1), A15–A29. https://doi.org/10.2308/ciia-52356

Sonnenberg, C., & Brocke, J. vom. (2014). The missing link between BPM and accounting: Using event data for accounting in process-oriented organizations. *Business Process Management Journal*, *20*(2), 213–246. https://doi.org/10.1108/BPMJ-12-2012-0136

Sosin, A. (2018). How To Increase the Information Assurance in the Information Age. *Journal of Defense Resources Management*, *9*(1), 45–57. Retrieved from http://capella.summon.serialssolutions.com.library.capella.edu/2.0.0/link/0/eLvHCXMwrV1LS8QwEB58IAgiiopv8gdW85h005tVutaDLNiKx9Jk0uMisv7_TZqCr4MHPSaBGSYhmZnkyzcASl7xybczwZnOCY8kCf3UoemJpDVoXHB3ytvs6wPvR-WvCBFLbMFpHq8lWUvcWTVFRMd7qwUp6jPSTqLr9Tpshoglx5Rcxcp

The Open Group. (2011). *The TOGAF® Standard Version 9.2*. Retrieved from https://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html

The Open Group. (2016). *ArchiMate® 3.1 Specification*. Retrieved from https://pubs.opengroup.org/architecture/archimate3-doc/toc.html

The Open Group. (2018). *The TOGAF® standard, version 9.2*. Retrieved from https://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html

Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of Analytic Monitoring for Continuous Assurance. *Journal of Emerging Technologies in Accounting*, *1*(1), 1–21. https://doi.org/10.2308/jeta.2004.1.1.1

Vasarhelyi, M. A., Alles, M., Kuenkaikaew, S., & Littley, J. (2012). The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. *International Journal of Accounting Information Systems*, *13*(3), 267–281. https://doi.org/10.1016/j.accinf.2012.06.011

West, D. M. (2012). Big Data for Education: Data Mining, Data Analytics, and Web Dashboards. *Governance Studies at Brookings*, (September), 11. Retrieved from http://www.brookings.edu/~/media/research/files/papers/2012/9/04 education technology west/04 education technology west

Zakir, J., Seymour, T., & Berg, K. (2015). BIG DATA ANALYTICS. *Issues in Information Systems*, *16*, 81–90.

LIST OF FIGURES

LIST OF TABLES

APPENDIX A: DETAILED INTERVIEW RESULTS

Interview 1 with RA1

General interviewee information (#general_information)

Education	Economics at Tilburg University and post-master Accountancy
Current role	Senior manager in Audit
Continuous Financial Monitoring experience	None
Amount of SMB Trade Organizations	6 to 10 organizations
Amount of experience as accountant	15 years

General notes (#general_note)

1. The sales process is very organization dependent and therefore it is quite hard to define standardized controls.
2. Controls can only be properly tested if the entire process (precondition) is tight. So, if you have to do an ERP export and you can change that file before importing it into a bank application, the process can still fail.
3. Continuous Financial Monitoring might be beneficial for an organization because it will decrease their error margin. However, once they have set it up, they might not manage it properly. CFM might also be beneficial because the accountant can rely on that system and can focus on other aspects during the audit.

Approach to start audit (#audit_approach)

1. How are the business processes structured?
2. What IT systems are involved in those processes.
3. Are the business processes documented.
4. Are the IT General Controls (preconditions) in place.
5. Define the controls to be used.

(Financial) Department structure (#fd_structure)

- Finance department
- Warehouse department
- IT
- Procurement and Sales

Processes, Controls, Data and Systems (#process, #control, #data, #system)

Control	Type / Process	Description	Data	System
Three-way-match (three_way_match)	Procurement	A purchase order should have a receiving receipt and invoice. Those three	- Purchase orders - Receiving receipts - Invoices - Product contract	Enterprise Resource Management (ERP) system

		items should match and be tested by different people (segregation of duty).	price (part of control product pricing)	
Product pricing (product_pricing)	Procurement	The price of products on the receipt should match the price as stated in the overlapping contract.	- Invoices - Product pricing contract	ERP system
Change creditor master data (change_creditor_master_data)	Payment	Changing the data of a creditor (person or organization who receives money) requires segregation of duties and has to be checked by at least 'four eyes.	- Creditor database	Bank application / ERP system
Payment segregation of duty (payment_segregation_of_duty)	Payment	Making a payment requires segregation of duties and has to be checked by at least 'four eyes'.	- Payments - Invoices - Invoice approvals	Bank application
Access security (it_general_access_protection)	IT General			
Branch Comparison (branch_comparison)	Sales	Comparing the margins, daily		

		turnover, and even daily turnover per seller of one branch to another to find deviations.		
Change management (it_change_management)	IT General			

List of unique used keys

#audit_approach
#control_branch_comparison
#control_change_creditor_master_data
#control_it_general_access_protection
#control_it_change_management
#control_payment_segregation_of_duty
#control_product_pricing
#control_seller_badge_scan
#control_three_way_match
#control_tree_way_match
#data_change_creditor_master_data
#data_payment_segregation_of_duty
#data_three_way_match
#data_tree_way_match
#fd_structure_it
#fd_structure_warehouse_department
#general_information_amount_trade_organizations
#general_information_cfm_experience
#general_information_current_role
#general_information_education
#general_information_experience
#general_note_1
#general_note_2
#general_note_3
#process
#process_payment
#process_procurement
#process_procurement_steps
#process_sales
#system_bank_application
#system_erp
#system_payment_segregation_of_duty
#system_sap
#system_three_way_match

Transcript

SP1: What is your background, regarding education?

SP2: I myself studied Economics in Tilburg at the university and after that I did the post-master Accountant, also in Tilburg. That is now about eight or so. #general_information_education

SP1: Yes. Beautiful. Okay. What is your current role within Baker Tilly?

SP2: I am a senior manager in the audit practice, most of the time, and also a part of the activities of the Finance branch, takeover investigations, but most of the time I am just an accountant, so to speak, in the audit practice. #general_information_current_role

SP1: The best thing there is, right?

SP2: Yes, if you say so.

SP1: I sometimes hear it.

SP2: It is very beautiful, but entrepreneuring is also beautiful.

SP1: Yes. Exactly. Okay. Then I'm curious… Do you have any experience with continious monitoring or automated controls?

SP2: Well, of course with our control approach with application controls, for example, but not that it happens on a continuous basis. However, it is tested once a year, that the operation is determined, the same applies to control strategy and matches, things like that. Yes.

SP1: Okay, so you haven't actually done much with it yourself, but you do see possibilities.

SP2: Yes. Idon't know exactly what you mean by it, eh, if you say that we control the customer's process and something is not quite right, we don't do that. We don't do that. #general_information_cfm_experience

SP1: No. Okay. That's a good one. Do you have customers who might be interested in this, for example?

SP2: Depends on what you mean exactly. If you say, "Yes,I'm talking about continuous process monitoring, ”I think some customers do. I just think they do that themselves and they don't let the accountant do that. #general_information_cfm_experience

SP1: Yes. Exactly. Really the internal control.

SP2: Yes. That is, of course, quite a lot.

SP1: Okay. For this research I want to look at the business typology trade organizations, just to scope, because I would of course prefer to capture all controls, for all the different processes you can think of, but unfortunately I do not save that, in terms of time, so opted for the type of trade organization and then purchasing - and the sales process. Do you have trade organization type customers with these two processes?

SP2: Yes enough.

SP1: Enough. Look. Do you have any idea how many there are? Are we talking about ten or rather about fifty?

SP2: Customers I serve now?

SP1: Yes, of the trade organization type. That may just be a good bet.

SP2: I now have about twenty customers, which I really have in terms of customer reach, of which I trade… About six or ten. #general_information_amount_trade_organizations

SP1: Exactly. Well, good. Then I can derive some value from your answers.

SP2: I've been doing this for fifteen years, so I've had enough customers. #general_information_experience

SP1: Yes. Exactly. Okay. Then I am curious about your approach path to the control of these two processes, because if you start an audit for one of these customers, I think the first thing you will have checked is the ITgeneral controls. Is that right?

SP2: Well, that is one of the things that we naturally have checked, but the basis is that we know how the processes work for the customers. "When you talk about purchasing and sales, how are those processes going?" and then in the broad sense of the word, including the use of IT systems that underlie this. #audit_approach #process

SP1: Yes. Exactly, so you have to really understand how those processes, indeed, work, to know if you are controls.

SP2: Yes and that there are IT aspects, but certainly not that it is only IT. #fd_structure_it

SP1: No. Exactly. How do you determine which controls you will use, within such a process?

SP2: Well, you look first how the process works of: "Well, I'm going to use it." Then the question is: "To what extent is it documented? These can be reliable controls, but to what extent is it documented? " and if it is IT, it is actually by definition documented in the system, but then a very important precondition is that you can do something with that documentation, so there we have a piece of ITGC as a precondition. Well, if there is, then it is only an option at all to rely on that internal control, but the question whether you want that is often also an efficiency issue, further perspective, especially if you only have relatively small customers and you are talking about trade. We often think that IT is not good enough for those customers, so that does create problems with support for internal control measures. You might not expect that, but it is, and it is often driven by the fact that we simply cannot lock on those preconditions. #audit_approach

SP1: No. Exactly, but that's actually a decline, right?

SP2: Well then look into the system for access security and stuff. This is important. Legal protection in systems. There are few customers who have sufficient mastery of that and the standard that is maintained there and it is getting higher, so that's a bit of a problem, especially in rights in all systems. No one customer has mastered that. #control_it_general_access_protection

SP1: Okay and that's just because they are too small to do this?

SP2: Sometimes because they are too small, sometimes because systems are simply complex. Sureto determine it. For example, I have one of my customers, Swiss Sense, who have a very advanced SAP system, which hundreds of people have access to. The question is, "how are you going to find out about the roles and rights they have?" where you have thousands of rights out there, that sometimes bite each other and the customer really has an opinion about that. He really manages it, but then you set a bar against it, a norm. Then we want to see that they actively manage this and that often goes wrong. #system_sap

SP1: With that last step, then? The last few steps? The complexity and above all: if one is already set up, will it be kept up to date?

SP2: Yes, demonstrably tracked. That traps people.

SP1: Okay. That's an interesting one.

SP2: I also see it a lot more, because I checked stock market funds for this, DSM and companies like that, and you actually saw that those IT auditors hardly test IT controls. All they do is general IT control and usually conclude that it is not good or not demonstrable and then go more towards data analysis or sometimes a bit of process mining.

SP1: Yes and it stays there. Okay.

SP2: Yes.

SP1: Interesting development. I have not yet seen or heard it. Okay. If you then look at the control of those processes, they are controls that you use the same with an IT-like control, where you can rely on IT as when that is not possible or do those controls actually differ?

SP2: Those differ. These are basically intended to cover risk. They work in much the same way. For example, if you're talking about one three-way-match when purchasing, you can do that in the system or you can do that manually. Yes, that differs. The method is different and the determination is different, but the background, the idea, is of course the same. #control_tree_way_match

SP1: Yes. Exactly. Okay, so only the way you're going to do it is different, but the idea of, "You want to check those three things," remains the same?

SP2: Yes.

SP1: Yes. Exactly. Okay. If we take a look at the purchasing process, you just mentioned the Three-Way-match. What are the controls that are most, most often used in the purchasing process… or actually: what are the controls that you use most often for a purchasing process?

SP2: Purely on the purchasing process is that a three-way match, an order with receipt and an invoice and then underlying how it came about the order, was that done by segregation of duties? They have an invoice and receipt. That is a precondition, but the most important is the three-way match measures. The control is called the three-way match. And somehow ... The basis is the three-way match in numbers, the heading of price. Often price is part of the three-way match, which must match the price with the contract. #control_tree_way_match #data_tree_way_match #control_product_pricing

SP1: Yes. Exactly and you usually have to have this checked manually.

SP2: Well, that depends. Sometimes we just enter this into a system, which we say as a way of saying: “We have a contract with this supplier. If I want to order pens, they cost one euro each. ” Then we will receive an invoice. We have someone who checks whether there is one euro each on the invoice and the numbers follow from the orders, the receipt and the invoice itself. #process_procurement_steps

SP1: Yes. Are there any further… because this is mainly the most common, but there are still more controls that you often use?

SP2: Yes, if you go to payment. I don't know if that is part of your research, buying and selling, or if payment is part of that. #process_payment

SP1: Yes. Sure.

SP2: Well, there are often measures in it management of creditors master data, change master data of creditors, and what rules are there? Actually a kind of four-eyes principle. Subsequently, there are also internal controls with the payment. As a rule at the bank that not everyone is allowed to pay just like that, using the four-eye principle, but usually the check takes place through such a payment list, which then reads: "Would he really have received it and approved it himself?" #control_change_creditor_master_data #control_payment_segregation_of_duty

SP1: Okay. In the meantime I am writing along. Those are indeed three checks that you do when paying at the Finance piece. Are there further checks on your stock and the like with your purchase?

SP2: With the stock?

SP1: Yes. At least within your purchase. That Three-Way match already covers a lot. I'm just looking. There you have no further controls at?

SP2: Not on the purchasing side. Well forthe whole circular inventory and stuff.

SP1: Okay and then the same for sales, if we have purchasing a bit, because what are you looking at on the sales side?

SP2: That is a difficult one, because it is, I think, very dependent on the business model of your customer. That can really be very different. You have trade and commerce, but that is also where it starts: "How does the customer work now?" Look. I work for Swiss Sense, for example. If you go to Swiss Sense in the store, you can buy a bed there, but it is not the case that you walk out with a bed on your shoulder. Then you order a bed there. They order this at the head office and then someone else will deliver your bed to your home. Then you have to pay a part in the store and the payment is made upon delivery, so to speak. This ensures that various people are involved in such a sales transaction, so that there is a whole function statement. The person who will buy the bed in The Hague has no idea who will arrange the delivery at the head office and has no idea at all which driver is on the truck, who will eventually deliver the bed to you in The Hague. If you are not talking about Swiss Sense, but you have the Shoe Giant, a shoe store, you enter the store, you take out a pair of shoes, you go to the checkout, you pay it and they will never see you again.

SP1: So how would you do that for such a shoe store?

SP2: At a shoe store you are talking about branches. There are often several branches, if you are talking about a large chain.What is often the measure there that they are not allowed to buy themselves, to prevent a store from being created in a store. In addition, those people often get some sort of bonus based on sales. That is also, in particular, a measure to ensure that everything goes through the cash register. Furthermore, you can often compare the same branch with each other because you have several, what are the margins per branch, turnover per branch per day, even per seller, because the customers, in general, at such a checkout ... That the seller badge must scan, that is the one with you, so you also know exactly per employee what the turnover is. #process_sales #control_branch_comparison #control_seller_badge_scan

SP1: Again. What kind of analysis did you call?

SP2: "Branch comparisons," I said

SP1: Yes. Exactly. Branch comparisons, to see how that works. Okay, so then you can already see that the purchasing process is more dependent and therefore a little more difficult to test. #general_note_1

SP2: A lot of customer specific. It depends on the business, because I have now mentioned two companies that you feel may be very close together. They can literally sit next to each other in the shopping street. Both are sales to private individuals, but there is essentially a completely different

internal control. When you talk about trade, if you supply trade to companies, the alert changes. Or where you do not even see the goods physically at all, because you do. #general_note_1

SP1: Yes. I find it clear. Then I would really like to go back to the purchasing processes and I am especially curious about what data is needed to test the controls, so what you need per control and what type of systems that comes from. Well, I can do that part of 'what type of systems'... That's pretty straight forward, I think, but if you look at that Three-Way match, for example, orders equal to receipt, equal to invoice, what systems do you come often against this, where this data is in?

SP2: These three are generally in an ERP system. They can all be in themselves. Every system can do this, I think, at its core. #system_three_way_match

SP1: Okay. It is, I think, just plain clear. You then have as dates your list of orders, your list of receipts and your list of invoices and you will check them. Does this require additional data? Then you look at roles again, I think, the people who have authorized it. #data_three_way_match

SP2: Yes, that is a precondition generally eh, where does that data come from? You would expect that order receipts are only entered by the Warehouse department, for example. That is then something you will look at. That is next to our Finance department, which ultimately has to check invoices, for example, that they also fill in the receipts. Something goes wrong there. So in general you want to have a separation of functions between the three steps determined by three different persons and not three different persons, but persons with a different role in the organization, who have provided three pieces of source data, so the order by someone from the Purchasing department , the receipt by someone from the Warehouse, the invoices are processed by someone from Finance, say. #fd_structure_warehouse_department #control_three_way_match

SP1: Yes, and when that is not the case, that it is not done by three different people, can you then immediately shoot off that control or is it not that bad?

SP2: Well, in our industry with not 100% professional companies, there is always an exception. Then the question is actually: "What can we still do with it?" In practice, you do have a challenge every week and it may be that there are an X number of transactions, in which the segregation of duties has not really taken place. You can then find something about it, depending on how much or what amounts it concerns, whether that is reasonable, or whether you can understand that. It could also be - as I had last week - that it is very well arranged in itself, that order, receipt and invoice processing is done by different people, only the entire processing in the system, which was only done by the department only Finance. So there was a whole stream underneath, with papers, where they received some list of received goods upon receipt, which they actually gave to Finance. Finance said: "We received this in the system and then the list was thrown away by Finance." If you then look into the system you will see that Finance has received a receipt and that it is approved. And underlying there was a list and if the customer is smart, they still keep those lists of receipts and put an initial of that man on it, but yes, if not ... That is often what happens with our customers . They use an ERP package as a kind of luxury Excel sheet, but not as a control tool. ”If you then look at the system, you will see that Finance has received a receipt and that it is approved. And underlying there was a list and if the customer is smart, they still keep those lists of receipts and put an initial of that man on it, but yes, if not ... That is often what happens with our customers. They use an ERP package as a kind of luxury Excel sheet, but not as a control tool. ”If you then look at the system, you will see that Finance has received a receipt and that it is approved. And underlying there was a list and if the customer is smart, they still keep those lists of receipts and put an initial of that man on it, but yes, if not ... That is often what happens with our customers . They use an ERP package as a kind of luxury Excel sheet, but not as a control tool. #process_procurement #system_erp

SP1: And then with totals, when checking creditors master data? In that, you actually look at the same thing again, don't you, with the separation of points, for adapting it?

SP2: No.

SP1: Accounts payable master data, control thereof.

SP2: Yes, if that is already controlled, because that is not always smooth, but who can change creditor master data at all? Is that also someone who can organize payments? Hopefully not. And ideally that also happens with the four-eyes principle, changing creditors master data. #control_change_creditor_master_data

SP1: Four eyes, indeed and hereby? Do you see that this is often well organized or is it not that easy?

SP2: This is usually not very well arranged. No.

SP1: No. Okay, because I've seen that myself at municipalities, that they do have that in their standard package.

SP2: What then? Also that the four-eyes principle is applied?

SP1: Yes, it too four-eyes principle, for a check, approval. #data_change_creditor_master_data

SP2: Which is also mandatory?

SP1: Yes, it is also mandatory. That's a good one indeed, because you can have the principle, but if it's not mandatory, then ...

SP2: They can't get around it, say? It is not the case that you can still pay if it is not automated?

SP1: No, we saw it that way, at least.

SP2: Because with most bank packages… With your creditors, master data - I don't know if you looked at it - are often in some ERP package and that must go to a bank from ERP, if they want to pay. You do not want to know how often you have an ERP, but that you have it close, that you then come to the bank and then you can happily change everything or even from a file, usually that is such a file that you have something from the ERP download, which places somewhere on a server and then reads into the bank, you can also open that file in a Wordpad and you can adjust the bank account. You see that very often, so yes, it is closed, yes, in ERP but in ERP you do not pay. Apart from manual payments, because they are also used. That's just going straight to a banking package and typing in a payment there. #system_bank_application #system_erp #general_note_2

SP1: Yes, so you actually check all of those things. You all have to check to be able to say anything about this control. #general_note_2

SP2: Yes.

SP1: And if you look at ... Just take a look. That is it four eyes principle. That will be on the control of the payment list. That was actually the third you mentioned. What do you look at with that control?

SP2: It is often with customers who that process is completely 100% closed, the creditors master data and so on. What they usually do then is the payment list that is in bank packages, actually pay everything, test there on the basis of samples or something, participation. Is there really an invoice underlying this payment, we have approved the invoice internally and write down the bank number with the payment list and complete with the bank number what is in that invoice. This way you keep a lock on the door, because the entire process for it becomes more transparent. #data_payment_segregation_of_duty

SP1: Yes. Do the invoices actually match the bank rules? Okay.

SP2: And if you don't pay attention, a customer will only do that from ERP, because it also contains a payment advice list. In itself it is nice,only you still have the point that it is also an interface with a bank and that you may be able to adjust something in the bank yourself. #data_payment_segregation_of_duty

SP1: Yes. Is that then completely covered? Then you just have to have very good banking software or in your banking software you should have arranged the segregation of duties and segregation of duties. #system_payment_segregation_of_duty

SP2: Yes, that is also a precondition and who can read all those files, who can change things. So that is actually a basic precondition that you must have, that your banking application is properly set up. A few years ago it gave a payment package from SAP or whatever a hash total, if I had changed something in the meantime, then that bank package saw that, because it calculated that hash total again and compared it with the piece that was printed on that batch from SAP and if it was not countable then you just got an error. Then you could not pay the batch. That was a really good measure, but those banks no longer do that. #data_payment_segregation_of_duty

SP1: Okay. Yes. That's a good one. So that banking application actually crosses all processes, doesn't it?

SP2: This is approached in the section procurement, also in a section of pay, I think. If it pays, it depends on how you explain it, but the most important thing is often with the suppliers and your staff.

SP1: Yes. Okay. Clearly. Then I am almost through the questions again. It is actually too much for the sales processcustomer-specific to further say something about this, in a general sense, what kind of data is needed to perform this check automatically.

SP2: Yes. Then you really have to take one case, simplify it and look at it, because it is so different.

SP1: Yes. I understand. Do you see the added value in thistest controls several times a year? It's more like, "What is your opinion in that sense?" Would that be useful? Is that really adding value?

SP2: Added value for me as an accountant or for my client?

SP1: Actually for both, starting with the customer.

SP2: Especially for the customer, I think, but I think that customers often do that themselves, if they find it important, so that's why there is added value, otherwise I don't think so and things like Three-Way matches, they monitor that, handled by dropouts. And you already have lists like that, so customers monitor the process continuously throughout the year. It is often the case that once they have set it up, the software, the technical layout, they will not assess that every week. #general_note_3

SP1: No. Okay, so that's one of those preconditions. Can you then rely on that control carried out by the customer? Well, if a customer says, "We have these, these and these mechanisms to control that Three-Way match," can you rely on that? Do you assume this or does it really have to be checked again? #general_note_3

SP2: Suppose the customer says, "All our store invoices go through the Three-Way-match," and that looks at the numbers, too, and a deviation of half a percent or less is good, then we can accept that, but if that is more is then it should be on the signal list. You just can't, so reject it at first. You might be talking about that kind of controls. You will have to determine that this control has work all year round and not just by chance the one day you are looking at it, which is why change management is so important, for example, the preconditions. #general_note_3 #control_it_change_management

Interview 2 with RA2

General interviewee information (#general_information)

Bachelor / Master study	AA and RE training
Current role	Accountant in Audit
Continuous Financial Monitoring experience	None
Amount of SMB Trade Organizations	5 to 6 organizations
Amount of experience as accountant	17 years

General notes (#general_note)

1. No experience with Continuous Financial Monitoring due to the lack of IT maturity / general controls.
2. In the optimal situation, one would always confirm all data from inside the company (orders for instance) with data from outside the company. So, requesting the orders that have been placed from the suppliers.
3. Most controls can only be tested if IT general controls are sufficiently functioning.
4. Continuous Financial Monitoring will save a lot of time during the audit. Samples can be made more specific and the auditor can focus on the actual justification of purchasing and the commercial nature thereof.

Approach to start audit (#audit_approach)

1. What is the business revenue model.
2. Where in that business revenue model is room to temper with the revenue streams.
3. What are the business processes.
4. Defining relevant IT systems.
5. Perform risk analysis using fraud triangle.
6. Define controls.

(Financial) Department structure (#fd_structure)

- Finance department
- Warehouse
- IT
- Procurement and Sales

Processes, Controls, Data and Systems (#process, #control, #data, #system)

Control	Type / Process	Description	Data	System
Access security (it_general_access_protection)	IT General			
Change management (it_change_management)	IT General			
Three-way-match (three_way_match)	Procurement	There has to be segregation of duties	- Order - Goods receipt - Invoice	- Oracle Cloud (ERP)

		between 2wordering, receiving the goods and payment of the invoice. It also shows per transaction that is been honest. The three-way-match	- Message traffic (EDI)	- Banking application
VAT (vat)	Sales / Procurement	Ensure that the VAT code is set correctly in the system.	- Application settings	ERP
Turnover (turnover)	Sales	The amount of sales (Q) can be tested by the inventory at the end of the year minus the inventory at the begin of the year. In between, the amount of sales and failure can be seen.	- Sales orders	
Product pricing (product_sales_pricing)	Sales	The sales price of a product should be properly defined. Who defines the sales price and has it		

		been done properly.		

List of unique used keys

#audit_approach_define_controls
#audit_approach_it_landscape
#audit_approach_revenue_model
#audit_approach_risk_analysis
#control_it_general_access_protection
#control_it_change_management
#control_product_sales_pricing
#control_three_way_match
#control_turnover
#control_vat
#data_bank_information
#data_creditor_master_data
#data_edi_messages
#data_three_way_match
#fd_structure
#fd_structure_financial_department
#general_information_amount_trade_organizations
#general_information_cfm_experience
#general_information_current_role
#general_information_education
#general_information_experience
#general_note_1
#general_note_2
#general_note_3
#general_note_4
#system_bank_application
#system_erp
#system_financial_administration
#system_inventory_management
#system_three_way_match

Transcript

SP1: What is your background in this?

SP2: Well my background is at Baker Tilly financial audit. So I do financial audits where I have always been interested in yes how you could give IT a better interpretation. Here the focus is SME. So it is always a challenge to give IT substance, but that is why I am now also completing the RE training. So yes, in that sense I do see opportunities to shift. Only that is an option but also a very big challenge. #general_information_current_role #general_information_education

SP1: Yes, exactly. And that is RE after the RA training.

SP2: I did not do RA training, I did AA training. #general_information_education

SP1: Okay.

SP2: Only I, since 2003 working in the audit practice and switched from the assembly practice to the audit practice, I made that choice at some point. #general_information_experience

SP1: Yes cool. Okay. Nice that RE training then, I think Martin should be very happy with that. Still a kind of supporter that you can discuss together. #general_information_education

SP2: Yes, I also spoke to him for a while so that is fine.

SP1: Yeah okay. And your current role is indeed in the audit.

SP2: Exactly financials audits within SMEs. Financial statements audits. #general_information_current_role

SP1: Do you already have some experience with financial monitoring, continuous monitoring or to perform such checks in an automated manner?

SP2: Not by virtue of an audit firm. Particularly because you can make so limited use of the general controls, that the information that could get out of it that you would have to provide so much data in order to obtain information assurance value from it. Yes, the disadvantages do not outweigh the benefits with the work involved. #general_note_1 #general_information_cfm_experience

SP1: Yes exactly, because it is just too common that those SME customers do not have the general ID controls in order and you simply cannot rely on them?

SP2: It is the rule rather than the exception.

SP1: Yes, exactly. Okay. And on advice to adjust this, then we can help you much easier, you say that is actually not.

SP2: Well that is also very difficult and therefore, it obviously takes a lot of investment and the IT that develops is of course also very hard where you could say now, given all Cloud solutions that are available, that there is now the chance because we think about it better and make the right decisions. Because by definition you already have a design in which part of the general ID controls have already been sufficiently implemented via the Cloud solutions that are available. This depends on the choice made and to what extent Cloud applications are used.

SP1: Yes, exactly. And would some Cloud applications be better suited to that because they no longer have to do many general matters themselves?

SP2: Right. Then you are only talking about management and organization and logical access security. #control_it_general_access_protection

And a piece of change management and the like. Yes then you don't have to worry about it anymore. And also general access security, because within Baker Tilly we have two aspects of access security. #control_it_change_management

You've probably seen that before? Let's just say network path, to put it plainly and the logical access protection within the application itself. Then I am not talking about the overall security measures against external infringements.

SP1: No. So just the accounts.

SP2: Exactly.

SP1: The actual accounts.

SP2: Yes.

SP1: Okay interesting. And also nice that you can see the added value of this, you can of course do a lot with it in the future.

SP2: Yes.

SP1: Just to cut right in. Do you have customers of the type of trade organization?

SP2: I have that one.

SP1: And are there many, about how many are we talking about?

SP2: Take a look, count it. I quickly think about five or six. Of course they are bigger customers, so I think they are five or six trading companies. #general_information_amount_trade_organizations

SP1: Yes exactly okay. Then I also know how much, yes beautiful. And what is your approach at the start of such a check? I think you will first look at the customer's process, how are those purchasing and sales processes put together.

SP2: No. The approach is initially and that is fairly new, but we have always tried that because the first approach route to use. What is the revenue model of that customer, where exactly is the value. That is the first question we ask. If you know that, you immediately know where there is room for control in your results and control in prices, because if you are talking about trade organizations, that can be clearly framed into a good movement in the price component and quantity component. That model can be in quantities but can also be in prices. You first try to find out and then you also know with what approach you can ask the questions surrounding the processes. #audit_approach_revenue_model

SP1: Yes and then you go after the processes third?

SP2: Drawing up an overview of the IT landscape is part of the processes and those processes. IT landscape means, relevant to you, that we look at which processes influence which applications. This is what the process match matrix calls, but we also try to summarize that in one scheme. And we also compare that with typology that is relevant. So basically we are trying to translate the value of the recycling process into IT applications with associated access from outside or from the office or where the server is located. Not a technical drawing but just very simple for a layman to understand. Here is a computer, which is a server, for example there are the stock data. In Groningen there is a CRM application so to speak. It has no link or a link with such drawings. #audit_approach_it_landscape

SP1: How can you do that and things like that.

SP2: Yes, an office worker may be added, a customer may be added, the messages will be posted incorrectly, things like that.

SP1: Okay. That's a nice approach indeed. Especially the view from the earnings model. Okay. And after drawing up that application process matrix, do I think you will determine the controls based on those applications?

SP2: No no. Before you start doing this, you first do a number of other things that all support your risk analysis, because your annual audit starts with risk analysis. Risk analysis consists of analyzing events that could affect the financial statements. Because that is ultimately the goal, we must issue a statement regarding the fairness of the annual accounts. So the numbers that are there and the information it contains, explanations and so on must be truthful. Accurate, complete and all kinds of claims are part of that. Well, the risk approach means that we actually inventory all items, all processes, for possible risks. Initially not taking into account controls or other internal controls. #audit_approach_risk_analysis

SP2: Then we weigh those risks with possible impact and chance in the fraud triangle. #audit_approach_risk_analysis

And the next step is okay, which processes may influence those risks in a positive sense and which control measures are in place. That's just going through the process, the line check. Conducting interviews, looking at the extent to which there are controls and to what extent we could use them in the audit. And controls are very broad. Manual controls, IT, depended manual controls, which has become increasingly relevant by the way. Application controls authorization controls. #audit_approach_define_controls

SP1: Yes. Indeed, it takes those pieces. And if you look at the actual end of the ride, are you going to determine the controls yes well then you are actually going to see which controls can I use.

SP2: Yes.

SP1: Which controls are available. And when you look at the purchasing process, which controls are so common?

SP2: Well the controls normally on the front that focus on the integrity of the goods movement, incoming goods movement. This means that there must be a segregation of duties between the orderer in the first instance, arranging goods receipt and payment of the invoice. #control_three_way_match

SP1: That's that three-way match? #control_three_way_match

SP2: The three-way match that shows it. There must be a separation of functions first, that is the precondition. The three-way match is more of an activity that shows that there is control over that segregation of duties. And that three-way match also shows per transaction that the transaction has also been honest, so that order corresponds to goods receipt, corresponds to invoice and corresponds to the agreed price. #control_three_way_match #data_three_way_match

SP1: Exactly. So indeed your separation of functions is a precondition, it just has to be arranged.

SP2: Yes.

SP1: Incidentally, does that often happen that it is well organized?

SP2: No.

SP1: Oh no?

SP2: Well it is well organized, but we cannot see it.

SP1: Okay.

SP2: That's the point. Be sure to look at those large trade organizations that have really arranged that well, but yes, we used to be able to find several initials on every invoice. On the basis of the initials list, we could also see who set that initial when and what does that initial actually mean. Goods are received in accordance with order. Invoice is in accordance with goods receipt and order. Invoice is posted in the financial administration. VAT is good, coding is good. Well that kind of initials were put in the past. Now that is different nowadays. If I have one of the trade organizations in mind, an order is simply booked in Oracle Cloud, the goods are received via a logistics service provider outside the organization. It provides a dump of the goods receipts that have been imported or imported into Oracle Cloud and Oracle Cloud ultimately takes care of the processing of the invoice for the three-way match because the invoice has the same purchase number. So that

is more digitized but again it is not visible. #control_three_way_match #data_three_way_match #system_erp #system_three_way_match

SP1: No okay and how do you check that?

SP2: Data-oriented. He will eventually get the goods movement and the three-way match if you talk about the side of the purchases and the price setting and payment, yes you also check that on the basis of goods receipt. #data_three_way_match

SP1: You are going to calculate and combine them yourself, then you do that with your sample, grab him an x percentage of the transactions?

SP2: Yes depending on the risk, because the question about risk is what you see with that company.

SP1: Yes that's true. And would you, because in principle these are three lists of data. Your purchase invoices or your purchase orders, your goods receipts and your invoices.

SP2: Right.

SP1: Could you also take that complete list of data and just put it side by side?

SP2: No because you are comparing system with system. I mean system a with system a. And that is only possible if you can enrich that data analysis with data from third parties. We also try as much as possible. If I am talking, for example, about that part of the procurement from the organization that I now have in mind, we ask for balance confirmation. So then we just go to the external suppliers. The suppliers who simply indicate how much has been delivered in both Q and P and we put that total next to the list, after which we can possibly repeat that three-way match with the data analysis. And because it is still in its infancy, the follow-up to bank payments. #general_note_2

SP1: Okay, because you can indeed do that three-way match, those three dates are usually in one system, so you always have to go to a third party to verify that? #general_note_2

SP2: External information outside the system. #general_note_2

SP1: External. And can it also be information outside the system that is available within the company?

SP2: Yes like banking information. #general_note_2 #system_bank_application

SP1: But actually more data sources than bank information or does it stop there?

SP2: You also have messaging with companies.

That is not the case with this company, but it is good that I come across EDI messaging around purchases from the main suppliers. The stock flow in itself is not within the organization, that is outside the organization of course. Furthermore, there is not really digital data that I say well you can do something with that. Yes, the creditor master data, you might be able to do something with it sometimes, but that is often very difficult to disclose. So the data is there only the unlocking of it is then such a big challenge, that it takes so much time with the knowledge that is limited with the customer that we say that it is more efficient to spend on that point for example. Then we will not do the entire sample on all elements of the purchase, but the part that we cannot find out, we will then include in the sample. #data_creditor_master_data

SP1: Yeah okay.

SP2: The disadvantage of this is that you have to check all other elements because if something is wrong and you have not seen it then you have not done it correctly.

SP1: No no no. And if, just a side jump. The moment you come to check all data in the system, all data from the three-way, well all data from the system. For example, everything that is in the system can be characterized by the bank details, should you still check whether the system is actually integer? Because your starting point is your bank details.

SP2: That depends on so many factors, you cannot say that one two three. It really helps in the sense that a bank, yes, you can do that with integrity. #system_three_way_match #system_bank_application

SP1: Yes.

SP2: So that supports the reliability of the moldings. It is a bit of a theme in every audit of the annual accounts and also the moldings we get, we must have established the reliability of that.

SP1: Yes, exactly.

SP2: That means that parameter, period cut is a very important where standard applications are concerned. Change management then becomes more relevant because you really have to research it as a theme. A piece of precondition. And you have to see whether you can check all aspects that you want to check or that they can be overcome with the other external information. #control_it_change_management

SP1: Exactly.

SP2: So it is again very much dependent on the risks you see and want to cover.

SP1: Yes. And there it is, yes I get it. Is there such a purchasing process even more different controls that you see there by default?

SP2: Yes, then of course you are talking about foreclosure of payment powers. Controls that we generally do not use, but which are there, are the VAT controls. It is of course an application control that ensures that the VAT code is correctly reflected in the general ledger. #control_vat

SP1: Okay.

SP2: There are also application controls that show for an order where the goods receipt differs from the order. It will not necessarily be given the status abyss, it is not yet finished with the tree-way match, shall we say. In principle, this is an application control only, which again belongs to an IT depended manual control, because the moldings that come out of it must be handled by a buyer who says hey those differences, the outlayers what should I do with that. If the order was not registered correctly, it will go back to the source and it will be completed in that sense. Only that is often so poorly regulated in terms of powers within the process that you can not rely on it. So then we will also look at those outlayers ourselves. Disruptions in the money goods movement.

SP1: Yes.

SP2: But they are application controls that are out there but don't use them.

SP1: Exactly because you cannot rely on the generals.

SP2: Exactly yes.

SP1: Okay. And then we have had the purchasing controls a bit, I think.

SP2: I think so.

SP1: Yeah okay. And if you look at the sales process.

SP2: In that sense, exactly the same applies to eh. That is the registration of a sales order in relation to goods issue in relation to the processing in the financial administration. In so far as it is a separate function and the authority regarding price fixing. So by separating the function between issuing goods and processing an order that has to do with the Q component.

And the P component in that sense is actually much more relevant for an audit of financial statements at a trading company. Particularly because the turnover, the Q component, ends up in that turnover. If you do an annual audit at a trading company, you will look at the initial stock and the final stock, the Q component that you count or whether you do a sample or keep an inventory. In between are the purchases, we have just talked about that, there is also that piece of three-way match and Q-buyer at an outlayers you check. And the results must be the Q component of sales. #control_turnover #fd_structure

If that is not the case, then there are other faults due to the failure, containers that have fallen over, I will just name it. So that is the Q. The P-component is often much more interesting in that sense because yes, who determines the price when entering into sales transactions? And is that person allowed to do that? #control_product_sales_pricing

SP1: Yes. And is it also interesting how that price is determined? Or isn't that so exciting?

SP2: You should put that next to the earnings model, because you start there again. And that earnings model would mean that in the business exploration we know okay at this article group or at the total level, we would expect that an margin of x percent should be realized. That is margin, so that is sales price minus purchase price, but determining that price in itself is determined by powers. That is also often not visible, especially with trading companies where it goes very quickly and where you have to deal with suggested retail prices in a store, for example. Look at a toy wholesaler who does games, yes, of course, a Bol.com says that a puzzle or a game must be placed on my website at a price X, but you ensure a good cost price for me. There is a certain market agreement for that kind of thing, there is a specific framework agreement for that. But well, they are also dependent on people. Annual contracts. #control_product_sales_pricing

SP1: But I think they are registered in that system, right? The moment a price changes.

SP2: Yes at transaction level. Yes, there is the bugs, because who changes that price or who exactly registers that price and who may determine that price? There are often far too many freedoms, so you still have to have compensation control afterwards to determine that no accidents have happened. #control_product_sales_pricing

SP1: Okay if the product has rolled over the counter way too cheap.

SP2: Exactly. You do not have to be very afraid because it is simply not paid to the debtor. That is the link that we also establish, the existence of those debtors. Then you will finish those debtors neatly.

SP1: Yes.

SP2: And then I can go there too, not at a Baker Tilly but to give an example from the past of a company where that was really a problem. Onion wholesaler or onion nursery or grower what do you call it, but well it also had a very incoming flow of onions. You can see that part as a trading company. There was a lot of export there. Everything was recorded digitally.
And the problem was that the price was agreed with the customer afterwards. That is a problem. The second problem was that debtors were not all through the bank, but also through cash flows. And the third problem was that the debtors did not always go through the memo through money flows but also through write-offs. Well then it stops for that P-component because the integrity of that P-component can no longer be determined afterwards. And then you can use so many data analyzes, it ends there for a while. That is why we start with the revenue model and then we look at which piece of data analysis would be suitable and will you then focus that data analysis on

certainty or will you focus that data analysis on, well let me say mapping exceptions. We call this work exploratory or process mind-like. I haven't actually done that first anywhere. That exploratory data analysis, apart from indeed looking at it, is more to get confirmation that what the customer tells me is reflected in that data.

SP1: Yes exactly where it comes from.

SP2: Yes.

SP1: Okay. Are there other components or other controls when you look at sales?

SP2: Yes, the authorization controls apply to both purchasing and sales, so the powers within the systems to perform certain actions. So entering into sales transactions but also changing the stock. These are all authorization controls that show that there is a separation of technical functions. #control_it_general_access_protection

SP1: Yes, that stock is not simply written off.

SP2: Yes. So on the one hand that is a precondition, but on the other hand it is actually also a control that should adequately mitigate the risk and the challenge of that is how do you determine that this happened in the system all year round.

SP1: Yes, you can never say that with complete, with one hundred percent certainty, of course, unless you have a Cloud application.

SP2: That also depends on the Cloud application, some Cloud applications keep the history and some don't. Or have the history but that cannot be determined.

SP1: No okay clear. Yeah okay. The controls you mentioned a bit are generally the same for your different customers or is it also very different?

SP2: Yes, basically these controls are necessary and they are generally present, but they are decorated in a different way and have slightly different accents.

SP1: Okay.

SP2: If you are talking about a beverage wholesaler, there is still stock of drinks at all, and there is a specific check on excise duty. That is an additional check that then takes place. So that can actually mitigate the risk for a piece but if they do not have that in order, they also have a very big problem because then they lose their how you call that excise goods place, that has at least a certain status, a certain permit to work with excise duties in this way.

SP1: Yes. Yeah okay so that testing on that kind of checks could be interesting for a company itself?

SP2: That is for the company, well not so much testing but making sure that everything is in order, absolutely. Look and there are also just tests from the tax authorities, but they do not report. So we can't do anything with it.

SP1: No. No, you cannot derive any rights from that?

SP2: No.

SP1: Okay. Let me think. Then I have the following question. Which data is needed to test the controls and from which systems does that data come, but actually we do now. For example, message traffic about an order that actually comes out of your mail traffic.

SP2: Yes or EDI. I have one that has EDI registration.

SP1: Okay. What kind of system is that?

SP2: Let's see, yes that is quite old, that is a Navision based system only that Navision version is just very old. There is a kind of fixed format designed to let the larger transactions simply process the purchasing transactions within the customer's financial administration. So what we did then is compare that EDI message traffic to the actual purchasing transactions. #data_edi_messages #data_three_way_match

SP1: Yes, but manually?

SP2: Yes, we did let one of the data analysts or one of the IT auditors look at the message traffic. Is this suitable to use to connect that? But that is again to get an external confirmation of what was processed in the system of income at that supplier because it was a large amount.

SP1: So if a customer would have two different systems that, for example, would not be fully integrated, you could say that you can perform your check more easily because actions take place in two systems, so you can compare data from one system or you can not that.

SP2: That depends on the system. Just think, how can I best explain that. Imagine you have a separate inventory management system compared to your financial administration. They are two different programs. Even then, you can make use of this only if the precondition is, say, sufficiently filled in and then you are mainly talking about access security. You also see that financial people cannot do anything in that inventory module. And that they cannot reach it in any way. That is a utopia in SMEs. So different systems within the same customer require even more attention to the general ID control before you can compare that data at all. So then you go outside that company again. What really happened. #control_it_general_access_protection #general_note_3 #fd_structure_financial_department #system_inventory_management #system_financial_administration

SP1: So the most reliable moldings I hear from this is actually bank information, you can always rely on that? #data_bank_information

SP2: Or information from outside the entity. We mainly try to look for that. Information from outside the entity that can underpin that data within the entity for integrity. And that does not necessarily have to be digital information, which can also be external other source information. Without samples because confirmation can also be very strong to say oh this data is indeed in accordance with reality. #general_note_2

SP1: And do suppliers often help with this? The delivery of.

SP2: That changes. If you operate internationally, it is a bit more difficult than if you have the Dutch market.

SP1: Just okay. How do you see the added value of testing these controls that we have just discussed several times a year?

SP2: In the end it will save a lot of time, because I think if those controls are tested several times a year or continuously where you would like to go, that means that you can actually just extract the integrity of that data from its financial processing . That means you can reduce your samples a whole lot. So that you can organize your samples much more specifically. That you are going to say okay those powers around pricing is perhaps the only issue that remains, but that tree-way match has been resolved. If we can make a link in one go between order data, creditor master data, actual changes without taking into account who made those changes and we can directly link with bank data, it will save a lot of work because that means that we have a very large do not have to do part of the sampling work. Then the sample work focuses on the actual justification of purchasing and the commercial nature thereof. #general_note_4

SP1: Yes check. And could your customers also see the added value of this?

SP2: They see that. Yes, they are also open to it.

SP1: Okay so you can, you also talk about it here with your customers.

SP2: Increasingly.

SP1: Yes. And then I am also curious, a recommendation regarding, for example, IT optimization that is reflected in the management letter. Do you see that there is actually something being done with it?

SP2: Is often very difficult. That is very limited, it is done, especially because it is seen that in accordance with our recommendations people do work and yes to close or document such things yes that is not really seen as interesting, because yes what do you earn with that. And two, if you limit matters in terms of powers, you will lose flexibility within your organization. And then SMEs come into the picture again, yes someone who works for an SME that should actually be at home from all markets. One must be able to receive some of each other.

SP1: Certainly, you are the real all-rounder there.

SP2: Yes. And then I think it is not yet a point that that is the case because that is part of it, but then you have to be able to extract those kinds of exceptions from that data.

SP1: Yes, because if someone really organizes all three transactions from a three-way match, it might not be that bad if you just capture it and then check that exception afterwards?

SP2: If it has acted entirely in accordance with the set framework and it is a transaction that runs very normally, has generated normal margins and afterwards it is still looked at within the company, then that was a shortcoming in your internal control on that transaction or on that group of transactions during the holiday periods, but afterwards the company has built in a control itself. That may be a manual check to determine if any accidents have occurred. And we can achieve that again on the basis of source data.

SP1: Yes as long as the data is good.

Interview 3 with RA3

General interviewee information (#general_information)

Bachelor / Master study	Business Administration, Tax and Law at Erasmus University and Accountancy post-master.
Current role	Accountant in audit practice.
Continuous Financial Monitoring experience	Using data analysis for a single control.
Amount of SMB Trade Organizations	3 or 4
Amount of experience as accountant	7 years

General notes (#general_note)

1. Per business type (typology) there is a pretty standard list of things to take notice of and standard risks to manage.
2. If the IT general controls are in place e.g. sufficient password protection, monitoring, and logging of accounts, the data from ERP system is enough to test with. No external data is required.
3. Multiple people always have to be involved in every transaction (e.g. 3 for three-way-match).
4. Continuous data analysis should be the next step in auditing. This will also allow benchmarking to be done and therefore see trends over multiple companies.
5. A Financial Monitoring setup could have extraction teams who focus on gathering the required data and load it into the data layer. The data layer is a data warehouse at Baker Tilly which contains all data such as salaries, active users, financial transactions and more in a structures format. Standardized controls can be run on this dataset which will result in a list of exceptions or outliers. These can be manually checked by auditors. Also, based on the data, yearly trends and benchmarking can be done which can provide valuable insights for the customers.

Approach to start audit (#audit_approach)

1. What are the risks in the financial statement.
2. What are the business processes.
3. Define controls.

(Financial) Department structure (#fd_structure)

- Warehouse
- IT
- Procurement and Sales
- Finance

Processes, Controls, Data and Systems (#process, #control, #data, #system)

Control	Type / Process	Description	Data	System
Product price (product_pricing)	Procurement	In incorrect purchase price is used		

		(too high). What discounts have been granted.		
Product delivery quantity (product_delivery_quantity) This control is integrated in the Three-way-match	Procurement	The amount of delivered products is not correct.		
Payment segregation of duty	General	All payments must be checked by at least two people.		
Turnover (turnover)	Sales	The amount of goods at the start of the year + amount of purchased goods minus sold goods is the amount of goods at the end. Inventory counting.	- Product stock (inventory counting) - Sales orders	
Three-way-match (three_way_match)	Procurement	The purchase order (price and quantity) matches the received goods (quantity) and matches the invoice (price). Matching for this specific control has	- Purchase order - Delivery notes - Invoice Datasets can be very large and hard to extract because of the volume.	SAP (ERP)

		been done before.		

List of unique used keys

#audit_approach_define_controls
#audit_approach_define_process
#audit_approach_financial_statement_risks
#control_payment_segregation_of_duty
#control_product_delivery_quantity
#control_product_pricing
#control_three_way_match
#control_turnover
#data_three_way_match
#data_turnover
#fd_structure_warehouse
#general_information_amount_trade_organizations
#general_information_cfm_experience
#general_information_current_role
#general_information_education
#general_information_experience
#general_note_1
#general_note_2
#general_note_3
#general_note_4
#general_note_5
#system_erp
#system_sap

Transcript

SP1: First of all, what is your background regarding training and the like?

SP2: I studied at the Erasmus University in Rotterdam, where I studied business administration and tax law, where I eventually completed my training as a registered accountant. After that I worked for one of the big four offices for a few years. In particular control of financial institutions and since 2013 working at Baker Tilly. In audit practice responsible for financial statements audits in the region of Leiden, The Hague, Rotterdam. #general_information_education #general_information_experience #general_information_current_role

SP1: Yes exactly. And do you have any experience with anything from Continuous Monitoring, Continuous Financial Monitoring, automated controls? Has there ever been something done with it, what of heard at all?

SP2: Yes heard of, read a lot about it. I have not seen many real examples in practice where real Continuous Monitoring simply takes place on a day-to-day basis for transaction review. But I do a lot of data analysis in my checks. I also manage many control teams by doing data analyzes. #general_information_cfm_experience

SP1: And what kind of analyzes are they then?

SP2: In the context indeed through thesis and trading company, we have attempted at a recent trading company to carry out the money-goods movement and the three-way matching in our control

environment. Is actually a very concrete SAP system here where we try to download the SAP data and then perform our own analysis on it. #general_information_cfm_experience

SP1: Yes okay nice. How many customers do you have approximately of the type of trade organization?

SP2: That will take a look, there will be about three four. #general_information_amount_trade_organizations

SP1: Three four, yes exactly. Okay and are those really the smaller customers or are we talking about the bigger ones.

SP2: No yes so the one we want to apply it to is Toms, which is a shoe store and does about sixty million in shoes on an annual basis. Say about ten million pieces.

SP1: Yes. Ten million sixty euros indeed.

SP2: Yes.

SP1: Nice okay. What is your approach route when starting such a check?

SP2: For example with Toms to give a good example.

SP1: Yes. What is the first step you take? Are you going to initially look at how the processes of such an organization are structured?

SP2: Yes, as an accountant you actually always start with a fixed pattern. One you look at what are the risks that I see in the financial statements. The second is that you then look at what the company does about those risks. So what measures and processes has the company set up. And then when you have looked at that picture, certain residual risks arise and you want to work on this as an accountant. #audit_approach_financial_statement_risks

SP2: One of the examples is, for example, as a risk, you see that unjustified discounts can be granted. Well then you first look at what does that company itself do to control discounts. If there are things in systems that should not give discounts from a certain bandwidth, they contain authorization strokes. If you have mapped that out, you can do desk work there or work as an accountant yourself. #audit_approach_financial_statement_risks

SP1: Yes exactly okay. Then you go there I think you define controls of the different processes?

SP2: Yes. #audit_approach_define_process #audit_approach_define_controls

SP1: For purchasing and sales processes too. And on what basis do you define those controls, for such a purchasing process, for example? That's based on those risks?

SP2: Yes yes and actually per typology as it is called, per type of company in this case trading company you often have a standard set of things that you pay attention to. Other than a set of risks you look at. And then you go to the organization to see how it is organized and how they manage those risks themselves. #general_note_1

SP1: Yes, exactly. And what are, for example, those standard risks or those standard controls for purchasing and sales?

SP2: At a trade organization, one of the risks is that the purchase price is not correct. So that's the P component of purchasing. The second risk is that your quantity of purchase is incorrect. So that's the component as we call procurement. #control_product_pricing #control_product_delivery_quantity #control_three_way_match

SP1: And how can the quantity not be right?

SP2: Well, for example, that you have ordered a hundred and that you only receive eighty, for example, but that you have to pay a hundred. #control_product_delivery_quantity

SP1: Yes, exactly. Also a piece of stock. Those are two controls, well then you just mentioned the three-way match.

SP2: Yes. That is often for the Q component indeed and partly also for the P.

SP1: Oh yeah okay. That is actually a control with which you can combine the different, well, what?

SP2: Yes.

SP1: Yes. Also, if you look within the procurement process, do you also look at things like payment how this is done?

SP2: Yes. It is often the payment process you watch yes. #control_payment_segregation_of_duty

SP1: Payment process.

SP2: Yes. Is indeed to whom is paid, how is paid, the correct bank account number is paid.

SP1: Yeah okay. To stick with purchasing for a while. The moment you have set up these controls, these are the things you will look at with a customer.

SP2: Yes.

SP1: Are you going to collect specific data internally or are you doing this externally?

SP2: It depends a bit on how the customer is arranged. If it itself has a very good control environment, you can rely on that, if not, you will indeed get data and try to analyze it yourself.

SP1: Okay and how was that for this customer, for example?

SP2: For this customer, we ultimately chose because we also partly have a tool within SAP tool within Baker Tilly, so we chose to use that SAP tool to see whether we can perform our analyzes properly. #system_sap #system_erp

SP1: Yes. And will all the different controls be covered by this analysis?

SP2: Yes that matches yes.

SP1: You can match that.

SP2: Yes.

SP1: Yes, exactly. And you have the other things manually.

SP2: Yes sometimes sometimes not, but I think I can draw on the board for a while.

SP1: Oh yeah.

SP2: It is very simple to purchase from a trading company. On the purchasing side you have a Q component, that is the quantity. And a price. You have the same on the sales side. There you also have a Q component, the quantity sold and a price. Often there is also that on the Q side you have

of course your Q-start plus your Q-purchase minus your Q-sale is your Q-end. That's how the Q runs. Well what you often do as an accountant is to establish this again, to establish the existence of this. You do this through inventory. Is just counting. Well here too, but you often did that in the previous year. So this is check number one. Control number two is that you want to understand this connection. This is called the money flow movement. That's control number two. That is what I had at the start plus your purchase and sale is then your end. #control_turnover #data_turnover

SP1: Yes. And what are the discrepancies in it?

SP2: What are the discrepancies? Yes, they are very large or are they small. So you want to know. And you indeed want to know your P on your purchase. That's risk number three we're looking at. And you often use the three-way match for that. As a three-way match match nicely covers the P and the Q, if it is good. In the three-way match, one of these I say buys at this price, one says this has been delivered and there is this price on the invoice. So if all goes well, that's the three-way match. You do the same with the price and the Q on the sales side. So there you have to see the three-way match. And someone says dude I want this and someone says we delivered this from the warehouse and someone puts that on the invoice. It also shows the three-way match. And then you also want to see the connection between this and this. This is then called margin analysis. #control_three_way_match #fd_structure_warehouse

And it then states how many discounts have been granted, at what prices have been sold and bought, what margins there are and that is in accordance with what we expect. #control_product_pricing

SP1: Exactly.

SP2: And very crudely, this is an audit of procurement.

SP1: Yeah okay. And if you look at the three-way match. What is important in this? That the division of roles. #control_three_way_match

SP2: Yes, so that there are three different parties that say okay, these are one party that is responsible for the purchases. So it determines the P at the time of purchase. And the Q at the moment of purchase and an independent person then says what is the delivery of the P, of the Q especially sorry. Also on the P of course because it is expected what has been delivered, the right quality. And on the other hand someone other than who checks the administration of hey when we receive that invoice, connect it with what I ordered and what I received. #control_three_way_match

SP1: Yes we are going to pay it. Yeah okay. And these are mainly peripheral matters, of course, because if that is not properly arranged then.

SP2: Then it becomes very difficult to determine.

SP1: That makes it very tricky to determine.

SP2: Yes.

SP1: Okay clear. Very clear picture too, I have not seen it yet. At least the explanation, but that picture is very nice. I'm going to take a picture of it.

SP2: Very well.

SP1: Okay. The moment you then collect that data to test these different things, you can of course get it very nicely from such a SAP system. #system_erp #system_sap

SP2: Yes.

SP1: The purchase orders, the invoices and the delivery notes, for example. #data_three_way_match

SP2: Yes.

SP1: Can you really rely on the data from that SAP system or do you still have to get data from external sources to do some kind of extra verification?

SP2: In this case, take a look, yes, of course we always look at your IT general controls. And then very specific in this case to your authentication, so let's say to your users, if that's correct. That it is sufficiently monitored, that there is sufficient password protection and logging out of accounts. So the authentication is then determined in the system and then determined by means of data analysis that everything always involves three parties. #general_note_2

SP1: Yes exactly and then you do not have to have data from, for example, such a supplier of what have you supplied to us. #general_note_2

SP2: No no. #general_note_2

SP1: You are not looking for that?

SP2: No. In this case, we specifically looked at whether it is said that the authentication is correct in the system and in this way we can determine that there are always three parties involved. #general_note_3

SP1: Yes clearly. Then you also get a very good overview and you can actually say of every transaction whether this is correct or not.

SP2: Yes.

SP1: And did you check all outliers on that basis or were there any outliers at all?

SP2: I think in this case, just looking back at the data, it was a while ago. In this case there were no offshoots, but otherwise you have to contact Michiel Boers who also has this data analysis all by himself. Executed and designed.

SP1: Very well. Yes clearly. This is actually the process that you maintain and this is, well this is very broad actually for all those different organizations you use this.

SP2: Yes.

SP1: Yes. You already indicate that you can get all data from SAP and this yes for this is more interesting because whole.

SP2: Yes Michiel indeed did the export there and I think we did have some trouble getting all the data from the sales side. Then you should ask Michiel if that worked out in the end, but the amount of data is so large that I think we had some problems on that side. But I think it is best to make an appointment with Michiel because he said of how we draw from SAP by means of our own data extracts, we extract all that data from SAP and then we will see how we can do it together. match, combine, validate. #data_three_way_match

SP1: Okay. Well then data and system, yes we went through it quickly as I almost ran out of my questions. Yes, do you see any added value in carrying out a data analysis that we have now done until the end of the year on a continuous basis? Because in principle that could now? If you only have the data constantly, you can run the analysis constantly.

SP2: Yes. Yes, the question is always how many transactions actually go through the system and do you monitor it on a daily basis, on a monthly or semi-annual basis. But in the end I do think that that will be the goal. #general_note_4

SP1: Yes okay okay. And does your customer see that too, the added value of, for example, continuous monitoring?

SP2: Yes, if you think I do that in combination with benchmarking, grade assessment and grade analysis, so actually management information. Can I also draw on the board, but first take a picture of this?

SP1: Yes, I, M gonna do that. I have already thought about it well.

SP2: Yes. Did you take a good photo?

SP1: Yes, I have a good photo, thank you.

SP2: Just draw. Just signed, I think that this is where the continuous monitoring or actually your future audits go. Explained very briefly. You actually work with a data layer. I don't know if you already know a lot about it, but data layer is a standardized layer where data is stored in a standard way.

SP1: Exactly. Key data warehouse actually.

SP2: Key data warehouse, which you just manage, as it were, at Baker Tilly. The data layer where you store a standard field of data in a standardized manner according to a standard data format. You will eventually work with extraction teams. So teams will only specifically collect data. That you have teams, as it were, that have the most knowledge to retrieve that data and that you can also be trained the most per application what is going to happen. Before we work with a data layer, you can load with various things. You can load salary data, you can load effective directory, you can read PMT2 data. You can read financial data, you can read statements. You can read in what you want. In your data layer you then have to use standardized controls, per typology. I would like to minimize the fact that you say this. Things like what I have already said, for example, changes, salaries you see in your effective directory and you see changes in payroll. That would actually be one to one. #general_note_5

SP1: Agreement must come.

SP2: Yes or there are some freelancers among them, but you could find them in the ZZP-register, so that you can compare more data, as it were, and combine different sources. And you must then have standardized checks on this with analysis teams that will investigate exceptions. And actually three things should come out. One audit evidence from us as an accountant is correct. You have audit evidence. But two other things and I think that there is the value for the customer, for example, because the customer finds control important on the one hand, but thinks much more important about what figures come out. What trend do you see as an accountant, what details do you see as an accountant. And actually as a third element also benchmarking. If you download that for example for all car companies, what trend do you see in salaries or FTE. What trends do you see in reward, what trends do you see in sales. What trend do you see in the market. #general_note_5

SP1: Exactly. And the last two, can you already participate there for the customer? Yes, you already do something about those trends.

SP2: Not right now I will say because we don't have this listed. We don't have a large data warehouse. And it is one, it is possible but it is a very manual process. While you actually have to say yes in the long run, just leave it here in your data layer, let's say twenty, let's say, you have thirty control customers for automotive and 50 assembly customers, yes you load that in the data layer. #general_note_5

SP1: Yes because that is indeed what I am looking for in the research. What will that data layer look like, what kind of data do you want to have in it and what will that layer of controls look like? What kind of controls are they. And I try to do that for the trade organization in the first instance, on top of the general controls of course, which you would prefer to continuously test automatically. Because as soon as something changes there, your case changes. #general_note_5

SP2: Yes.

SP1: If an application is updated yes well then you should take a look at it. So I really like to see that you are also responsible for this, because this is indeed where you would like to go in the long run. #general_note_5

SP2: Yes.

SP1: Also looking from the theory.

SP2: It will still take, it will take another five years before we build it.

SP1: Yes. PWC already has something.

SP2: Yes?

SP1: I think PWC has a continuous monitoring dashboard that analyzes on location. They put a kind of black box on location, a piece of software that actually analyzes the data continuously and the outlayers are sent to the PWC dashboard at PWC to the data layer. Well that's quite an interesting one.

SP2: Yes.

SP1: And actually if you have your general control in order, it is best to implement it easily, because the data is good, the invoices, purchasing and things like that are all standard fields.

SP2: Yes. Yes, but I do think with our type of customers, because of course we have slightly smaller customers, you often see the IT general controls are not in order or are not completely in order, where there is often a super user or too many super users. Or is the superuser exactly in the wrong place in the organization. So then often ID general control is not the support. So I actually want a lot more that you load all data from the customers into your data layer. Also because it is often still limited by our customers. Look at Tops I ran into a maximum. That I think we have to ninety-nine percent of the customers we do here easily put the number of transactions into a good data layer, as long as you have a good equipment app behind it. And that you will indeed look through cross connections of what I see, what details are there and that you indeed have a standard set of controls and that will slowly expand.

SP1: Exactly. And indeed just keep expanding and in the long run you can say I apply every control to every dataset.

SP2: Yes.

SP1: And then we'll see what we find.

SP2: Once yes.

SP1: Yes interesting, okay.

SP2: I think that is the picture of the future and again that you will also look at that piece of figure assessment and benchmarking on a case-by-case basis. I think we have yes audit information is important to us also ultimately for the audit and signing off and that customer is also much more

interested yes. How do I do compared to the rest. Where is the improvement potential, how do my margins compare to other customers. What do my personnel costs and housing costs and my marketing costs do and how do they relate to my.

SP1: Because can you say something about that? Can you say something to one customer about your entire set of customers? You don't think they like that.

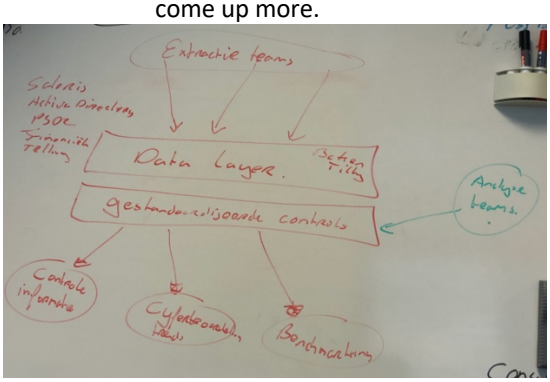
SP2: No, you have to think about it in the end, how do you guarantee privacy, how do you guarantee confidentiality, how will I present this in datasets themselves. I mean I do not think you can say this at customer x of this I see at customer y. You can anonymize that you say hey within a branch I have at least twenty customers. Twenty customers because data is still fairly anonymized.

And then I see that the average labor costs at a car company or a construction company are the labor costs are fifty K. Or maybe between forty-five and fifty K, well this customer is at fifty-four, you are reasonably high in that line. In that line yes. Could there be another explanation that it says dude I work with more experienced people because I see benefits in that. That could be. But if he can't explain that, you can have a conversation with him, hey, how come you are so high.

SP1: Can we help you?

SP2: Yes.

SP1: Yes, exactly. Interesting. Well okay I actually heard that piece of benchmarking and data analysis come up more.



Interview 4 with ITA1

General interviewee information (#general_information)

Bachelor / Master study	Bachelor and Master Accountancy. IT auditing post-master.
Current role	Manager IT Advisory, mainly in IT audit
Continuous Financial Monitoring experience	No practical experience

General notes (#general_note)

1. A much-used example for continuous access protection monitoring is putting code at the customer location which periodically checks for changes in accounts and policies and reports those.
2. Most of the data for the general access protection control can be deducted from logging, if properly setup.
3. Segregation of duties is important, especially for change management, to ensure no single person has made system changes without approval.
4. Companies often have a mix of various systems where the data comes from. These are a mix of ERP systems and financial systems.

(Financial) Department structure (#fd_structure)

- HR
- IT
- Finance

Processes, Controls, Data and Systems (#process, #control, #data, #system)

Control	Type / Process	Description	Data	System
General access protection (it_general_access_protection)	IT General		- Users in the systems - Their last login - Their roles and rights - Account details (username) - Last password change	Active Directory
Identification (it_general_access_protection_identification)	IT General	Which person does a user in the system represent. When you login with a username, does that represent a person.	- Users in the system(s) - Usernames convention / mapping	Active Directory

Authentication (it_general_access_protection_authentication)	IT General	How do you prove that you have that identity. Are password requirements proper.		Active Directory
Authorization (it_general_access_protection_authorization)	IT General	What can you do in the system. Roles and rights within the system.	- Roles and rights per user in the system(s) - Which user should have which roles/rights	Active Directory
New Employee (hr_new_employee)	HR / IT General	When a new employee joins the company, an account has to be set up. How is ensured that he get the right access (authorization).	- HR mutations	
Employee new role (hr_employee_new_role)	HR / IT General	When an existing employee gets a new function, his roles and rights should change as well. How is ensured that his access is proper (authorization).		
Employee leaves (hr_employee_leaves)	HR / IT General	When an employee leaves the company, his access should be revoked (authorization)		
Change Management (it_change_management)	IT General	What changes in system configuration have been made and what software upgrades have been performed. What was the impact of	- Overview of all system changes and updates - Changelogs per update - Approvals per change	- Ticketing system for storing tickets. - System logs - System configura

		those changes and how have they been tested to ensure the correct functioning of the system(s) and business processes. This can be for custom-made software and off-the-shelve software.		tion for version
Business Continuity (it_business_continuity)	IT General	For businesses where IT is crucial in day-to-day operations, the continuity of these systems should be guaranteed by having proper backup and recovery measurements in place.	- Backups schedule - Backups test - Overview of IT landscape	

List of unique used keys

#background_information_cfm_experience
#control_hr_employee_leaves
#control_hr_employee_new_role
#control_hr_new_employee
#control_it_business_continuity
#control_it_change_management
#control_it_general_access_protection
#control_it_general_access_protection_authentication
#control_it_general_access_protection_authorization
#control_it_general_access_protection_identification
#data_it_business_continuity
#data_it_general_access_protection
#data_it_general_access_protection_authorization
#data_it_general_access_protection_identification
#fd_structure_hr
#fd_structure_it
#general_information_current_role
#general_information_education

#general_note_1
#general_note_2
#general_note_3
#general_note_4
#system_active_directory
#system_it_change_management
#system_it_general_access_protection
#system_ticketing

Transcript

SP1: To start briefly, could you briefly tell us what your background is and what training you have?

SP2: As for training? I have had an accountancy training. I have a higher professional education and a master's and a post-master's degree for accountants. So I theoretically graduated for that. Practical internship never achieved. And I followed the IT training afterwards. At the UvA. That is the basic training. #general_information_education

SP1: Yes. And what is your current role within Baker Tilly.

SP2: I am responsible for the offices Zwolle and Almelo. And then I am mainly involved in the financial statements audits. And also a little bit for consultancy assignments. But that's a lot Tino takes up in our office. #general_information_current_role

SP1: Yes, exactly. And what type of consultancy assignments have you… do you like the most so to speak?

SP2: For example, what I do most are baseline measurements. Do you actually look at a certain moment how an organization is set up and where could it tighten? Or, for example, can efficiency gain? I have sometimes done an assignment in the context of privacy. But core activities 90% - 95% are audit of financial statements.

SP1: Yes, exactly. Do you have any experience with continuous financial monitoring or automated controls or something along those lines? Have you ever done anything with that?

SP2: Well, of course I'm on the accountants side. So do something with it yourself, that's what the companies I visit do. I don't think we do much with Baker Tilly. So practical experience that I see monitoring myself, that might be a… we receive a weekly email if someone has not opened the schedule. That's an automatic email you get, so that's a bit of continuing monitoring. But not much more than that. #background_information_cfm_experience

SP1: The questions I mainly want to ask are about IT general controls. The first question is what are the IT general controls that are tested in practice? Or who you come across? Of course I have a theoretical framework in this? But what do you encounter yourself?

SP2: I would say, take our guide, it contains all the general IT controversies that we test. And we also encounter them in practice.

SP1: You mainly encounter them. And if you then ...

SP2: Now make a distinction between what we do a lot in practice is to determine things yourself. These are in fact not controls at a company. So when I go to a company and I see that said have set up password requirements. But that they do not check themselves and that they have good password requirements, I do not think that these are general IT controls. I don't know how you defined the general IT controls?

SP1: Actually assessment steps that are used to test the preconditions of an organization.

SP2: Yes, but I would expect controls that is a way in which the organization actually tests itself.

SP1: Yes. And this would be a way in which we can test that organization to say that it meets those preconditions. So how do we actually do that to actually say in the long run that this is… they meet or they do not.

SP2: Yes, but I just want to make the distinction. Because if I support continued monitoring and general IT controls… those are more control measures that a company has set up to monitor itself. If I am going to request an annual audit: how are your passwords arranged? Then I carry out a check at that time. But then I am not determining how the organization controls itself. Then I'm checking something myself.

SP1: Exactly. And actually it is mainly about the first one, that is, those control measures.

SP2: What are you looking for now?

SP1: Exactly and those are actually the things that I would like to test on a continuous basis in my solution later. Because if we can test it on a continuous basis and that is good, then that says something. So that's what I'm looking for.

SP2: When I count it down, we have some facets that we are looking at. One of these is logical access protection. This is again divided into 3 sub-areas. Identification, authentication and authorization. Identification is aimed at who are you? Authentication, how do you prove that you are? With a password? And then your username would be the identifier. And authorization is what can you do? #control_it_general_access_protection #control_it_general_access_protection_identification #control_it_general_access_protection_authentication #control_it_general_access_protection_authorization

SP1: Exactly, your roles and rights.

SP2: Yes. If I take a look at this, what do we encounter in measures of how the company controls itself? Then we come across fewer measures in identification and authentication. That is usually something that has been set up, but that they do not control the customers well. Might be very good. You could enable a log in or enable a notification if your password requirements change. But we often don't see that in practice. So if it is what am I really running into? Then nothing is set up for that. What they often have is a process for making changes to usage rights. So someone is hired, then a process is initiated. HR usually starts, which says someone will be hired. It must have access to certain applications and certain rights. It needs certain hardware. A computer and telephone and things like that. Then a process is initiated. There is usually some control over the company itself. So that they check themselves with when someone enters the service, they also get the right consumables. The right permissions in applications, access to the correct folders on the Windows Active Directory. Can't he just reach the MT folder for example. Usually there is a check on what rights someone gets. And is that therefore right that he gets that? Same with if someone gets a new job or something. Then he'll probably get some more rights. And maybe issue some rights. There is a check on that. And the same if someone leaves employment, those rights must be revoked for everyone. So on the authorization part. #control_hr_new_employee #control_hr_employee_new_role #control_hr_employee_leaves #control_it_general_access_protection_authorization #data_it_general_access_protection_authorization #fd_structure_hr #fd_structure_it

SP1: Yes. And identification and authentication, how would you then ... so they test less themselves, but could you test that in an automated way? Then you are actually talking about logging and that kind of ...

SP2: Yes, you could enable notifications for example. What Martin always has an example about is what one of the big four companies is doing now. They put a robot at a company. And what it keeps track is, which checks every now and then whether the password requirements, your domain policy on the network, on your Windows active directory, or which is unchanged. That way you can monitor, is there a change? And yes, there is a change, that somewhere a light comes on with this you have to check. Because this is a change in our policy that we did not expect. For example, you can enable passwords. #control_it_general_access_protection_authentication #general_note_1 Identification is a bit tricky. Because that is about issuing usernames. Then you should check with this is a valid username. For example, you may have a naming convention. For example, your username is always initial plus last name you often see. That you have a kind of check that deviates from someone, then an alarm bell should also ring. Or I monitor that too. That is possible. I don't see it in practice. #control_it_general_access_protection_identification

SP1: No, clearly. And the data to, for example, test your identification… which is of course available again. Because that is….

SP2: The data is there.

SP1: Only the test itself is not performed?

SP2: Right.

SP1: And that applies to all three parts?

SP2: Hell yes.

SP1: I think it is still useful to continue with this. What kind of data entities are you talking about? What data do you need to be able to perform that test? I think it starts very easily with an AD user list? #data_it_general_access_protection #system_active_directory #system_it_general_access_protection

SP2: Yes. #data_it_general_access_protection_authorization #system_active_directory #system_it_general_access_protection

SP1: And what else are you looking at? And I'm actually talking about data that you can derive from the system?

SP2: In any case, I think what you should always start with is that you have some kind of standard. So you will have to know somewhere if they know the password policy, we take as a basis, of these are the minimum password requirements. That you can do a test on that. You can easily extract the data from the Windows Active directory from the system. It is simply available. So that are usernames, account details, last login time, last password change, you must meet the password periodicity. How is the domain policy organized? All that data is available from a customer. #data_it_general_access_protection_authorization #system_active_directory #system_it_general_access_protection

SP1: Yes. And with that you can actually use the identification… no, sorry… with that you can mainly use your authorization?

SP2: That was before authentication, which you could test with that. Identification is the same, you need some kind of convention, a standard, with this my username has to meet. And then it is only an export from your AD or application with usage data that can be retrieved from the directory anyway and in fact you should be able to get the data from every application there. So that test is very easy to do.

SP1: Are you actually putting the AD data next to your payroll or workforce?

SP2: Yes, that would be possible. But it just depends on what do you consider to be a standard as a customer? Where can I find as a customer that my passwords must meet? Where do I find as a customer, how should a user get their name, how should they be identified? If you have users called 1234, you don't know who is behind it. If you guarantee that it is always initial plus last name, you will experience some problems in practice. Because there will be several P. Janssen at a large company. But if you have good rules for that, you can always identify people. Then you always know based on the username, that person has done this mutation ... because his print is there. #data_it_general_access_protection_identification

SP1: Yes, exactly. What if you look at authorization?

SP2: Basically, the most important of these is… which is what most of our customers don't have, a clear standard that states… if someone has this position, then those rights are part of that. And especially not these rights. Because if you had that included, it could break through our intended segregation of duties in the system. And we want to prevent that. So you will first have to determine what kind of rights can a person have in a particular position? And then it is a… often a person has a role and a role has rights. So then you will have to determine that the role always has the associated rights. And that only the persons who should have a role also have that role. You could check that continuously, of course. You can hold any change against that standard and check whether it is sufficient? #data_it_general_access_protection_authorization

SP1: Yes, I understand now… you could get those changes from the log.

SP2: Yes, for example. But you could also put a notification on it. If someone makes a change, at that moment there will already be a notification that picks up person X has made this change, which has given Pietje role Y. That you receive an e-mail or receive a notification in some other way. Does not even have to be written in a log, but then you already have a notification. #general_note_2

SP1: Exactly. I get that. Then I think I have the ... Okay. Then the next control or at least the next group is change management, which is common. When we talk about that, what does it consist of in practice? #control_it_change_management

SP2: That differs per organization where we come. Generally we make a split between one, some companies have a standard application. So they take something and they never develop anything themselves. Nothing is ever developed specifically for them. And you have organizations that build an application themselves or at least develop it themselves. These are two different approaches that we use for this. If you are an organization that has a standard application, then you will receive an update from your supplier with ... you are put on fact, dear customer, this is the update and success with it. Then as a customer you will have to determine… I will get this update, but what impact does it have on me? Most customers have a test environment where they are the first to update. And then they will test all existing functionalities. Are they still doing what they have to do? You can do that in a risk-oriented way. So you can say, I think this is a key process. So I'm going to test this. And this other process is less important to me, so I do less about it. As a customer, you first perform test activities on your existing functionalities and on the new ones that you receive from your supplier. Is there anything I can do with that? What do they do for me? How are you going to affect my processes? And then if you say this is good, then you give a 'go' with this allowed into the live environment. With your own developed application, you make something yourself. So what you often see in practice is that you actually have two types of tests on everything that develops. So you will have a development environment and something will be created there. Then something is put to an acceptance environment or a test environment and more technical tests are carried out there. So often a source code review or something. Someone who can also develop well and watch what source code or something have you written? And does it actually do what it has to do? And then when we know the basics are doing what they have to do, it ends up in an acceptance environment. And therein would actually be the test that I just outlined for a standard application, in which that test is performed. So a user or an application manager or someone who knows a lot about how we use this application? He will then test… nice that the update technically

does what it should do, but how does it affect our process now? And how we work with this application. He will then carry out test work there. #control_it_change_management

SP1: I get it. And the moment you come to a customer and you see if they have it under control, what do you check?

SP2: Well, what I often start with ... questions do you have an overview for me that you are sure that all changes are on it. Do you register any changes that have been made? And then I have to say, I think that is more important with a self-developed application or where self-development is involved, than with a standard application. Then you can usually use the… or something from the supplier, which has a fixed version numbering that you can see from the previous control version 2 and now version 4. So there will have been an update. Then I can still keep track of the changes there have been. If you are going to develop yourself, you cannot necessarily always follow it that easily. And do something to register what changes have there been? Then it depends on how I want to test. I assume that the organization therefore has control. And that they can test controls. And not that we determine anything ourselves. Then I would test it, they have a process where they say every change is done ... first technical test and then use test done ... then show that it happened. Then I can, for example, in a ticket system or something they have seen that someone from the technical department first has the test or has prepared the update. Can I see that a second person from the technical department has approved that change. I then see that he has been transferred to the acceptance environment. And I see that a person from a key user has also approved from the users. Then I would test it, they have a process where they say every change is done ... first technical test and then use test done ... then show that it happened. Then I can, for example, in a ticket system or something they have seen that someone from the technical department first has the test or has prepared the update. Can I see that a second person from the technical department has approved that change. I then see that he has been transferred to the acceptance environment. And I see that a person from a key user has also approved from the users. Then I would test it, they have a process where they say every change is done ... first technical test and then use test done ... then show that it happened. Then I can, for example, in a ticket system or something they have seen that someone from the technical department first has the test or has prepared the update. Can I see that a second person from the technical department has approved that change. I then see that he has been transferred to the acceptance environment. And I see that a person from a key user has also approved from the users. Then I can, for example, in a ticket system or something they have seen that someone from the technical department first has the test or has prepared the update. Can I see that a second person from the technical department has approved that change. I then see that he has been transferred to the acceptance environment. And I see that a person from a key user has also approved from the users. Then I can, for example, in a ticket system or something they have seen that someone from the technical department first has the test or has prepared the update. Can I see that a second person from the technical department has approved that change. I then see that he has been transferred to the acceptance environment. And I see that a person from a key user has also approved from the users. #control_it_change_management #system_it_change_management #system_ticketing

SP1: So really those different people are really very important then?

SP2: Yes. Right. As a user who has absolutely no experience with how do I rate a source code. If he has looked at how that source code is written, that does not mean anything to me, it must be someone I expect to be able to look closely at it. So which person did something does matter. And I also have an interest in if several people are involved, for example, there will be less fraud. Suppose I… someone develops something in a payment process and develops a new feature that includes it and transfers 1 cent from every transaction that is made to my bank account number… if you do one alone, then no one sees it and never has to notice it. If a second person looks at it and sees a piece of source code from write part of it to this bank account, he will pull the alarm bells. So that's why I think it's important that multiple people watch it. That not one can cheat. #general_note_3

SP1: So in summary, you want to know if they use standard application or develop it yourself. Do you want to know that there is an overview of all changes?

SP2: Yes.

SP1: When there is an overview of all changes, you want to know per change what have they been? And with an internal application you really have to be able to get it somewhere. And with an external application can you find it in the release notes?

SP2: Yes.

SP1: In addition, it is important how the various changes have been tested in the core. Have they been tested in different environments? Approved by different people?

SP2: Yes.

SP1: Do you see that occurring in practice? Do you really see that it happens because of a lot… that something really goes into production such a test acceptance?

SP2: Sure. Many of our customers have standard applications. Then you have that less. Then you just put something in a test environment and tested it there once and then put it into the production environment. Actually all customers that I have with their own developed applications… the risk is much greater that something will go wrong. If an Exact Globe or something releases a new release and there is an error in it, so that something really goes wrong with a customer of mine, that new release will be rolled out to thousands of customers of exactly the same. They ensure that there is no error in their update. At least, there is no major mistake. And that reduces the risk of something going wrong. May still be that something is going wrong. Because every customer has his own specific way in which he uses an application and his own way of internal control. Something can still go wrong. But it will usually have less impact. #control_it_change_management

SP1: Yes, I understand. If you then look at the necessary data entities to automatically test this piece ... and now we only look at the standard application. Then you mainly want to keep track of whether there have been changes in the system?

SP2: Yes. There is sometimes, sometimes or sometimes no log of available in the system where you can see which updates there are. What we encounter quite often is that they have a ticket system. This is then kept up to date and there is a change and immediately, if it is properly set up, it is kept up to date with who then carried out the test work. And some… then you have more companies that really develop themselves, they also have applications in which the OTAP street therefore develops, tests, acceptance, production. Which is also enforced there. So that you have certain measures of you have written a piece of source code here. That piece of source code is then always put to the test environment first. Then someone first has to approve and only then to the acceptance. Then you can really bring the source code to the production environment in a controlled manner. #system_ticketing #system_it_change_management #control_it_change_management

SP1: I get it. So that's why you see, that's actually a system where you can see what changes there are and if they've been approved?

SP2: Yes.

SP1: Here I have the information I need for this piece. If I am correct, is the third chapter continuity in the checks?

SP2: Yes correct.

SP1: How do you test that? Is that recorded?

SP2: Less is done with us. Being a team anyway. We will discuss the access, security and change management components more than continuity. Actually with background… I can now see from the annual audit how we look at those general IT audits…. The change management and access protection firstly ensure that the change management, if you do it right, the system does what it should do, in short. It cannot be that during the year 1 plus 1 was three at once, for example. The system doesn't have ... no functions actually. And access protection ensures that you can also keep segregation of duties. So that you also, everything you do in a system, that it is controlled. The only thing that can do continuity is make sure that if my system breaks down, I can restart. It is usually the case that when we come to perform an annual audit, we will see whether that system is still there. So the risk that there is absolutely nothing left and the customer is uncontrollable because a system cannot be recovered or something, we do not consider that to be a very high risk for most customers. Most customers still have papers or backups at different levels in so many places that they could still reconstruct things, that we could still carry out our audit. That is stated in the guide, a number of conditions ... suppose you are bol.com and you have to continue to deliver very quickly and you must be continuously available, otherwise you will fall over ... then you should have financing at the bank that you do not have to can stand still. So you go bankrupt if you lie flat for a while. Reasonably short period, then we will only do more on continuity. Otherwise we will do more of the basics… to ask what is your continuity measure like now? Then we will test less deep ourselves. I don't know how relevant that is to you. #control_it_business_continuity

SP1: Interesting knowledge anyway. But indeed what you already say, if it is important for the continuation of business operations, then it must be in order. Otherwise, yes ... not flatly stated.

SP2: Right.

SP1: Check. Clearly. Then I will not continue to question this further.

SP2: I can mention a few things we could do. Because actually, we have some parts that we look at. The most important thing the company needs to do is backup. And that is something that they monitor quite a lot on a continuous basis. For example, it runs a daily backup, incremental backup. A full backup every week. And a snapshot every hour. So they have a number of different times when a task is running to make sure they still have the data. And usually there is a monitoring that checks: has this job been completed? Have any errors been identified? Has it been completed successfully? Actually, there are often such measures. Plus what companies do less, but should do, is that they also periodically perform a recovery test. So they actually say we made backups and tested that they went well. But have I ever put a backup back into the live environment and does it really work? So with a recovery test you will determine ... my assumption that my backup went well all the time, I will test it again by doing it myself. #data_it_business_continuity

SP1: Okay. And what you actually want to see is that they actually monitor backups and that it is recorded that they have performed a recovery test, for example?

SP2: Yes. When I see what often goes wrong is if the backups are not running. Then you have a problem. Or your monitoring is not on or is it on. You often see that in practice a landscape changes somewhat. They are buying a new server forgetting to backup. Then the monitoring is running, but you no longer know what your landscape is. So it also helps to scan what is there now ... which databases are active? You could also monitor something there. And then indeed it is backed up. Is there content in that backup? Has that backup been successful? Has it just been completed or has it been cut off because something went wrong? You could monitor all those things. And many companies do it too. #data_it_business_continuity

SP1: Especially internally for own…

SP2: Yes.

SP1: Okay, then did we have IT general control?

SP2: Yes, the most important things are. We have a part of problem management, incident management, management and organization ... but those are more supporting processes, I think. If you want to take the most important parts with you, we've had them.

SP1: Okay. I also had a question about application controls. But that is more an in-depth question… I don't know if you can answer that directly. The accountants have listed a number of controls that are used to test the purchasing and sales process. In addition, they also have data entities that are required. I don't know ... can you name the following data entities as an example of specific systems where they come from? Then I am talking about, for example, purchase orders and receipts. Where are they often registered? Do you know that?

SP2: Most I encounter is that a company has an ERP system. If that kind of data is available, they usually have an ERP system and that includes a purchasing component. There you record your purchase orders. This includes a logistics component. And there you record your goods receipts. And there is a financial part and you record your purchase invoices there.

SP1: Exactly. And that is mainly for those things and then creditor master data? Are they in the same system?

SP2: They always come in the financial application. Because you use that, creditor master data, generally to make ome and payment badge. And they usually run from your financial application. This can also be part of such a package, but can also be a separate application. #general_note_4

SP1: And does the same actually apply to payment lists?

SP2: Yes.

SP1: And product prices? Also an ERP system?

SP2: Yes, you can also have one… you also have special logistics systems for example. They could also be suffering in that. That ERP system is a combination of systems. What I just mentioned, it could also have been an order system or purchasing system, a logistics system and a financial system. In practice, you often see that this is an ERP system. That they don't let three separate systems talk to each other, because they have to work together a lot. But that they place it in an application. #general_note_4

SP1: And financial applications, do you see them more often separately or more often integrated?

SP2: Yes… it is often a mix. It is often a financial application with… there is often something in it, which you can do something more with. You can also sometimes manage projects with it. Or you can manage your articles with it. I couldn't say what most ... whether it is really bare financial or whether it occurs most or another that has something more to it. #general_note_4

Interview 5 with ITA2

General interviewee information (#general_information)

Bachelor / Master study	Practical education in Network and System Engineering. Bachelor in Business IT. Master in IT audit.
Current role	Senior IT audit and Data Analytics consultant at Baker Tilly
Continuous Financial Monitoring experience	None.

General notes (#general_note)

1. The customer should have its procedures in place in order for controls to be useful.
2. The audit process focusses on finding out how a customer does things (what is its own standard). Next, the standard is being assessed, does it match prescriptions. Lastly, the standard is tested, is it really implemented and used as described.
3. Systems of which the IT general controls have to be tested (such as change management) have to be in the scope of the financial administration.
4. Each system has a user list, all of these should be tested. Users can be centrally stored in an Active Directory but to test if they had access to the specific systems, those should be checked as well.
5. Some systems may delete data after it is not being used anymore. Data such as purchase orders.
6. Matching users can be tricky because names are not always consistently entered across all systems. Therefore, manual matching might be necessary.

(Financial) Department structure (#fd_structure)

- HR
- IT
- Finance

Processes, Controls, Data and Systems (#process, #control, #data, #system)

Control	Type / Process	Description	Data	System
General Access Protection (it_general_access_protection)	IT General			
Identification (it_general_access_protection_identification)	IT General	Are the users in the system traceable to a real person. Matching all active users in the system with a physical person.	- List of active users from the system - List of employees from HR	- Active Directory
Authentication (it_general_access_protection_authentication)	IT General	Is the password policy up to requirements and do all accounts comply to this. Test this by	- List with password requirements	- Active Directory

		inputting passwords that do not match the policy and see if this is allowed. Is two-factor authentication enabled.		
Authorization (it_general_access_protection_authorization)	IT General	Who can do what in the system and are they allowed to do that.		
New Employee (hr_new_employee)	HR / IT General	What roles and rights does a new employee have and who has authorized that this person can have these roles and rights.	- List of HR mutations	- HR Application - Active Directory
Change Management (it_change_management)	IT General	How are changes and software updates being implemented and is this in a correct and reliable manner. What things were changes during an update and what was the impact on the systems. If the used systems are from suppliers that are being audited themselves, it is very reliable. Are changes tracked in a ticketing system and being approved by multiple people.	- List of all software systems - Changes per system (based on version number) - Changelogs for the updates - Change tickets from ticketing system.	- Ticketing system - ERP system
Business Continuity (it_business_continuity)	IT General	How are backup and recovery managed for systems where		

		the business depends on (systems that are business critical e.g. webshop). This control is not used often and mostly performed manually.		

List of unique used keys

#control_hr_new_employee
#control_it_business_continuity
#control_it_change_management
#control_it_general_access_protection
#control_it_general_access_protection_authentication
#control_it_general_access_protection_authorization
#control_it_general_access_protection_identification
#data_
#data_hr_new_employee
#data_it_change_management
#data_it_general_access_protection_identification
#data_user_lists
#fd_structure_hr
#general_education_current_role
#general_information_cfm_experience
#general_information_education
#general_note_1
#general_note_2
#general_note_3
#general_note_4
#general_note_5
#general_note_6
#system_erp

Transcript

SP1: Well, just to start: what is your background in training?

SP2: My background? I once started on it MBO. There I did System management. From network management I moved on to system management, so that was quite a technical training. From there I continued to bachelor and there I studied Business IT. #general_information_education

SP1: Okay.

SP2: Sothere I had technology as well as people and business administration. And after that I actually went to VU, studied… For IT audit, to be a RE'er and I succeeded. #general_information_education

SP1: Wow. Okay. Nice route... to RE. Then you have, you really have seen all aspects of well, really IT from all sides. Well, at least many sides.

SP2: Yes that's right. Yes.

SP1: Then you can also spar with your customers on a technical level. Cool. Okay. What is your current role within Baker Tilly?

SP2: My current role? I am in the position of Senior. And with that I am actually partly responsible for all IT audits. And in addition to the IT audit, I am also involved in various data analysis, projects, including the DataFactory. You may have heard of it. So, I am involved in that too. Qlik Sense, ClickView at the time, and also a bit of technology. For example, cyber security scans, vulnerability scans and the like. I am also involved in that. #general_education_current_role

SP1: Okay. So you have a good background, to actually be able to take the step towards continuous financial monitoring over time.

SP2: Yes, for that matter. I have little background in that regard in terms of financial statements. I'm going of course, I have been employed for 9 years, so from that experience I have seen the necessary, but I have never been trained as an accountant.

SP1: No. Exactly. Okay clear. That is most of our colleagues, I don't think they want to go that way.

SP2: No no. I don't think most of them indeed. Although it is especially nice if you work in the annual audit work, then it is to understand the basics. Accounting, but also how yes, how do you enter an audit, what are the points for attention, what is correctness, what is completeness? And accuracy in the form of accuracy. It is nevertheless important that you understand those concepts.

SP1: Yeah, I get it. Okay. Do you have any experience with continuous financial monitoring or automated controls or something along those lines?

SP2: Limited. What I have experience with, for example, but that is, for example, part of Process Mining, if you look at it from the IT angle, which also gives insight into the processes, so you can let continuous monitoring go of course. And from your work as an IT auditor you already have knowledge of controls. And of course a control is also a way to perform continuous monitoring. #general_information_cfm_experience

SP1: Yes. Okay. Okay, check. Well, then first of all I have an extensive question about this the IT general controls. What are the IT general controls that you encounter in practice, that are actually tested there? Because of course we have a very nice guide. It says a lot, but ...

SP2: Yes.

SP1: What exactly do you do in practice? Because I think you actually have three mainlye controls: logical access security, change management and continuity. How do you test it? For example, to start with logical access protection.

SP2: Logical access security always starts with a bit of knowledge of the organization. So you have an interview or you take note of documentation, of procedures that the customer has. It always starts with that and on the basis of that I will look at those measures that I could possibly test, so that they then channel IT control, as they call it so beautifully ... And if the customer has set up the control but not has formalized, so you can not rely on his work, then I make a lot of use of the general IT control work instructions and that we will independently determine the status of institutions in terms of data? Do they conform to the customer's standard, if any? Or is it, does it meet our own value? #control_it_general_access_protection

SP1: Yes, exactly.

SP2: The prospectus.

SP1: And when you talk about logical access protection, you naturally have those three parts…

SP2: Yes.

SP1: Of that. Identification,car, what is it? Authentication and authorization. Could you elaborate on that? How do you test? Actually, I would like to know per part how you specifically test it. For example, what kind of data do you use? Or yes, what control steps do you perform?

SP2: Well, speaking of identification, that is actually the easiest. The data I use for this is always a list of users, active users from the system. And you check that yourself, or then you analyze that list and then you see which users are on it. Are these traceable to a person? Yes or no. And you often do this based on the naming that the customer assigns to it. Well, with the customer. So that's a bit of handwork, I'm afraid. #control_it_general_access_protection_identification #data_it_general_access_protection_identification

SP1: Yes and that is actually. But actually it is a check of two, put two lists side by side.

SP2: No no. It is one list that you export and you view that list from now on, I see Pietje, Pietje Puk.Okay, in this case that is a personal accountant if Pietje Puk actually works there, of course. But if you, says Head of Purchasing, then you know: that is not a personal account.

SP1: Okay. And how do you know that that is a personal account or not? Oh that just distracts you from the list, because you're not going to put that list next to an HR list, for example? #data_it_general_access_protection_identification

SP2: No that's right. #data_it_general_access_protection_identification

SP1: Okay, so you're actually taking out, are you actually filtering out all non-personal accounts?

SP2: Yes.

SP1: Yeah okay. That's a good one. Okay. Of those personal accounts. The piecetest whether those accounts are actually still employed by that person. Does that fall under identification or is that the next step?

SP2: Well that often falls under a bit of yes, procedures included de, I think especially under, yes I don't know if it falls under identification or also process, but that doesn't really matter.

SP1: No.

SP2: In that case, we will look at the processes of how are hiring and how are leaving employment and how is job change going? That is without a process what the customer may have set up and if they can use it and then we can determine that the request has been made by an authorized person. So, for example, did Harry make a request? And was it then properly handled? So he gets function X and function X must be able to A, B and C. We know that, he already knows when he makes that request, ok Pietje gets access so Pietje becomes the name. That is in accordance with their own standard, so you can determine that. For example, he gets three roles. So you can determine those three roles. And the last step is of course someone, he still has to check what it says now and is that correct. And that is actually the mastery you are looking for. #control_hr_new_employee #data_hr_new_employee

SP1: Yes, exactly. Okay. And that actual control thereof? Is it true of what it says? You then perform this again on the basis ofmutations?

SP2: Yes, if you have what we have nowthen. You know the concept between design, existence, operation?

SP1: Yes. Yes.

SP2: Okay. So we have the setup: this procedure. And you assess the procedure of well, is there enough yes, key points with which I think I can establish existence. If there is, then you will establish existence. Then you actually perform a line check. So then you pick one random or the customer delivers one random example. In doing so, you will then determine whether the points, as stated in the set-up, or which are reflected in it. Then, if you really want to go to work, for example, you go to an overview from HR. Then you ask: give me an overview of all people who have been employed, for example. And based on that, you then make a partial observation based on the frequency associated with the process. #fd_structure_hr

SP1: Exactly. Okay. Clearly. That is then just as an intermediate step. If we go back to logical access protection, then after identification you actually have authorization, I think?

SP2: Yes, completely fine. That is about the rights and roles in particular.

SP1: Exactly. What do you do with that?

SP2: For rights and roles is a piece of knowledge of an organization important. So that's to see who can do what? And in particular who has the rights to adjust mutations? Who can create users? Who can adjust rights and the like? So those are superusers, to gain insight there. And then we go back to the procedures as the customer has. So how are rights roles assigned and how then, once assigned, are they periodically reviewed? And that may be based on a job matrix, which the customer has thought up in advance, well, I have a job buyer. A purchaser may do X, Y, Z. And based on the audit and dump from the system, start then you look at a list what you can use for that so you should get a list of the total rights role per user. You can provide insight into what is actually in the system. And by a customer that has been noticed, that check is carried out. #control_it_general_access_protection_authorization

SP1: Exactly. Okay. And what kind of substantive tests do you perform them there? You are indeed going, you have a printout of those rights roles per user and you are going to look in the matrix to see if that suits his function.

SP2: Well, that is something the customer should do as a control measure. In many cases this is not the case, but we do have insight into, for example, who can do what? So we do have insight into it the high rights, for example. And if the customer himself has no procedures to get authorizations in order, that is what I think happens only in well, 95% of the cases. But you must have heard that before. This does not really guarantee that the authorizations are good all year round. And with that you cannot rely on application controls, we will soon, if we come to. #general_note_1

SP1: Exactly. Okay. Clearly. Then you have likeactually last authentication in the list. How's that going?

SP2: Actually in a similar way. So first you look at what is the password policy for examplepassword policy. What is that? What are the requirements from the organization? What do they consider important? In addition, you can of course also ask the customer the question to what extent do you know that the password policy is well organized? So do they have periodic checks on this themselves, for example? On the other hand, we can independently assess these are the password requirements and meet the well, the best practice as we have defined it. #control_it_general_access_protection_authentication

SP1: Exactly. Indeed, because imagine that she, that their requirement is a password must contain four characters, which of course does not meet best practices that we know, but…

SP2: Right.

SP1: You may, you may then also say.

SP2: Yes. So for that matter, you again use lists from the system in which for examplethan the requirements with regard to the password that is taken. Sometimes that is not visible, but you can check it based on a test with the system. So just enter a password as two characters and if all goes well, you will also get a message: “Can't”. Then you keep going until he says I accept it now. Then you know that the number of characters must be minimal, for example. That way you can also do some test versions with it. #data_ it_general_access_protection_authentication

SP1: And password policy is all you have actually does authentication?

SP2: No, password usage is part of that. For example, you also look attwo-factor authentication if there is one. #control_it_general_access_protection_authentication

SP1: Yes. Okay. Any other things you could look at? With authentication?

SP2: No, I think it is in particular. Password policy, two-factor authentication, in particular the authentication of your user when you log in. How do you know that you are you?

SP1: Exactly. Okay. Clearly. Wellyes, then the following is actually in the list: change management. How are you going to check that? Have change management in order?

SP2: You also start with knowledge of that again an organisation. So how does the customer control it himself? And based on that, you could then perform test work, just as the customer has a procedure to determine that changes are being implemented correctly and reliably. Can use the process that the customer has. Not all customers have that and in some cases you will come to a piece of what the release notes, for example. To see if there is standard package, what has changed? In this way you gain insight into changes and then you can determine the impact of any controls you test. #control_it_change_management #general_note_2

SP1: Yes, exactly. And do you often deal with standard packages? Or do you also have a lot of custom development?

SP2: I think 80% just uses standard packages. So that's quite doable. Nowadays you also see more and more the surprise. So that you increasingly use AFAS Online for example or Exact Online. So, and then it has become a lot easier in terms of control, because often those third parties who have an external insurance statement, whereby a third auditor checks whether the change process has been properly set up. #control_it_change_management

SP1: Yes, exactly. And how, okay, how do you know, for example, how are you actually going to check well, how do you know there has been a change in the system?

SP2: Well often, you can see it based on a version number, for example, that there is ... What's in it and all standard packages in any case just have a release note and have a version number. #data_it_change_management

SP1: Yes.

SP2: So based on the previous fiscal year you've been there, you know then was version 1 and now it's version 2, then you know that in the meantime has been updated.

SP1: Yes. Okay.

SP2: In some cases, customers also have an entire change process themselves. And then you also see that they have a ticket system, for example where they keep track of the changes. And if. Yes. And changes need to be approved in many cases and all those approvals and change requests that are recorded in the ticket system. So based on the ticket system you could also determine which changes have been made. But of course the preconditions must be in order. That ticket changes cannot be removed and the like. So there are some preconditions. #data_it_change_management

SP1: Yeah okay. Indeed. Preconditions for the system. From which systemdo you mainly check this?

SP2: You actually check that for all systems that are in the scope for that annual audit. And that is in many casesis that the financial package. There is also a lot of moldings. So a debtor / creditor list, stock list and the like. And in many cases, customers therefore have ERP systems that include the financial flows as well as purchasing, sales, logistics, stock and the like. You also check those processes. In addition, various systems also depend on the audit approach. In some cases if, for example, the personnel process is a significant process and where material flow flows through, then you sometimes see that an HR package is supplemented as a system there, and you can also check how certain things are going there. #general_note_3 #system_erp

SP1: Yes, exactly. Okay. Check.

SP2: Basically it goes actually always about what turnover / costs go through.

SP1: Yes, all those systems.

SP2: Yes. Generally the main part. If a significant flow of material flow passes through it, then often want to at least know the setup. How's it going? What is it? And based on any controls that we will test, you could also go to work for a particular system.

SP1: Yes, clearly. Okay. Then I have change management and then actually the third continuity.

SP2: Yes.

SP1: Well, the same question: What do you do for continuity then to test?

SP2: Continuity is in that respect one, according to the guidelines a little easier. In doing so, it would be sufficient to have only intent. So what the customer tells how the process works.

SP1: Okay. And the moment you, why is that? Why should you only have enough, enough with the setup?

SP2: Well, it's basically Civil Code, well, paragraph out, I am not there, I do not know specifically, but it says that the accountant must report on the continuity piece ... And that design has actually already been mentioned, so taking note is sufficient. In cases where we say that it is very dependent on this, suppose I have a webshop and a lot of money goes through it, then you can feel on your clogs ... If it breaks down, it can really have an impact on the continuity of an organization, so then you have to consider that I think I am doing enough to just set up or should I also move on to minimal existence. Checking, verifying it is so nice, I do a backup, just show that a backup is being made and let me see that that backup can be restored. #control_it_business_continuity

SP1: Yes and do you make it yourself or does the accountant do that?

SP2: We actually make those ourselves. I often do it in agreement with the accountant. That I indicatewell, we think we should do something about this and then consider with me I think it should or should not.

SP1: Yes, exactly. Is it common? That youthis control test?

SP2: No. No. No, actually not, because we, at least the customers I serve, have very little webshop ... Or where the webshop flow is not significant, so that only a limited flow goes through. So where, should it fail, the customer could just call and then place the order.

SP1: Yeah, I get it. Okay. Have I actually had the general controls? Or are there any controls I missed?

SP2: No, I think you have certainly had the most important controls. Of course we test for our, to gain knowledge of an organization, we do test more. Or should we describe more I should say. This concerns, for example, a piece of management and organization, incident process problem management, process management, so how does the customer proceed with IT.

SP1: Yes. But those are not actually controls but more supportive descriptive to get an idea of the organization.

SP2: Right, Yes.

SP1: Okay clear.

SP2: So that is not immediately relevant, but it is important. It may sound a little weird, but what I mean by that is, for example, management organization if the customer has no policy at all,has no idea where IT should go, then it may of course happen that IT is going all the way. And that also has an influence on the change management component. Does it affect access security on continuity and the like.

SP1: Yes, exactly. If you deal with it lax, then you already know that that part would not be good on other points either should sit.

SP2: Right.

SP1: Okay. Clearly. Well, the next question I had was: ideally, which sets and data do you need per check, in the ideal situation, to test them fully automatically? But we actually have them, well we have already discussed them for logical access protection. In change management you indeed indicated that you actually need the change in version numbers between different applications. Well, that might be a good one: changes in applications themselves. And then I'm not even talking about an update but for example a change in the application.

SP2: Yes.

SP1: Correct, are you still doing checks on that?

SP2: Limited. Unfortunately, our customers are not so good that they also parameter changes, because that is what you aim at to set up and administer yourself. So often there is unfortunately not.

SP1: No. Exactly. And you don't have to then, you don't have to do that check or is it just, you just can't do that?

SP2: Well, in some cases is that, a control simply does not exist, because the customer who adjusts it when he thinks well, I think this must be done differently and he adjusts it. There is no registration, so you have, do not know what has changed. In some cases, for example, a system has a login where you can identify someone has changed it, yes or no.

SP1: Yes.

SP2: But those are more compensatory measures to establish that things have not gone wrong.

SP1: Yes, exactly. Okay.

SP2: But otherwise since the same method also applies. If it is documented then you should also go based on changes and tickets.

SP1: Yes. I get it. Okay. Check. Have I. Thenwell, the following. Those are actually three questions that we combined at once. Which system does that data come from? Are they specific systems per data

identity? Well, you had that with logical access protection you indeed called the user list that you need.

SP2: Yes.

SP1: Where does it mainly come from? Or from which system?

SP2: From the system you control. Each system actually has a user list. #data_user_lists #general_note_4

SP1: Okay. So you actually check all individual user listsand of the individual, of the systems? #general_note_4

SP2: Yes. #general_note_4

SP1: Yeah okay. So you don't do it based on one user list, for example your AD? #general_note_4

SP2: No. #general_note_4

SP1: Okay. Why is that, for my image? Because most systems would now be linked to your AD, so you have one central user base? #general_note_4

SP2: Yes, agree. It just doesn't want to be like thatthat if I have an AD and I have a user there, that user is also created in the financial package or in the logistics package or in the HR package. So I have access to AD does not mean that I can access the financial package. So in order to really determine the impact for the financial package, you have to look at the users that are created there separately, if they have been added. #general_note_4

SP1: Yesyes yes, that is a good one. Users are very dependent on each system.

SP2: In addition, not all systems are singles alone. Although I prefer it that way, of course, it is nowhere near that it is arranged that way. It is getting more and more. I also have new solutionand as identity and access management, where everything is centrally arranged. It is not arranged for most SMEs that I visit.

SP1: No. Okay clear.Okay. Yes, then I actually have one, then I actually have the most important data that I had to have and now you have that. In the application controls I tested, I mainly came up with the three-way match, which is actually very important. Sorry, for your image: so I looked at the buying / selling process at a…

SP2: Yes.

SP1: Trade organization. That's just a process to start with. Well yes, I have to start describing it. Well, I actually got the main controls from that three-way match… the three-way match.

SP2: Most complex control out there, but ahead.

SP1: Yes, exactly. Well, well. Then you had the payment lists and creditor master data and at the time you, that those controls are covered, then you can actually say a lot.

SP2: Yes, if you think the three-way match is effective, then you already have a lot of certainty about the correctness and completeness of your purchases. Right.

SP1: Well, then the question to you. Then you havein a three-way match, indeed a list of your purchase orders, your receipts and your invoices that you are going to match. What specific systems do those lists come from, in your experience?

SP2: In my experience, most comen luckily in the system. Where the purchase orders are sometimes removed, so that is still a challenge.

SP1: Okay. Why is that?

SP2: Well, there is no obligation on a purchase order in itself.It only becomes an obligation when you have received the goods. Many systems think now, I have now received it, so I can put the purchase order away; it is no longer used. After you have also made the matching, of course with the invoice. But you also regularly see that there is a separate system where, for example, the matching takes place, where the purchase invoice is scanned and approved. So then you often have the same system in terms of goods receipt and purchase orders and then it sometimes happens that invoice processing uses a different system. #general_note_5

SP1: Okay. A financial system, for example.

SP2: A financial but also a purchase related system, so really what debit / credit is only used to scan purchase invoices, for example, to digitize, an approval workflow to be able to do this, but also to allow matching to take place.

SP1: Yes, okay, because such a customer does. Does that match often happen to a customer in their own system?? Is that their own control that they actually do automatically?

SP2: Yes. You have several customers who have set up that. So that, for example, the system checks when the. That the purchase order is stated, I have made a receipt and I receive an invoice, that it looks like, what is my price on my order? How many did I receive? And that price on the order times the amount I receive, that must also be the price on my invoice. So if that matches or within a certain bandwidth that they say a deviation of 1 euro or 10% that - I just mention something - that is allowed. Is it automatic, is it booked in and is it approved?

SP1: Yeah okay. Okay. The following listthen: creditor master data. Of what kind, are they in a separate system or are they processed in the same system, generally?

SP2: Accounts payable master data is almost exclusively contained in the financial package.

SP1: Okay. If you are actually your second system, your financial package.

SP2: Yes. Yes, unless it is an ERP, of course, as a module there is already financial. Accounts payable master data are by definition actually in the financial module, financial system.

SP1: Okay. And then the latter: product prices.

SP2: Yes.

SP1: Where do they often come from?

SP2: You often see these in the more logistical part of the system.

SP1: Okay and that is often your ERP package.

SP2: That's often you ERP, yes.

SP1: Yeah okay. So in a typical check you run, how many different systems do you check? Because it does sound like you really only have one ERP package. You check that. Is that really the case, in practice?

SP2: In practice you have a lot of ERP indeed. So that makes the number of applications easier. For example a Navision, that is a total solution in that respect. It contains everything. But in many cases

you also just have a separate logistics system, a separate purchasing system, a separate financial system.

SP1: Yes, exactly.Okay. Clearly. I think I've had all my questions. Yes. I'm through it.

SP2: That was short.

SP1: So that waswell that was very short. I mainly need additional information from you and for this also from Stef and your information that fits together very well, so I can process that in one fell swoop. I am also working on a real qualitative research, so more on, not immediately that all data need to be confirmed by several people. It just has to be in line and when it does, that's enough for my research.

SP2: Yes.

SP1: So thus. So thank you very much for this,for your help with this and then I can continue with this.

SP2: Well, you're welcome. Yes, I am just after myselfmore practical too. Because a lot of data is created in a fairly standard way. Only a lot of things have to be interpreted by someone. And that's not something you can automate very quickly, oddly enough.

SP1: What kind of interpretations are you talking about?

SP2: Well, for example, I can. In some interpretations you could also verify, for example the password policy. If you can fish it out in a standard way and you always know in field A1 there is a value X, as an example. Then, for example, the minimum password duration. Field 2 will display this field so you could standardize it further. User lists, for example, who comes from what. Who has the highest rights? Then you have a list of users, but then you don't know who they are in the end?

SP1: Yes. Yes Yes Yes. You don't know if it is a real user or not.

SP2: Right.

SP1: And you would just then in anticipation of my research, but you would, I would say well, put it next to you from your salary package, for example. And then at least it filters out the real users.

SP2: Yes, can. Can. Only I have tried it once. But there you will also come to differences. For example, it may be that people in their AD, for example, that they do not put the name there completely. Or that someone is married in the meantime well, then an extra name will be added. Or names that are very similar or commas in them or special characters. There are some snags and you never get outside people out that way. Because some people are also simply hired externally. They do have a personal account, but they are not on the payroll. #general_note_6

SP1: No. Exactly. So what you actually want to do with this is, you want to automate most of the control and you really only want to work with exceptional cases.

SP2: Yes.

SP1: And the moment you, normally I don't think you have the time to check all exceptions, but because now, because the default part of the check actually runs automatically, you can focus your entire time on those exceptions.

SP2: Yes.

SP1: You would so be able to work much more accurately.

SP2: Agree, yes, Yes. That's right.

SP1: I am myself, I have a background myself, well, I have a bachelor's degree in computer science. After that I worked a lot in different facets from development to data analysis to infrastructure management, so actually the versarigging the asing of certain applications. Data migration, things like that. So, and also just manipulate a lot of old data in such a way that it can also be used for new analysis applications. There you also see that in principle there with certain keys you could always transform data correctly, so that you can at least filter the majority of the noise from it and then you only have a very small set of exceptional cases that you have to inspect manually.

SP2: Yes.It is so. In that respect, it can certainly help. A number of things are becoming particularly difficult to be able to export a number of data sources in a structured manner. Not every package is best suited for this. Some lists you only get in PDF. The system cannot even transfer it to Excel. Or that you get a text file, but these are also exceptions. So if you stick to the 80-20 rule ... Then you can automate a very large part and then you can focus on the exceptions, which of course is much stronger and provides much more added value. I totally agree with you.

SP1: Well, I must say when I came to you, I saw very quickly that quite a lot was done by hand and I was shocked by that, because I am actually not used to that from my IT background. There is always a madman in my team who says: we are going, I will put it in for an evening and I will make sure that it is automatic from now on.

SP2: Yes.

SP1: So, well, I'm really curious if we're here also something to go with it.

SP2: I think you can, but dayou must be able to justify and document properly. Because in the end we all give, we give assurance… And when we throw something in a black box and something comes out and we say “this is good”, then every auditor wants to know what will happen in that black box? So that is a very important art to be able to tell something useful about it. That's a challenge I can tell you.

SP1: Yes, that is indeed the trick. Well, then hypothetically you would.

Interview 6 with VAL1

General interviewee information (#general_information)

Bachelor / Master study	Postmaster Register Accountant
Current role	Director Professional Competence Center
Continuous Financial Monitoring experience	None

Approach to start audit (#audit_approach)

1. Start with the revenue model to find opportunities of fraud.
2. Define the risks based on the revenue model.
3. Defining business processes.
4. Define IT landscape.

Controls and Opinion regarding usefulness

Control	Description	Usefulness
Three-way-match (three_way_match)	A very useful control but it is important to (manually) monitor deviations when mismatches occur.	Yes
Product pricing (product_pricing)	This is important but if a price doesn't match the pricelist or contract it doesn't mean that it is incorrect because there are a lot of motives for this to be different. Misconceptions can occur easily.	Yes
Creditor master data (creditor_master_data)	It is important to ensure that someone cannot mutate master data in a way that is will benefit himself.	Yes
Payments segregation of duty (payment_segregation_of_duty)	The check is important but depends highly on how it is executed.	Yes
VAT (vat)	This control is important but not 'the most exciting' because a mismatch has never occurred before.	No
Change Management (it_change_management)	Change management and General access protection are very important and cannot be separated. They should be both in place to provide certainty. General access protection is very important, but an occurring misconception is that when it is not in place, there is no security. This is not true because it can be that only a very small part was not functioning which has no impact on the systems. This control should be assessed very carefully.	Yes
General Access Protection (it_general_access_protection)		Yes

Business Continuity (it_business_continuity)	Organizations are very dependent on their IT systems. Therefore, business continuity is very important and should not be neglected. However, Baker Tilly does not have clients that depend much on IT, so it is not important for them.	Yes

The interviewee stated that the mentioned controls are the most important ones. (controls_completeness)

Occurring Systems (systems)
There are three types of systems: off-the-shelf systems, custom developed systems, and all in between. Mostly, ERP and Financial systems are uses. These are often integrated.

Continuous Financial Monitoring usefulness (cfm_usefulness)
The most important part would be the assurance that general IT controls are functioning throughout the year. If that is in place, it is guaranteed that all other controls can be tested. Accountants don't always realize this.

List of unique used keys
#audit_approach_business_process
#audit_approach_it_landscape
#audit_approach_revenue_model
#audit_approach_risks
#cfm_usefulness
#control_creditor_master_data
#control_it_business_continuity
#control_it_change_management
#control_it_general_access_protection
#control_payment_segregation_of_duty
#control_product_pricing
#control_three_way_match
#control_vat
#controls_completeness
#general_information_cfi_experience
#general_information_current_role
#general_information_education
#system_erp
#system_finance
#systems

Transcript

SP1: What is your education background?

SP2: Yes, what do you want to know? The final course is a postdoctoral register accountant. Postgraduate. #general_information_education

SP1: Yes exactly, okay. Yes no, that is actually enough. And your current role within Baker Tilly?

SP2: director office technical accountants, that is my job. Do you want to know more about that? #general_information_current_role

SP1: Very briefly, please.

SP2: I am mainly concerned with answering concentrations, I am responsible for the training programs of our accountants, and responsible for our audit methodology. And the translation of that methodology into the tool we use.

SP1: Okay clear. Do you already have some experience with continuous financial monitoring or automated controls?

SP2: No. I have an opinion about everything, but I have no experience with it. #general_information_cfi_experience

SP1: Okay, very good. Then we come to the questions I asked the accountants. The first question I asked was: what is your approach in such a control process, and especially when you talk about purchasing and sales recesses within a typology trading organization. Well, what I actually heard from the accountants there is the same way, but a slightly different start sometimes. One started by recording the risks, the other started by recording the revenue model, because on the basis of this you could actually find the spaces to manipulate the result. And the other started mapping the processes. Well, this is actually a multiple choice question: what is your view on that?

SP2: And I have to choose one of those three?

SP1: No it can also have its own…

SP2: Well, look, if you want to get a good picture of how an organization acts, then the revenue model is a good starting point, simply because the revenue model almost always determines… because then you are talking about typology, then you are talking about opportunities, and actually why they exist as a company. So if you take that revenue model as a starting point, then ... And if you ... Do you know the, if I ask a very stupid question you have to say it, do you know the Barring cycle model from Starreveld #audit_approach_revenue_model

SP1: Not by name.

SP2: Is very old, but still applicable. The value cycle model is actually that there is a relationship between all positions and flows that are in an organization. And if you make a drawing of that, of the value cycle, then the top of that value is cycle, which is generally about the yield flows. And the bottom is about say the purchasing and payment processes. The top of that model always contains the business model, because each business model has its own value cycle. If you have a trading organization that you assume, then that cycle is very simple, because you buy something and you save something. That purchase is a process, that storage is a stand, and then you sell it again, and you get money for it, and that circle is complete. If you have a production process, you will see that the top, where you only buy and sell at a trading company, it becomes a bit more complex, because a conversion process takes place. So if you take the business model as a starting point, you can then relatively ... then you can sort of ... modeling is not quite the right word, but then you have an idea what that organization should look like, in order to facilitate that. So the revenue model is an important starting point in such a setup. Simply also if you have multiple revenue models in an

organization, then you should actually have a separate overview for each revenue model. then you can relatively… then you can sort of… modeling is not quite the right word, but then you have an idea what that organization should look like, in order to facilitate that. So the revenue model is an important starting point in such a setup. Simply also if you have multiple revenue models in an organization, then you should actually have a separate overview for each revenue model. then you can relatively… then you can sort of… modeling is not quite the right word, but then you have an idea what that organization should look like, in order to facilitate that. So the revenue model is an important starting point in such a setup. Simply also if you have multiple revenue models in an organization, then you should actually have a separate overview for each revenue model.

SP1: Yes. and do you see that colleagues actually draw up that?

SP2: Sometimes. It is very different. Sometimes you have to look very far in files, they often continue on what they know about a customer from previous years, that is their starting point. But do you really want to visualize again from scratch how they got those positions, and how do they work together? You just don't see that very much, while you actually just need it to be able to make a good estimate of what those organizational structures look like, what process procedures do I actually expect, and by extension: what risks do I actually see ? #audit_approach_risks

SP1: Yes exactly, that is the order indeed. Okay, very clear. Well, what actually happens next, and that is consistent everywhere, is that the processes are actually outlined with the corresponding IT landscape, a kind of matrix is made, and that in a very clear way. This is also done by the accountant or by the team of the accountant, and not directly by the IT department, the IT auditors. Can you agree with that piece? #audit_approach_business_process #audit_approach_it_landscape

SP2: You mean the way the IT landscape is captured now?

SP1: Yes.

SP2: Yes, in itself. Look… that IT landscape, in the end it is useful to connect that to how it interacts with the business model we just talked about, with the business model. But I think the way in which Beat is meant in particular is happening, there are enough elements that support that. God, what a bad answer. But you also have to do it the right way. What you see a bit at the moment, I think, at least it seems, is that they have opted for a more or less standardized recording. And that is possible to a certain extent. It is not so bad in the IT landscape in itself, but if you capture that IT landscape you must capture it as completely as possible. And why is that? the moment you say, we have an application that we re-scoped out first, and then they don't include it in their IT landscape. And actually that is very strange, because that landscape should actually cover everything, and then you decide: which part of that IT landscape do I need to perform my audit work? That is a slightly different approach. What you sometimes see is that it is being scoped out, and is therefore not included in the IT landscape. I don't find that very useful. #audit_approach_it_landscape

SP1: Okay clear. But for my… from my interest then: why do they scope that out? Does that simply have to do with time and money?

SP2: No, because they think it is not relevant to the performance of an audit. The interesting thing is that they sometimes underestimate that, in which they mainly scope out a BI tool and then use moldings, and usually the question arises: where does that come from? And then in most cases it comes from that BI tool, so you cannot scope it out. Well it is possible, but then you have to use it. So what you mainly see in that is that it is very difficult to be very consistent. Very consistent in business model, how do the positions and flows from the business model interrelate, what IT landscape is there, and how does that IT landscape then support that business model? What is the IT landscape actually designed for? It is a tool, it is not an end in itself. #audit_approach_it_landscape

SP1: No indeed. Okay, that's a very good one indeed. The next question I actually asked them is: what kind of controls do you think when you are talking about such a purchasing sales process, and then I actually got, what is it, five controls forward, and one whole important preconditions that stood out for a while, and the precondition control was actually powers and segregation of duties within all applications, that it must be in order. And then as five controls you have to match the threeway; the price control, who paid the price? Creditor master data, transaction, payment control and VAT checks.

SP2: Yes, those VAT checks are important, of course, but not the most exciting from a control perspective. But you also have the purchasing recesses now, right? #control_vat

SP1: Yes, purchasing sales.

SP2: Okay. Look, that threeway match can just be a very useful control, the question is how they classify and qualify it. That three-way match assumes that the system connects those three different registrations, and when that is the same, or stays within a certain margin that is entered, that transaction just goes through that system. You can determine whether it has been set up properly. What they sometimes forget in that statement is that it almost always includes a manual component because you have to monitor the deviations. So the question is whether they interpret that three-way match correctly… I understand the answers they give to this. #control_three_way_match

SP1: Okay. Yes, I have indeed heard the manual component come up, because there is just always a certain sample that they have to perform.

SP2: Yes, that's something else, I think that is the data-oriented work that you mean, or not?

SP1: Yes.

SP2: Yes no, but this is what matters when you look at a three-way match in itself, and consider it a goal… if the three-way match shows that an order is, for example, in accordance with invoices and receipt. If that connects one to one, then ultimately the system concludes that that transaction can be forwarded and validated, that probably happens at that moment. Every exception, so if, for example, an invoice differs from order and also receipt, it must be assessed manually within the organization. And there too, the question is briefly: how do you define… because you are mainly talking about application controls. #control_three_way_match

SP1: Right.

SP2: How do you define now, and how do you define your application control? Because application control in itself is only the fact that a match takes place, but the whole control also involves settling the exceptions, which is another activity because it is a manual activity. That's what I meant.

SP1: Yes, I understand that indeed. That is indeed how you ensure that it is actually properly registered and that all exceptions are indeed assessed.

SP2: Yes correct.

SP1: Okay, so that was the threeway match we heard coming up. Then you have the price control; who determined the price at the sale? Also considered very important. I think you agree with that?

SP2: Yeah, it kind of depends on how they mean him. What we audit: we audit the financial statements, ultimately the financial statements must account for what actually happened. Suppose for a moment that they agree on a price with a customer that does not match a price list, for example, this does not necessarily mean that the annual accounts are incorrect, that may simply be the choice of the organization to do so. It is also possible that they agree on a price zero because they like to give someone something, or… you can think of anything for that. It only has an important

advantage if it connects to a price list because it often leads to the conclusion: then it will be good. So if the price is in accordance with the price list, then the good price will be invoiced. #control_product_pricing

SP1: Yes, exactly.

SP2: So that price control is important in itself, but if the price that is invoiced does not match the price list, this does not necessarily mean that it is wrong. And there you sometimes see some misconceptions arise about setting the price. #control_product_pricing

SP1: Okay. I also write it down. and what misconceptions do you see arising?

SP2: Yes, especially that it is sometimes said: the price is not in accordance with the price list, so it is wrong. Well, that's not wrong at all, if the price is the billed but justifiable. The only risk you still run is that someone in the organization has made an appointment with their customer, a kickback or something. So you get a slightly different risk profile. But that does not necessarily have to be the case. But the starting point that they say: how that price came about, and how it eventually came about ... because you mainly look at automated systems, I think, how it ended up in a price table, then I understand that they have it as important experienced, and rightly so. #control_product_pricing

SP1: Okay, check. And the third, creditor master data, is considered very important.

SP2: Well, that has to do with payments and the security of your outgoing money movement. Because in the end, if you separate your creditors master data, and separate the transactions from your payment organization, then at least you can be sure that someone cannot mutate master data in such a way that it will benefit you, because it has no purpose, and the one that pay should not be able to get there. So that's a logical response. #control_creditor_master_data

SP1: Okay. Well, then we had control of the VAT, you just indicated that it is not a very exciting one.

SP2: Well, you know, if that VAT percentage is correct in one go, not so much exciting happens anymore. And then you make a round trip based on the turnover, and at least you know that you have accounted for everything. So to a certain extent I get it because it is about tax and your tax return should just be good, but it is not the most complicated. If it is wrong in the system, you have it consistently wrong, that is the disadvantage. #control_vat

SP1: Check. Do you ever see that happening?

SP2: No. No, I don't see that anyway, but I never hear anything about it.

SP1: No, okay.

SP2: No, but you know, how complicated can it be? In most companies, I don't even know what the percentage is, 21 and 8 percent I believe nowadays or something?

SP1: Yes.

SP2: Yes, it can go wrong, but it doesn't happen that easily. #control_vat

SP1: Okay clear. And then the last check that came up is actually the check of the payment list, to finish the five, what do you think of that check?

SP2: That is a very broadly formulated control in this way, the question is then very much what that control entails exactly. The check of the payment list, yes you know ... that is probably in the range of: invoices are collected in a batch, they come in a list and the one who is allowed to authorize in a payment organization, has to give his approval. Then the question is what the person does when

he authorizes the payment list; does he take a quick look or does he also take all the invoices and all kinds of other documents and look in some more detail? So in itself, that check is important, but it is very much dependent on how it is completed and executed. #control_payment_segregation_of_duty

SP1: Okay, but a very important control.

SP2: Well, it is ultimately your final check before your money leaves your company, so in that sense it is an important check.

SP1: Okay, so all five of the controls I've actually seen coming up here are pretty important in themselves, just ...

SP2: They are not surprising.

SP1: No exactly. Only the VAT control is one of which you say: that is such a simple one, not much happens with that.

SP2: No.

SP1: Okay, do you have a control that you expected to see coming up that I haven't mentioned now?

SP2: Well, if you look at the process, there are always two elements in such a process: purchasing and sales numbers and price. The numbers should be received in the threeway match if it is properly arranged, so in principle that is a very important check if it is functioning properly. And that price component is in the price control that we just talked about, so yes, I think that's what you usually have captured. With all the conditions that are arranged around segregation of duties and what you also see here is that they also appoint the payment organization, so on the purchasing side you have the outgoing money movement ... so in that sense I think they are the most logical, the most mentioned obvious controls, especially within a trading organization. #controls_completeness

SP1: Okay, that's good to hear.

SP2: It wouldn't have been as nice if it hadn't been. #controls_completeness

SP1: Yes exactly, or that you suddenly see things that you actually ... okay. Well, then I do indeed have a follow-up question: what kind of systems do you usually encounter within that type of organization? And then I was actually told steadfastly: ERP and financial packages next to it.

SP2: Yes, I just wonder… I think if you look at the landscape of automated systems you now have three options: off the shelf, which is really completely standard, completely custom, that's what it says it is, and all that in between, what you see to an increasing degree, of course, is that they are standardized packages, but that you can make it very specific with all kinds of parameterisations. And whether it is an ERP environment that is fully integrated in one environment, or whether they are systems together, I don't know. I do think that teams sometimes underestimate whether there is an interface in other systems, and whether they always have sufficient insight. But that is a bit of a feeling, and especially the business intelligence environments, I don't know if they always have that in view. Yes, those ERP systems, it is indeed the financial system that is then integrated into the ERP system, you see that of course. #system_erp #system_finance #systems

SP1: Yes, check. Okay, well for the sake of completeness I also asked the accountant whether he saw the added value in testing these controls more than once a year, I got a firm yes to that. It might not be of direct interest to the customer because the customer often controls this internally as well. Do you have an opinion about that?

SP2: Yes, I don't know if the customer is always in control, that is of course the question, and if they are very aware of it, of the controls, especially in an automated environment, whether they are aware that they function, how they function, and in what context they function, I don't know. that will very much depend on the environment in which the customer operates. I think they understand that they want it to be tested more often. The question is how necessary this is if you mainly focus on general IT controls. If you look at the system of general IT controls, that they have to guarantee that ... application control would we mainly talk about, I think, that they work? then you don't have to look at the individual application controls. Because you look at that once. #cfm_usefulness

SP1: Okay, so the most interesting thing in this is to be able to guarantee that your IT general controls 365 days a year ...

SP2: I think that's the most important thing, yes, but I wonder if our accountants always realize that. I hope that IT realizes this, but in the end those general IT controls determine whether that application control can continue to function as you think it functions. #cfm_usefulness

SP1: Yes, clearly. That was also my approach at the beginning of the interviews, but that image did not live that way with the accountants, so I find it interesting to hear it again.

SP2: Yes, the question is whether they understand conceptually what the impact of automation is on internal management and all kinds of other aspects of customer control. And when they make these kinds of comments, you think, yes, I think ... then the question is whether they really understand the concept.

SP1: Yes, okay, clearly. Then we will continue with the IT general controls. Immediately a nice bridge there. First of all, the question: what is your ... you had completed an RA postmaster, or obtained an RA title?

SP2: Yes.

SP1: Have you also done something with RE?

SP2: No no, it is too difficult for me. No actually not. Or actually not, not at all. But because of my connection with the VU, I do look at the impact of IT on the audit. But I did not follow any training myself, no, and I must also say that I approach most things mainly conceptually and not so much in terms of content. I don't understand bits and bytes, but I do understand the conceptual framework of IT for the sake of control over the years. I think this is also the crux for accountants: if they understand that conceptual framework, it will become much easier. All right, go on.

SP1: Okay, well the question to the IT auditors was actually: what are the IT general controls that are tested in practice, and then three categories emerged, which are, as expected, I think logical access security, change management and continuity, whereby continuity is already almost falling off because that is just not often important. Logical access security was the most important IT general control, containing the three headings of identification authentication and authorization. Do you also see that as the most important IT general control?

SP2: Yes, of course it is true that if you have very good logical access security, but your change management is not in order, then I still think you have a problem. So I don't know if you can see those two completely apart. the only good news is that if you don't have a change, you won't be bothered by it. But these are certainly the most important. And those logical access conditions for knowing who does what and who can do what, and ultimately securing the segregation of duties that you have agreed in your organization outside of the automated systems. So yes, I understand that they are very important. What I find fascinating is continuity, of course that is a... if there have been no disruptions in a year, a somewhat less important concept. What you only have to realize is that the greater the dependence of an organization on the automated environment, the more important continuity. And I don't know if that is always reflected in the control files, because if that automation is fully interwoven with the primary processes, then good control of continuity is also

important for the continuity of the company. #control_it_change_management #control_it_general_access_protection #control_it_business_continuity

SP1: No, I did indeed get that as a very solid note from colleagues, continuity is generally not exciting because it is not supportive of the core business processes, or that these are not the only channels. But when that is the case, then something must actually be done for that. If something is done for that, it is mainly checked for existence.

SP2: Yes, it must be that this is happening now, in principle I understand that. This also has to do with the type of customer we have, we do not have many customers where the company is down as half a day, that they do not survive. So I understand that with a certain amount ... they don't put a lot of time and energy into drilling that. But again, that has a lot to do with what type of company it is. If you look at a company like Schiphol, I believe that if those two hours are without automation, they are bankrupt. So that's where the continuity aspect is more important, but I also understand the topics they mention.

SP1: Okay. Yes, I think the IT general controls are logical access security, change management, quite straight forward.

SP2: Yes, the only thing you always have to ask yourself, there you see a misconception sometimes I think between accountants and IT auditors; what is the actual impact of ... No, if IT auditors that logical access protection is not properly configured, the next question is: what is the direct consequence of the fact that logical access protection is not properly configured? Because that is of course also the extent to which the system enforces that, I know a lot, has to periodically change a password, that is also the complexity of the password that is enforced by the system, which is also the approach to that sort of thing, and the question is, suppose it doesn't meet the criteria that the IT auditor sets for it, what that means for the underlying information that is created in that system. Well, And that balance is still lost. I have seen quite a few conclusions in the past where the IT auditor said: The logical access security policy does not meet the criteria of the automated system. Well, that seems to me to be a conclusion that is a bit short-sighted. #control_it_general_access_protection

SP1: Yes, then you end up in that whole gray area where the human touch actually plays a major role.

SP2: Yes, I don't know if it is, I think it is mainly about understanding the importance of automation in this case of auditing the financial statements, and we don't audit an automated system, we audit the financial statements. So the automated system is not an object of investigation but the financial statements. And that is important.
Or the financial justification, if you want to draw it more broadly to your research.

SP1: Yeah okay. And you see that it is still sometimes missed.

SP2: Well, it is missed .. I think that the translation of residual risks due to not entirely optimal logical access security, that it is not good, and that it is said too rigorously if a gap is found in logical access security, that it does not can be supported on automated systems. I think that's a bit more nuanced.

SP1: Yes, clearly. Let's take a look, then the follow-up question was actually, but that is a more in-depth question, what sets of data do you need per control within the ideal situation to be able to test it fully automatically? Well, there you actually came on the standard list: usage lists per application, AD: active directory transport, and all users, passwords, changes of passwords, roles, rights, in order to indeed test that device. Well, change management release notes to check: well what has changed? Do you have any additions to that? Or is this outside ...

SP2: No, this is very specific. Not me. This is also very much an IT auditor party, so to speak.

Interview 7 with DA1

General interviewee information (#general_information)

Bachelor / Master study	Bachelor in Business Informatics
Current role	Manager at Baker Tilly IT advisory department, responsible for all data analytics solutions.

Automated data extraction from customer systems and Data Warehouse import (automated_data_extraction)

Baker Tilly currently uses specific tooling (for SAP ERP) to extract data automatically from a customer ERP system. An export request is defined, and the customer has to approve this. The data will be loaded on a central system within Baker Tilly. The further processing of this data has to be manually triggered. This has never been done periodically before, but it should be possible. Also, data is being extracted automatically from an Exact Online HR system.

Common ways of data extraction from customer environment (common_data_extraction_approach, data_extraction_limits)

Firstly, the needed data, tables, and fields are defined based on the controls that will be tested. These mostly come from one central ERP system. Then the way of data extraction is defined based on the system manuals. For some systems this has to be done manually through the interface by exporting data to an Excel file, for other systems this can be done by running a query on the SQL Server database. This is always done manually by the customer. This data is uploaded to a secure Baker Tilly file share. From the share, the data is either manually loaded and imported in the Baker Tilly Data Warehouse (using TimeXtender software) and displayed on a Qlik Sense dashboard. Or the data is manually loaded into IDEA which is a system for data analysis in the Accountancy branch.

No limits have been experienced yet. File sizes have been up to 45GB and all still work.

Data Privacy (data_privacy, data_anonimization)

Only data that serves the purpose (predefined goal), data such as personal identification numbers, can be extracted. Sometimes extra data is extracted as there might be a need for it later. Data does not have to be anonymized.

Data Retention (data_retention)

A data retention policy of 365 days is being used. Data cannot be retained after the audit has fully finished. If a comparative analysis had to be performed, that data will have to be requested again. This is important because if the customer get sued, Baker Tilly should hand over all data available on that customer. If Baker Tilly has data that the customer has destroyed, he will not be happy about that.

Data Integrity (data_integrity)

It is important that the integrity of the data from system to data warehouse is maintained. The data has to come directly from the system, has to be recent and cannot be tampered with.

Data Extraction tooling (data_extraction_tooling)
For SAP ERP data exports, SmartExporter is being used. For other applications data is mostly exported through the frontend or through the database such as Microsoft SQL Server. For other more modern cloud-based systems the API can be used.

Baker Tilly does not want customers to do things such as opening ports. Another approach that is being used Robotic Process Automization (RPA) where a robot is placed in the customer infrastructure which automatically exports data and uploads into the Baker Tilly premises.

General Note (general_note_1)
When data is being exported for other purposes than the financial statement audit, the usage of it depends on the agreements with the customer.

List of unique used keys
#general_information_education
#general_information_current_role
#automated_data_extraction
#data_extraction_limits
#data_privacy
#data_anonimization
#data_retention
#data_extraction_tooling
#data_integrity
#general_note_1

Transcript

SP1: Getting started, what is your background, education background?

SP2: Business Informatics. #general_information_education

SP1: Look. Business Informatics. And do you have anything else with it done an RA?

SP2: No.

SP1: Okay, alright. And what is your current role within Baker Tilly?

SP2: I am in Baker Tilly responsible for all data analytics solutions and the entire infrastructure that stands for them. So I manage a team that includes ... who are involved in all data solutions. #general_information_current_role

SP1: Alright, all right. Is automatic data extraction currently taking place from customer systems? And will this data also be loaded into our own Baker Tilly data warehouse?

SP2: Automatically, yes. Periodically, no. For example, we have purchased a tool for SAP that we can automatically let data export from our customers. So we define the export. And the customer has an application running, so to say that the export definition can be started. And that's where files come from. And well, those files still have to be manually put, say, on BCR and, so to speak, to be read into our applications. We could also set that periodically. We do not do this now, because that is not what the assignment is for, what we are doing it for now. And well, that data is then further processed. And I'm thinking for a moment. Furthermore - it concerns the audit, so the financial audit - nothing else. No. And look, at MKB Advies and Employment Advisory, that is what

happens. There we do automatically retrieve data from Exact Online and from Nimbus. And we process it. But that is another branch of sport. #automated_data_extraction

SP1: Okay. But the data is therefore also loaded in the Becatili data warehouse?

SP2: Yes.

SP1: And further processed. Okay clear. What are, how does that process go when you actually need data from a customer environment? Well, for SAP you did indeed mention theexporter. But what about the whole process when you want to have that data from the environment and load it into your data warehouse? So you just mentioned on Baker Tilly's side the exporter, an application has to be submitted.

SP2: Yes. But that… It naturally starts with fine tuning, what does the account want have ant now for a data and what controls does it want to seal with that? And then we go okay, what data do we need from the system? Well, that knowledge we have, it is there… and well, a number of others. With me, among others, of a number of systems. And then we decide okay, we need these tables and we have a manual for that - so we have a manual from Navision and a manual for SAP and a manual for Exact - how do you get that data out? And those guides differ from, left click, right click, export to Excel to, open the SQL Server Management Studio and run this query. Then - we often do that or together with the customer or the customer does it independently, depending on whether we know the customer and whether there is a good IT person or not, then we often do it together with a check - after that the data comes to us via a Huddle or via Baker Tilly Cryptshare. And we then read it into TimeXtender. And then it is actually relatively automated. It is read into TimeXtender and then panned to Qlik Sense dashboard and there is a result. That is one option, which is now the case with SAP. With the other it is often that analyzes are done in IDEA. And then that data ends up on our i-disk and from there it is loaded into IDEA and from there the analysis is done. That is one option, which is now the case with SAP. With the other it is often that analyzes are done in IDEA. And then that data ends up on our i-disk and from there it is loaded into IDEA and from there the analysis is done. That is one option, which is now the case with SAP. With the other it is often that analyzes are done in IDEA. And then that data ends up on our i-disk and from there it is loaded into IDEA and from there the analysis is done. (common_data_extraction_approach)

SP1: Okay. And what is IDEA for package?

SP2: IDEA is a data analysis toolfit, specifically for the accountancy sector. Because everything is logged in automatically, you cannot edit data, things like that. So it's a closed Excel, so to speak.

SP1: Exactly. Okay clear. Well, the next question is actually, are there, are there any limits in this? And a limit that I can already imagine, is that you can manually upload data to Huddle or Cryptshare, for example, and then load it into TimeXtender, which is the limit, the size of the amount of data. But also a limit, the automation. Is that really the case? Or…

SP2: No. We have not yet experienced it. We recently downloaded 45 GB files. And that is still possible, with Cryptshare we can transfer that data. So there is no limit. Neither is the TimeXtender side. Then the limit should be in our infrastructure. And we haven't run into that yet, because it will simply be expanded. #data_extraction_limits

SP1: Okay clear. Then we go tosome other types of questions. Because it is for you at the moment that the customer gives permission that you are allowed to use data - data from certain tables - that data may therefore be extracted from the table in its full original condition and used within Becatili for further processing. ? Or do things like anonymization or things like that need to take place there on the customer side?

SP2: Well, we should only have data that serves the purpose of the analysis. So if the analysis is, does every employee have a BSN number in the system? Then we may copy the BSN numbers and

employee information, because that serves a purpose. That goal must then be registered in the file. So we may not transfer data and then do nothing with it and in the file, so to speak. That data must then be removed. So then you have done an analysis, you have spent hours and then you delete everything. That does not happen. #data_privacy

SP1: Okay. And data such as transaction data - yes - no - invoice data, does not need to be anonymized?

SP2: No. We have to be the starting point, you have to get as little data as possible. Hey, so minimalist. But yes, sometimes we take extra fields, because we think we will need them in a later analysis, at a later stage. Or that it… Look, if you say to the customer yes, we have voucher number 1034. And then that customer says yes, no idea, who was the invoice addressed to? So that's why we take the invoice number and name with us. Strictly necessary, no. But it definitely accelerates, in other words, coordination with the customer about the results. So we weigh that up. #data_anonimization

SP1: That is indeed a consideration? Okay. And how long can that data be kept?

SP2: Nou, that's the discussion going on. In principle, we may no longer have the data on our e-disk if the file is closed. So if you are talking about annual accounts, then that data may be on-hand during the annual audit. But as soon as the file is closed, it should be in the file and no longer on our e-disk. And there, we cannot access the file, so to speak.

SP1: And the moment it is not on the e-disk, then it is no longer in TimeXtender?

SP2: No. Right. In principle we have a retention policy of 365 days. And the dashboard for 180 days. So we keep the data approximately 365 days. And the dashboard remains available to the accountant for 180 days. #data_retention

SP1: Okay. And when you would like to perform a comparative analysis the following year, is that not possible?

SP2: You have to request the data again.

SP1: The data from that previous year.

SP2: Because it is a new assignment. So then you have to say to the customer ok, I want the dates of 2018 and 2019. #data_retention

SP1: And are there no further agreements to be made with that customer? To do that…

SP2: Yes. Of course it is. Look, only then you have to make an additional assignment.That is difficult under the annual accounts flag. And if you do an additional assignment, you can.

SP1: Okay, exactly. So, for example, if you are busy with an actual data analysis assignment, you can do that kind of agreement again make it? And this piece is actually covered by the rules or conditions of the annual account assignment?

SP2: Yes. Because in principle it is so, suppose the customer gets a raid - from the For example, the tax authorities - then we must - no - they can then ask us to deliver everything we have from that customer. And if it contains things that are not in the file - for whatever reason - then we have to deliver them. While, if the customer has thrown away his administration - to say, to obscure something - and we still have that entire administration, we have to deliver it. The customer will not be happy with that. #data_retention

SP1: It is true.Okay. Then I am curious about the tooling that is used within Baker Tilly for data analyzes. So you just indicated that for the good thing, extraction is using a SAP tool.

SP2: Yes. At SAP we use SmartExporter. That is a tool that is from a German party and that is provided by CaseWare IDEA to us. So we just pay for that. Well, in other applications you can often get it out through the front end. Or via data, say Microsoft SQL Server, that we know the query, which is a kind of extracts of the data. For transforming and analyzing, we then actually use two flows. One stream is IDEA. So in that we actually do transformation and analysis, so to speak. That is one flow. And the other stream is then TimeXtender and Qlik Sense. And that applies to the standard analyzes. So then you mainly talk about SAP and audit file, that is financial journal entry testing, so to speak. For that we have standardized dashboards and then you talk about TimeXtender and Qlik. And you actually have a third stream, which is of course Excel. Because you always have stubborn figures who just keep doing the entire data analysis in Excel. #data_extraction_tooling

SP1: Exactly. Okay, between extraction and test formation, do you also have a bit of transport? Because the data actually comes from customer data and for that you only use Cryptshare and Huddle?

SP2: Yes. For financial statements activities, Yes.

SP1: And for other types of work?

SP2: Well, of course we have some software packages are in the cloud. And they have APIs that we can connect to and then we use them. Only that is really only for assignments that… We are not going to build a connection with an API for an annual audit. Because we don't know if that customer will still be a customer next year, so that's a shame. Look, if we have it, we use it. So if we now have a customer who has Exact Online and we have to do an annual audit there, then we can use that API, because we have that connection. And the same applies to Nimbus. So if so, we unlocked several such packages. And you don't see that very often in the audit of annual accounts. Because those are just the smaller customers. #data_extraction_tooling

SP1: And the moment you have one you have a recurring customer and you know that he will still have the annual accounts audit carried out by Baker Tilly in the next few years? Because I think there are also?

SP2: Yes. There certainly are. But still it must be within that budget of de annual accounts. And there is often just money for that. That should be done as lean and mean as possible. So we can place it with the customer. And that export, the customer can do fine, so why should we invest money in that?

SP1: Exactly.

SP2: That's kind of it… And look, it's not our project. So a budget is made and we are asked, how much time will you take that data analysis? And if that customer delivers it in accordance with our manual, it will take us eight hours. Well, if we still have an API would have to make to collect that data, it would suddenly take us forty hours. And that makes those financial statements much more expensive. And they don't want that. While it might bring them something in the other years. But it just isn't looked at like that.

SP1: Okay. And then imagine that you are kind of changing mindset. For example with one of the more innovative-minded accountants - who I also interviewed - who would like to do a piece of data analysis with, well, would like automated data analysis to take place over a number of years. Then you could, for example, build a connection to a client's API to get that data?

SP2: Yes. Then there are two possibilities in there. On the one hand, that is of course just look, many of our customers - the larger customers in particular - do not have cloud solutions, so it all runs on-premise. So if you want to retrieve automated data, then or you have to make a connection to that database, so you have to open ports. Well, that's what Baker Tilly is before and Baker Tilly says, we don't want that, pertinently. Because then we will tell a customer dear customer, port 443 on that server must be tunneled open to our data center and ready. And if someone has a ransomware attack and it has entered port 443, then we have all appearances against it. So they say yes, we

don't want that, until other solutions can be found. Another option is to use RPA. So say a robot, automated that allows data to be exported and uploaded somewhere. And on our side, another robot will take it off and we will process it. We're looking at okay right now, can we do something with that? Well and then it certainly could. #data_extraction_tooling

SP1: Okay. And within that first variant,Have you ever thought about putting a tool on the customer side - well, that is indeed RPA, what you say -?

SP2: Yes. We had a pilot with inFlow. So a product, say, which would also retrieve data. Only financial data by the way. There was the idea of yes, we install a piece of software at the customer and he will connect with the software in the cloud from inFlow to retrieve that data. But yes, even before that, gates had to be opened to establish that communication. And they said yes, we just don't want that. So ... Because there are - you know and with the type of customer we have - customers who just log into their firewall on their router and say okay, port 443 open. And don't think about the consequences. Have a look. And if you are talking about - well, within the scope of my research you also need certain sets of data for the IT general controls. A very simple example is AD exports. To be able to say something about the IT general well, about the control of well, as security, on a continuous basis. Then you actually want to measure on a continuous basis whether it is good, for example, which users all have a good password. Continuous retrieval of that kind of data - AD exports - has a certain tooling been examined before, for example? So we are now with trying RPA. I now have a server running on my local notebook with a robot on it. And it does nothing but download and save that CSVDE export every five minutes. So we are now testing okay well, does that work? And what should we arrange for this on the customer side? And what should we arrange on our side for that?

SP1: Exactly. And what should be arranged for this on the customer side?

SP2: Well, we have to put a piece of software there. So we need the agent therefrom UiPath in this case. So then we need an account under which that robot is constantly running. That robot needs an internet connection because it has to put down that data. And we must somehow establish that that customer has not edited the file before it comes to us. So actually that is relatively simple for the AD, because you can do quite a few checks on that. But yes, we have to organize it.

SP1: Be done. Okay. And to continue to establish that the customer has not manipulated data. The moment you, that the data is actually automatically read from a system, then there can be no manipulation in it?

SP2: Well, you have to interim save the data somewhere. And look, the customer has, we don't have access to the customer's system. So the customer can also say, you know what, I'm just going to manipulate that robot so I can say, just manipulate the file that he has to send to us. And things like that, of course, is quite possible. So you have to build in checks and balances of okay, how can I be sure that the file I have now received has not been changed? That he did not do strange things in it. Well, that is relatively easy to do for such an AD export. But if you start looking at parameters and a system. Okay, how do I know for sure that that parameter export was made today? And that it doesn't just send the old one from four weeks ago to us for three weeks? #data_integrity

SP1: Exactly. And of course this wouldn't be the case when you exported that data for a purpose other than for the financial statement audit, right? Because then the customer chooses that they want this analysis to take place. So they will also be less inclined to manipulate the data. #general_note_1

SP2: Yes. Unless you dare the one who cheats. Look, if you as a system administrator say, monthly transfer money to your account - by structurally including your bank account number in a payment batch - then you obviously do not want us to see that periodically. #general_note_1

APPENDIX B: CONTROLS, PROCESSES, DATA AND APPLICATIONS

Appendix Table 1 Processes, Controls, Data and Systems

Control ID	Control	Type / Process	Description	Data	System
C01	Three-way-match (three_way_match) (RA1, RA2, RA3, VAL1)	Procurement	A purchase order should have a receiving receipt and invoice. Those three items should match and be tested by different people (segregation of duty).	- Purchase orders (RA1, RA2, RA3) - Receiving receipts (RA1, RA2, RA3) - Invoices (RA1, RA2, RA3) - Message traffic (EDI) (RA2) Datasets can be very large and hard to extract because of the volume. (RA3)	- Enterprise Resource Management (ERP) system - Banking application (RA2)
C02	Product pricing (product_pricing) (RA1, RA3, VAL1)	Procurement	The price of products on the receipt should match the price as stated in the overlapping contract.	- Invoices - Product pricing contract	- ERP system
C03	Turnover (turnover) (RA2, RA3)	Sales	The number of sales (Q) can be tested by the inventory at the end of the year, minus the inventory at the start of the year. In between, the number of sales and failure can be seen.	- Product stock (inventory counting) (RA3) - Sales orders (RA2)	
C04	Payment segregation of duty (payment_segregation_of_duty) (RA1, RA3, VAL1)	Payment	Making a payment requires segregation of duties and has to be checked by at least 'four eyes'.	- Payments - Invoices - Invoice approvals	- Bank application
C05	Change creditor master data (change_creditor_master_data) (RA1, VAL1)	Payment	Changing the data of a creditor (person or organization who receives money) requires segregation of duties and has to be checked by at least 'four eyes.	- Creditor database - Data changes and approvals	- Bank application - ERP system
C06	New Employee (hr_new_employee) (ITA1, ITA2)	HR / IT General	When a new employee joins the company, an account has to be set up. How is ensured that he gets the right access (authorization).	- List of HR mutations	- Active Directory - HR system
C07	Employee new role (hr_employee_new_role) (ITA1)	HR / IT General	When an existing employee gets a new function, his roles and rights should change as well. How is ensured that his access is proper (authorization).		- Active Directory - HR System

C08	Employee leaves (hr_employee_leaves) (ITA1)	HR / IT General	When an employee leaves the company, his access should be revoked (authorization)		- Active Directory - HR System
-	General access protection (it_general_access_protection) (RA1, RA2, ITA1, ITA2, VAL1)	IT General	Identification, Authentication, and Authorization	- Users in the systems - Their last login - Their roles and rights - Account details (username) - Last password change	- Active Directory
C09	Identification (it_general_access_protection_identification) (ITA1, ITA2)	IT General	Which person does a user in the system represent. When you log in with a username, does that represent a person.	- Users in the system(s) - Usernames convention / mapping - List of employees from HR (ITA2)	Active Directory
C10	Authentication (it_general_access_protection_authentication) (ITA1, ITA2)	IT General	How do you prove that you have that identity. Are password requirements proper. Is the password policy up to requirements, and do all accounts comply with this. Test this by inputting passwords that do not match the policy and see if this is allowed. Is two-factor authentication enabled. (ITA2)	- Password requirements (ITA2) - Password policy per user	Active Directory
C11	Authorization (it_general_access_protection_authorization) (ITA1, ITA2)	IT General	What can you do in the system. Roles and rights within the system.	- Roles and rights per user in the system(s) - Which user should have which roles/rights	Active Directory
C12	Change Management (it_change_management) (RA1, RA2, ITA1, ITA2, VAL1)	IT General	What changes in system configuration have been made and what software upgrades have been performed. What was the impact of those changes and how have they been tested to ensure the correct functioning of the system(s) and business processes.	- Overview of all system changes and updates - Changelogs per update	- Ticketing system - ERP system

			This can be for custom-made software and off-the-shelve software. How are changes and software updates being implemented, and is this in a correct and reliable manner. What things were changes during an update, and what was the impact on the systems. If the used systems are from suppliers that are being audited themselves, it is very reliable. Are changes tracked in a ticketing system and being approved by multiple people.	- Approvals per change - List of all software systems (ITA2) - Change tickets from ticketing system. (ITA2)	
C13	Business Continuity (it_business_continuity) (ITA1, ITA2, VAL1)	IT General	For businesses where IT is crucial in day-to-day operations, the continuity of these systems should be guaranteed by having proper backup and recovery measurements in place.	- Backups schedule - Backups test - Overview of IT landscape	

APPENDIX C: VALIDATION RESULT FORMAT

Appendix Table 2 Customer application mapping

Application Component	Application Function	Actual System	Hosting location
Procurement portal	Supplier product pricing management		
	Procurement order management		
Warehouse management	Incoming goods management		
	Product stock management		
	Sales order processing		
Sales order management	Sales order management		
Bank system	Transaction management		
Creditor system	Manage creditor data		
Personnel management	Employee management		
	Employee function management		
User directory	User management		
	Authorization management		
	Authentication policy management		
	User authorization		
Support system	Ticket management		
	Release notes storage		

Appendix Table 3 Customer data mapping

Application Component	Data entity	Data location in actual system	Data access method	Data access frequency
Procurement portal	Procurement order			
	Supplier product prices			
	Procurement invoice			
Warehouse management	Goods receipt			
	Product stock			
Sales order management	Sales order			
Bank system	Bank transaction			
	Bank transaction approval			
Creditor system	Creditor data			
	Creditor data change authorization log			
Personnel management	Employee file			
	Mutation log			
User directory	User account			

	User authentication policy			
	Authentication settings			
	User account rights			
Support system	Release notes			
	Support ticket			
Target system	Application log			
	Application metadata			

APPENDIX D: VALIDATION RESULTS

Case 1: Interview results tables

Appendix Table 4 Customer application mapping case 1

Application Component	Application Function	Actual System	Hosting location
Procurement portal	Supplier product pricing management	Navision ERP	On-premise
	Procurement order management		
Warehouse management	Incoming goods management		
	Product stock management	WICS	On-premise
	Sales order processing	Navision ERP	On-premise
Sales order management	Sales order management		
Bank system	Transaction management	Rabo Telebankieren SaaS	Cloud
Creditor system	Manage creditor data	Navision ERP	On-premise
Personnel management	Employee management	Delta SaaS	Cloud
	Employee function management		
User directory	User management	Active Directory	On-premise
	Authorization management		
	Authentication policy management		
	User authorization		
Support system	Ticket management	Support ticket system	Cloud
	Release notes storage		

Appendix Table 5 Customer data mapping case 1

Application Component	Data entity	Data table in actual system	Data access method	Data access frequency
Procurement portal	Procurement order	Purchase Header	Database queries	Unlimited
	Supplier product prices	Standard Vendor Purchase Code		
	Procurement invoice	Purch. Inv. Header		
Warehouse management	Goods receipt	Purch. Rcpt. Header		
	Product stock	Local database		
Sales order management	Sales order	Sales Header		
Bank system	Bank transaction	User interface	Manual CSV Export	
	Bank transaction approval			

Creditor system	Creditor data	Vendor	Database queries	
	Creditor data change authorization log	Vendor Bank Account		
Personnel management	Employee file	User interface	Manual CSV Export	
	Mutation log			
User directory	User account	AD Database	Powershell scripts	
	User authentication policy			
	Authentication settings			
	User account rights			
Support system	Release notes	Unknown	Request CSV Export	Unknown
	Support ticket			
Target system	Application log	Unknown	Manual lookup	Unlimited
	Application metadata			

Case 2: Interview results table

Appendix Table 6 Customer application mapping case 2

Application Component	Application Function	Actual System	Hosting location
Procurement portal	Supplier product pricing management	SAP ERP	On-premise
	Procurement order management		
Warehouse management	Incoming goods management		
	Product stock management		
	Sales order processing		
Sales order management	Sales order management		
Bank system	Transaction management	ING Banking SaaS	Cloud
Creditor system	Manage creditor data	SAP ERP	On-premise
Personnel management	Employee management		
	Employee function management		
User directory	User management	Active Directory	On-premise
	Authorization management		
	Authentication policy management		
	User authorization		
Support system	Ticket management	SAP ERP	On-premise
	Release notes storage		

Appendix Table 7 Customer data mapping case 2

Application Component	Data entity	Data table in actual system	Data access method	Data access frequency
Procurement portal	Procurement order	EKKO, EKPO	Database Queries	Unlimited
	Supplier product prices	TVKD		
	Procurement invoice	BKPF		
Warehouse management	Goods receipt	MKPF		
	Product stock	S031		
Sales order management	Sales order	VBAK, FPAP		
Bank system	Bank transaction	Unknown	API	
	Bank transaction approval			
Creditor system	Creditor data	LFA1, BUT0BK	Database Queries	
	Creditor data change authorization log	LFBK		
Personnel management	Employee file	PA0003		
	Mutation log	PA0003		
User directory	User account	AD Database		

	User authentication policy		Powershell scripts	
	Authentication settings			
	User account rights			
Support system	Release notes	STMS	Database Queries	
	Support ticket	STMS		
Target system	Application log	STMS		
	Application metadata	RSPARAM		

Case 3: Interview results table

Appendix Table 8 Customer application mapping case 3

Application Component	Application Function	Actual System	Hosting location
Procurement portal	Supplier product pricing management	Proteus ERP	On-premise
	Procurement order management		
Warehouse management	Incoming goods management		
	Product stock management		
	Sales order processing		
Sales order management	Sales order management		
Bank system	Transaction management	Rabobank Telebankieren SaaS	Cloud
Creditor system	Manage creditor data	Proteus ERP	On-premise
Personnel management	Employee management	Proteus ERP	On-premise
	Employee function management		
User directory	User management	Active Directory	On-premise
	Authorization management		
	Authentication policy management		
	User authorization		
Support system	Ticket management	SQN Support SaaS	Cloud
	Release notes storage		

Appendix Table 9 Customer data mapping case 3

Application Component	Data entity	Data table in actual system	Data access method	Data access frequency
Procurement portal	Procurement order	PURCHASEORDERVARIANT	Database Queries	Unlimited
	Supplier product prices	ITEM		
	Procurement invoice	PURCHASEINVOICE		
Warehouse management	Goods receipt	PURCHASEINCOMINGITEM		
	Product stock	ITEMSIZESTOCK		
Sales order management	Sales order	SALESORDER		
Bank system	Bank transaction	Unknown	API	
	Bank transaction approval			
	Creditor data	SUPPLIERDATA		

Creditor system	Creditor data change authorization log	SUPPLIERDATA	Database Queries	
Personnel management	Employee file	EMPLOYEE		
	Mutation log	EMPLOYEE		
User directory	User account	AD Database	Powershell scripts	Unlimited
	User authentication policy			
	Authentication settings			
	User account rights			
Support system	Release notes	Unknown	Automated CSV Export	Daily
	Support ticket			
Target system	Application log	DATABASEVERSION	Database Queries	Unlimited
	Application metadata	DATABASEVERSION		