Deloitte Enterprise Risk Services

Investigating the application of process mining for auditing purposes

Date: August 16th, 2007

Status: Final

I.E.A. Segers
isegers@deloitte.nl
Student-#: 502485

TU/e

Eindhoven University of Technology
Faculty of Technology Management
Department of Industrial Engineering and Management Science

Dr. J.B.M. Goossenaerts	Assistant Professor, Dept. of Information Systems
Dr. A.J.M.M. Weijters	Associate Professor, Dept. of Information Systems

Deloitte.

Deloitte Enterprise Risk Services

Drs. E. Stoelhorst	Senior Consultant, Deloitte Enterprise Risk Services
W.L. Ypma RE CISA MBA	Director, Deloitte Enterprise Risk Services

“The world is moving so fast these days that the man who says it can't be done is generally interrupted by someone doing it.”

- H.E. Fosdick

Preface

Almost seven years ago, I decided to leave a shiny Curacao in order to pursue a higher education in the promised land of the Antillean native: "Nederland". I remember arriving at Schiphol airport with a bag of worn clothes and a shabby old winter jacket inherited from my dad. The man selling me a train ticket was a born grumbler and in the meanwhile, some sad sneakup managed to snatch my jacket from the baggage trolley, leaving me wondering what he possibly could want to do with such a wasted piece of imported cloth.

That day was seven years ago. For me, it proved to be the prelude to a great time of studying Industrial Engineering at the University of Technology in Eindhoven. I will skip ahead as my life is now approaching the "burger"-phase of human existence. For the conclusion of the student-life part, I had the honour to conduct a research with a great employer called Deloitte ERS.

Deloitte ERS is a wonderful place to work, developing all those involved in sharp business-aware participants. This would make you believe that no room exists for creative and innovative ideas. Not true. At ERS, people support each other to inspire new ideas. That is why I have come to believe that Deloitte is working on the cutting edge of science and business. No wonder so many Deloitte employees hold chairs at universities around the country and even more provide guest lectures.

I want to thank Deloitte for the opportunity that was given me to start as a consultant. After some really hard thinking, I finally made my decision to take on a new challenge as a trainee with Van Oord Dredging. But I will always cherish the time I experienced at Deloitte and recommend Deloitte as the prime employer of choice to those who are most close to me.

Acknowledgments

Here I want to use the opportunity to thank all the people that aided me in my research.

I especially would like to thank my Deloitte coaches Ernst Stoelhorst and Willem Ypma. Ernst, a man with very winning manners provided amiable guidance I could count on time and again. Even on the most awkward moments that I managed to barge in, Ernst freed up his agenda and sat down with me. Guiding the X-monitoring team, a group of people from all disciplines of ERS, Willem has been responsible for a lot of ERS inventions and tooling. As if that wasn't enough, he is currently busy involving the audit practice for even wider applicable tooling and stimulating that ERS and the core audit practice really understand each others work. Aside from that, Willem is a language purist avant-la-lettre. Just meet him, and you'll know.

Thanks to Richard Hoekman for setting up and getting me started in the SAP R/3 IDES environment. Michael ten Broeke, Michael van der Meulen and Paul Weel who shed light in the SAP wilderness. Knowledge management experts and Google-black-belts Adam Çetindag and Kenneth Vos for being relieving oracles whenever the end of the information tunnel just didn't

come in sight. Jon Ingvaldsen of the university of Trondheim and Gamal Kassem of the university of Magdeburg for sharing with me their process mining insights.

Special thanks go to Marc Verdonk. A man with clear process mining thought leadership, ready to boldly engage all the research groups who ever dared to claim that process mining in SAP is intractable to impossible. I have had the opportunity to join one of his projects and seeing him at work made my decision of not accepting Deloitte's job offer extremely hard. I am sure that he will be the one who not only solves the technical difficulties of process mining in ERP solutions but also bring it to commercial use, giving Deloitte a huge competitive advantage over the other 'big three'.

My fellow interns, Niels, Lawrence, Frank, Robin. I saw them all start as consultants, making me the "senior stagiair" within two months after my own start. Them and of course Danny and Lars, who were always drawing those lucky rivers on our regular poker nights. My parents, family, friends, and the special class of friends called 'dispuutsgenoten' for their ongoing interest in my project. And of course all the people I forgot to mention by name here.

Finally, I want to thank my university coaches Jan Goossenaerts and Ton Weijters. Jan for always reminding me of the academic relevance of a research project and stimulating me to take into account the wider implications of doing research. my co-reader Ton for his enthusiasm, investing his precious time and effort into a new approach of process mining in the audit practice.

Last but not least, I want to thank Femke for her ongoing love and (partly long distance) support. She helped me through some really tough decisions, both for her and for me.

Igor Segers

Eindhoven, August 16th 2007

Abstract

This thesis researches the applicability of process mining in the audit approach. Using a model-driven approach, it develops a model for using process mining in a general business cycle, a requirements model for applying process mining for testing application controls in the expenditure cycle and a model for applying process mining in the SAP R/3 environment in the purchasing cycle.

Keywords: corporate governance, internal control, continuous assurance, process mining, ProM, LTL-checker

Executive Summary

Context

Over the past few years, a wave of accounting failures induced new regulations such as the Sarbanes-Oxley (SOX) legislation. Continuous assurance is regarded as the product of ongoing initiatives such as SOX, creating the incentive for Deloitte to research new approaches towards reaching this form of assurance. Process mining has been proposed as a promising new concept for improving the auditing function in two ways. First, by helping the auditor in understanding the entity in identifying the real processes going on at the client by extracting a real process model, second by testing control objectives using historical data in order to gain assurance. Until now, process mining has been of limited use in ERP systems because of the lack of understanding and an appropriate technique able to extract and analyze trace event log data from ERP systems. A gap between the theoretical approach of process mining and the benefits of practical application in real situations exists which needs to be solved. The latter is the subject of research. Before continuous testing of control objectives is possible, first must be identified how process mining can be applied in the auditing process.

Project Definition

The project has been identified as follows:

> Develop a model describing the application of process model extraction and control objective testing using process mining in a general business cycle. Elaborate on the requirements of these applications using the expenditure cycle and application in the SAP R/3 environment.

A process model is defined as a visual representation displaying the execution of relevant tasks in the business process, providing information on order of execution, timing and resources associated. Applying process mining in ERP systems certainly is feasible, although some restrictions will have to be removed. This is the direct result of the fact that ERP packages are functionally designed, not directly supporting mining initiatives. Using the tables available in an ERP package it is possible to extract a dataset which can be mined. Because of the above-mentioned restrictions, using this dataset to extract a process model is rather hard, but possible. The more interesting application is to build linear temporal logic routines (LTL routines) in order to check predefined control objectives on a dataset. Linear Temporal Logic is a formal language used tot test conditions taking into account the time aspect. This application has two advantages over the eQsmart tool currently used. The first advantage of the proposed method is that historical data is used instead of current state settings. This prevents a user from changing the settings in between eQsmart checks. The second advantage is that control objectives can be enforced at the process instance level instead of the transaction level, creating flexibility in allocating work to employees.

A framework identifying the requirements of process mining and control objective testing in ERP systems has been developed. A dataset extracted from the SAP expenditure cycle has been mined and analyzed as a verification of the methods proposed.

Conclusions and recommendations

Conclusions on feasibility of testing control objectives

The testing of control objectives has been proven feasible. The most interesting class of control objectives is the class of segregation of duties (SOD) control objectives. When the control objective is specified, the dataset can be used to test these objectives and conclude if conflicting behaviour has occurred. Because a thorough knowledge of the data structure of an ERP application is needed, the application for SOD control testing on an ad-hoc basis, developing control objective test routines within the scope of an audit, is not very attractive. On the other hand, the data structure of an ERP application is rather static. If an adapter is built that specifies which data from which tables is needed and directly runs a LTL check using specified LTL control objectives, the application becomes interesting. An additional advantage is that the auditor just needs to make a data download and doesn't have to change data or settings at the client, which is an important requirement in an auditing environment.

Conclusions on feasibility of executing process mining

The technical feasibility of process mining in an ERP package has been proven as well but is less interesting for a straightforward approach. Problems with convergence and divergence exist, making the definition of a process instance very laborious. Furthermore, process mining in an ERP package does require a thorough knowledge of the data structure of the ERP package, which renders the application of process mining less interesting. It can be a handy tool to quickly inspect a specific cycle. A process model using heuristics miner can be generated and visual inspection can aid the auditor in identifying defecting behaviour.

Conclusions on feasibility in the SAP R/3 environment

In our research, we conducted a process mining project manually to experience which problems arise. In SAP, extraction and conversion of a dataset in a narrow scope has been executed and proven feasible. However, setting up an extraction and conversion mechanism in order to create an event log has been proven to be very dependent on the data structure. In order to test SOD control objectives, per specific cycle a clear data extraction and conversion script must be made before easy testing of control objectives is feasible. Automating this approach renders the method feasible for use in IT auditing. The drawback of the approach is that the assumption is made that the data extracted is complete and correct. This drawback is recovered by the fact that the approach is intended to contribute to the level of assurance based on the evidence received.

The last recommendation is to develop a ProM adapter import plug-in for the ACL package. ACL can work with extremely large exports of database records, making the testing of control objectives over a larger time frame more feasible.

Table of contents

List of figures

1 About this study

This report discusses a master thesis research conducted at Deloitte Enterprise Risk Services, shortly Deloitte ERS. First the context of the research will be described. Then the research objective will be proposed. In order to reach this objective, several research questions have been formulated. These research questions are answered using a research method.

1.1 Context

Organizations are exposed to errors, frauds, or inefficiencies that can lead to financial loss and increased levels of risk. In order to ensure that risk is properly being mitigated, the pressures of regulatory requirements and the need to improve business operations are pushing organizations to report the effective working of controls on a timely basis. (Near) real-time reporting is likely to necessitate continuous auditing to provide continuous assurance about the reliability of the information presented. The audit process has evolved from a conventional manual audit to computer-based auditing, and is now confronted with creating continuous electronic audits (Institute of Internal Auditors, 2005). IT vendors have started developing tools which assist clients in achieving compliance. Although several software solutions are in the market which are able to assess and control certain specific business cycles or legislative regulations such as the Sarbanes-Oxley Act, an integrated solution providing continuous assurance is something which is currently a hot topic amongst assurance vendors. To give a colourful example: according to Rasmussen (Rasmussen, 2007), in the United States more than 114.000 regulations have been introduced since the government started collecting the metric in 1981. Rapidly emerging information technology and regulator's demands for more timely communication of information to business stakeholders require auditors to invent new ways to continuously monitor, gather, and analyse audit evidence in order to keep their competitive advantage. As we speak, several continuous assurance tools are in use within Deloitte ERS, even as some data extracting tools for several ERP packages. The real challenge lies in integrating and automating these functionalities, reducing auditor dedicated time and opening the way to frequent testing and reporting of controls. Whether or not Deloitte ERS should invest in the development of a continuous assurance tool is dependent on factors such as the development of the continuous assurance solutions by other parties and the availability of expertise to develop solutions in-house. Deloitte ERS therefore is looking for a clear overview and evaluation of available tools and solutions in order to develop a strategy for the near future.

1.2 Definition and scoping

During the research, we used the following initial research objective:

> Investigate the CAT[1] capabilities of the major tooling currently available in the compliance software market. Discuss a case in which you suggest an approach for improving a selected tool in combination with an ERP solution in order to contribute to the integration of continuous assurance solutions

We will restrict our attention to automated process level controls and automated general IT controls. This decision is logical, because testing of these controls can be done with little to no human intervention and should thus benefit the most of the efficiency increase. A shortlist with an evaluation of the reviewed CAT supporting tools will be developed. Furthermore, a lot of knowledge on SAP and Oracle systems is available in-house. One of these ERP packages will be reviewed as a case for the application of a selected tool.

1.3 Relevance

Many tools are in the market that deliver auditing functionality on a specific area. These are not always continuous and most of the time they only cover a small part of the area that needs auditing attention. The state of continuous assurance yields many advantages, such as compliance, cost reduction, decreased auditing cycle time and the leveraging of the internal auditor's time to focus on other areas (Head, 2005). Developing a classification of tools helps speeding up the selection and implementation process of the most suitable solution(s) in aiding management in continuous monitoring. The decision to use a bottom-up approach of researching the application of a specific tool in a specific environment is done to ensure enough depth of the research.

1.4 Approach

The approach discusses the research questions, the research methodology and the structure of the thesis.

1.4.1 Research questions

The research questions in the analysis phase are the result of the research objective:

1) What is continuous assurance and continuous monitoring?
2) What is auditing, how is this performed in theory and in practice?
3) What are CATs (process mining, data analysis and automated testing)?
4) Which CATs supporting tools are currently available externally?
5) How can tool performance be measured and how are these tools performing?
6) Based on a case, how can the application of a specific CAT supporting tool be improved?

[1] CAT stands for Continuous Assurance Technique

In the analysis phase, some additional research questions for the design phase arose:

7) What is the feasibility of testing control objectives using process mining?

8) What is the feasibility of executing process mining in the audit approach?

9) What is the feasibility in the SAP R/3 environment?

These questions will be addressed in chapter 5 and following.

1.4.2 Research methodology

For the research methodology, we follow the regulative cycle by Van Strien for the auditing work system. The regulative cycle is the practical counterpart of the empirical cycle and contains five phases: problem formulation, diagnosis, plan, intervention and evaluation.

Two ways of gathering information are used. These are the use of **internal information** and **external information**. Internal documentation comprises internal reports concerning compliance software, expert interviews, specialised websites on the Deloitte intranet and Deloitte databases. External documentation considers websites on the internet related to compliance software, whitepapers by tool developing companies, library literature and third party research. Questions 1, 2, 3 and 4 will be answered by doing desk research. Expert interviews are used to gather information about question 5 and 6. Model driven development is used to answer research questions 7, 8 and 9. Appendix I provides a schematic representation and an overview of the time schedule used in the research.

1.4.3 Structure of the thesis

In chapter 2, the report starts out by giving a short description of the principal of the research assignment, Deloitte ERS. Chapter 3 discusses the theory on risk management and internal control, legislation and the audit process. It also elaborates on the techniques which support continuous assurance. Chapter 4 details the compliance software market, developments and trends. This chapter also compares several software solutions in the field of continuous assurance. Chapter 5 then continues by providing the diagnosis, providing the final assignment and the project plan for the second part of the research: the design phase. Chapter 6, 7 and 8 discuss the design models. Chapter 9 discusses the limitation of applying the method in an ERP environment. Chapter 10 and 11 discuss the implementation issues based on a case and a plan to introduce the design to application. Chapter 12 wraps up the report, giving conclusions and recommendations for further research.

2 Deloitte description

Being a part of the orientation phase, we will provide a short description of the company where the research project was conducted. Deloitte in general is described in §2.1 and §2.1 and Deloitte ERS will be discussed in §2.3. The chapter will be concluded by discussing the market situation. For a detailed overview of Deloitte Touche Tohmatsu, its service lines and the disciplines which can be found within ERS, we refer to Appendix II: Additional information on the principal.

2.1 Deloitte Touche Tohmatsu

While Deloitte is known in the global marketplace by the brand name, "Deloitte," the legal entity name — Deloitte Touche Tohmatsu — owes its existence to three leaders in the accounting profession who, from the beginning of their professional careers, recognized the importance of a worldwide practice. When the term “Deloitte” is used, it refers to the member firm “Deloitte Netherlands,” when referring to the global firm the abbreviation of Deloitte Touche Tohmatsu, DTT will be used.

Obviously, the global firm name “Deloitte Touche Tohmatsu” is based on the names of the founders. It is however not until 1990, that the firm is named Deloitte & Touche through the merging of Touche Ross & Co and Deloitte, Haskins & Sells. Only just in 1993, the international name Deloitte Touche Tohmatsu was established. Deloitte Touche Tohmatsu is structured as a Swiss Verein, an association of member firms that are legally independent of one another but operate under related names. The DTT board of directors is the highest governing body. They determine the strategic direction of the organization. Together with internal administrative functions, such as human resources and technology, they comprise what is referred to as DTT. The Verein sets guidelines for the member firms and provides each member firm with exclusive privileges in its specific jurisdiction. DTT does not provide services to clients as a Verein.

2.2 Market Situation

DTT is one of the ‘big four’ accounting firms. The ‘big four’ are the four largest accounting firms in the world, together responsible for auditing nearly all the Fortune 500 companies. The other firms that make up the ‘big four’ are:

- PricewaterhouseCoopers,
- Ernst & Young
- KPMG International.

With a worldwide revenue of $18.3 billion in 2004/2005 DTT was the runner-up of the ‘big four’ worldwide measured by revenue. The competition is fierce among the ‘big four’ companies. In 2004/2005 Price Waterhouse Coopers was the biggest big four company.

2.3 Deloitte Netherlands

Deloitte Netherlands is one of the largest member firms of DTT. With revenues just short of €800 million and around 6500 employees in 2004/2005, Deloitte is the biggest professional-, financial services firm in the Netherlands. This has been the result of several mergers and acquisitions that have contributed significantly to the growth of Deloitte. Deloitte originated from the "Nederlandse Accountants Maatschap" (NAM), which was established in 1955. The firm grew quickly in the 60s and 70s and changed its name to "TRN (Touche Ross Netherlands) Group" in the mid 80s to emphasize its cooperation with Touche Ross & Co. In 1988, the TRN Group merges with the Tombe/Melse Group. In 1992, the name is changed to Deloitte & Touche as a result of the international merger between Touche Ross & Co and Deloitte Haskins & Sells creating DTT. In 1998, Deloitte merges with the VB Groep, an accounting firm focused on governmental and non-profit organizations. Andersen Netherlands, member of former accounting firm Arthur Andersen, joins Deloitte in 2002 as a result of the Enron scandal. As of 1993 Deloitte & Touche was the official name of the organizations. Yet, in the fall of 2003 Deloitte & Touche chose to carry out its activities under the name "Deloitte". Deloitte's strength lays in its experience (over a century) in tax, accounting and consulting. The firm's untarnished reputation – particularly compared to its competitors – used to be a strength until the Ahold scandal of 2003. Although Deloitte got no blame so far, it put an end to the unblemished reputation. Nevertheless, Deloitte is restoring this image, and with results. It was recently ranked the best accounting firm in the Netherlands in the "Management Team 500"; a survey among many Dutch executives about their opinion on professional services firms. Deloitte scored first place in the accounting branch, leaving competitor firms far behind. One of Deloitte's weaknesses used to be its representation in the corporate market. Due to the nature of the company and some of the mergers, Deloitte was market leader in the non-profit and medium & small enterprises sector but stayed behind in the corporate market compared to its competitors. With the acquisition of Andersen Netherlands (Andersen being well represented in the corporate market) this was largely solved though. Currently Deloitte is well represented in the corporate market worldwide with global audit clients like e.g. Microsoft, General Motors, Merrill Lynch, Ahold, Carrefour, Dow Chemicals, Proctor & Gamble and many more in the audit as well as non-audit service lines, obviously keeping them separate to ensure auditor independence.

2.4 DTT Service Lines

DTT recognizes four service lines: audit, tax, consulting, and financial advisory. DTT's focus in 2003/2004 has been to restore its image as an accountant. All accounting firms have been criticized in the aftermath of the Enron debacle. Critique focused on integrity and independence of the accounting firms. Accounting firms were said to have lost their independence as a consequence of their consulting activities. Consulting activities not only performed by their consulting branch, but also within the audit activity itself. Auditing something, which has been established as a result of your own consulting activities, compromises the integrity and independence. Some advice resulting from audit or assurance activities is tolerated; however, official consulting projects for audit clients are inadmissible. Consequently, regulations were introduced that enforced a strict separation of consulting and audit activities. Hence, three of the 'Big Four', Ernst & Young, KPMG and PricewaterhouseCoopers, sold their IT, management and organization consulting activities, although they kept their tax and financial advisory services. Nevertheless, Deloitte chose to keep its consulting branch and comply with regulations to carry out its vision of being a full-service accounting firm. Still, more than half of DTT's revenues are earned with the audit activity and DTT will therefore probably always be regarded as an accounting firm by most.

2.5 Enterprise Risk Services

ERS is officially part of DTT's audit activities. ERS focuses on the risk management of the organization, information and communication technology, secure e-business, the integrity of IT infrastructures and the security of information systems such as SAP, PeopleSoft, Baan, Oracle, J.D. Edwards, and Siebel. Not surprisingly, ERS employs many IT- and operational auditors and management accountants. Using Deloitte INVision, ERS can integrate service provision with business processes via the Internet. DTT's vision is to lead the global firm, all member firms combined, in delivering a completely new level of client service excellence that clearly distinguishes Deloitte from all other firms. In order to realize that vision, DTT strives to connect competencies and industries to drive their strategies around the globe. Because ERS is geographically split up in a lot of locations, sound knowledge management is enforced to prevent among others double development of solutions.

2.6 Stakeholders of continuous assurance

Continuous assurance is the concept that reasonable assurance can be provided on the adequacy and effectiveness of controls. In order to reach this assurance, several stakeholders exist and as we will be discussing in this thesis, an array of techniques of tools and techniques are in place to assist these stakeholders. Here we will discuss the stakeholders involved with continuous assurance.

The **government** is the institution that provides at several levels the directives for continuous assurance in the form of developing and enforcing legislation. The interests of the government many. The most basic are to protect company shareholders and preventing unfair competition amongst companies. Another interest is to prevent large scale scandals, which can lead to loss of shareholder trust and eventually loss of confidence in capital markets.

Management has the interest of maintaining compliance in order to conform to regulators demands. Furthermore, corporate governance, which will be discussed further on, is an important driver for continuous assurance. Since management is responsible for its own business processes and financial reporting, assurance can be leveraged by installing continuous monitoring processes using continuous assurance techniques.

Assurance tools are used by the **auditor** to test the hypothesis that the client object under review is in control. In this sense, the auditor has stakes with continuous assurance and its involved techniques, because assurance is basically the product that is sold by the accountant. Improving upon the field of continuous assurance techniques will improve the audit process of the (Deloitte ERS) auditor.

2.7 Summary

Continuous assurance is of great impact on Deloitte's audit service line and especially Deloitte ERS. Deloitte ERS is faced with the challenge to help clients achieve continuous assurance on financial reporting risks. For Deloitte ERS this will affect several competency groups. Continuous assurance focuses mainly on competency groups like the security services group and control assurance. Risk consulting / internal audit are especially active in the first parts of continuous assurance. Competency groups like Web services and the group Data Quality and Integrity are not primarily involved for achieving continuous assurance. For Deloitte ERS the challenge is to combine the knowledge from the different competencies and to provide an approach towards continuous assurance for its clients. Therefore, Deloitte has to use its own knowledge and best practices. An orientation of relevant literature regarding the background of risk management, internal control and continuous assurance is presented in the next chapter.

3 Risk management and internal control

In order to achieve an understanding of continuous assurance, this chapter discusses the main concepts used in this study and how the internal audit is affected by continuous assurance. First we will elaborate on risk management and then we will continue discussing internal control. Finally we will deal with the auditing theory and in practice at Deloitte.

3.1 Risk management

A **risk** is the combination of the probability of an event and the impact in case that event occurs. A **control** is a devise put in place to ensure that according risks are properly mitigated (Demneri, 2005). Identification of control deficiencies on the other hand highlights areas of potential risk. (Institute of Internal Auditors, 2005). Deloitte defines Enterprise Risk Management (ERM) as follows: "A structured, documented way of dealing with risks across the company, from implicit to explicit." (Amato & Eysink, 2005). In order to achieve this, Deloitte uses a five-step approach. This approach can be found in Appendix IV: The Deloitte ERM approach.

3.2 Corporate Governance

Before we discuss internal control, we will clarify the notion of corporate governance. Many definitions of the concept exist and no specific one can viewed as the correct one because opinions and views continue to differ. We will use the definition by the Committee on the Financial Aspects of Corporate Governance:

> **Corporate governance** can be understood as the system by which companies are directed, administered or controlled. At the centre of the system is the board of directors whose actions are subject to law, regulations and the shareholders in general meeting. The shareholders in turn are responsible for appointing the directors and the auditors and it is to them that the board reports on its stewardship at the Annual General Meeting. (Committee on the Financial Aspects of Corporate Governance, 1992)

Deckers and van Kollenburg provide a clear explanation of why Corporate Governance is necessary (Deckers & van Kollenburg, 2002):

Each company has plans and goals. As the size of these plans and goals increases, more individuals get involved in the realization of the plans and delegation will take place. When delegation is occurring, the need for control arises both with the delegate and the delegated person. The delegate wants assurance on the correct execution of the delegated tasks, the delegated person wishes to give account of his delegated tasks and the use of the corresponding authorities. This process implies the need for reciprocal communication. As the delegation of duties increases, for example to a company with shareholders being the delegate and the board of directors having the delegated role, the control will become more indirect and the information will play a central role. As this role gets more important during the control of activities, the need for a guarantee that the information is reliable also increases. This because the chance of errors in the information also increases. Furthermore, the separation of ownership from control implies a loss of effective control by shareholders over managerial decisions. A system of corporate governance controls is implemented to align the incentives of managers with the objectives of shareholders in order to limit the self-satisfying opportunities for managers (Eisenhardt, 1989). Thus a need for control on the reliability and adequacy of the information arises.

This clearly describes the essence of internal control, which we will discuss in the next section.

3.3 Internal control and assurance

Corporate governance mechanisms and controls are designed to reduce the inefficiencies that arise from moral hazard and adverse selection (Becht *et al.*, 2003). The Committee of Sponsoring Organizations (COSO) of the Treadway Commission (Committee on the Financial Aspects of Corporate Governance, 1992) provide the following definition of **internal control** as:

A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

The notion of assurance is first used in this definition, requiring a definition here. Providing **assurance** in general can be seen as an impartial and independent opinion to a third party regarding the state of affairs, about a specific transaction business or governance process, risk, or overall financial performance of a business operation. **Audit assurance** is a statement regarding the adequacy and effectiveness of controls and the integrity of information. **Reasonable assurance** implies a high degree of certainty, but not absolute certainty. Before an accountant can give a positive advise, he must be reasonably sure that the internal control system is functioning well. When a **deficiency** is detected, the accountant must perform substantive testing in order to achieve reasonable assurance before he can give a positive opinion regarding the state of affairs. The US Statement on Auditing Standard No. 60 – Communication of Internal Control Related Matters Noted in an Audit (SAS 60) defines two levels of deficiencies:

A **significant deficiency**: this is defined as an internal control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process or report financial data reliably in accordance with generally accepted accounting principles, such that there is more than a remote likelihood that a misstatement of the entity's annual or interim financial statements that is more than inconsequential will not be prevented or detected.

A **material weakness**; this is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected.

A significant deficiency can, but does not have to, lead to a material weakness. In order to prevent material weaknesses, it is obvious that significant deficiencies should be detected in an early stage.

As said, a control is a devise put in place to ensure risks are properly mitigated. Controls can be classified in a few ways.

First of all, controls can be defined at several levels. At the **company-level** or **entity-level**, certain policies and procedures must be reviewed. At the **process-level**, controls exist such as to ensure specific steps in the process under review. For example, in the purchasing process, accounts payable amounts should be correctly calculated and recorded. Finally, **general computer controls (GCC)** are controls that are embedded in the IT infrastructure that is present. An example is strong password enforcement by operating system software.

Another split can be made between **preventive** and **detective** controls. Preventive controls are usually more robust, because they "prevent" the error from being made. The password example given above is a preventive control. Another example is segregation of duties enforcement in certain ERP packages. Unfortunately, preventive controls are generally also more expensive to implement.

The last classification we will discuss here is the nature of the control. This can either be manual, IT dependent or automated. A **manual** control is a control that is enforced by humans. Most company level controls (such as procedures and policies) rely on human review in order to be of effect. **IT dependent** controls are the typical controls that need an analysis of a dataset. **Automated** controls are those controls that need no human intervention to be of effect. Preventive GCC controls are an example, but also more and more automated detective process controls are falling under this category (more on this topic in § 3.4.2).

Internal control and corporate governance are closely related. The difference is that corporate governance delivers an abstract notion of how an organization should be directed and internal control provides an explicit and structured approach to implementing control mechanisms. Internal control frameworks describe guidelines and rules for implementing an effective internal controls mechanism and evaluating existing ones.

To conclude, one has to be aware that an important statement in the definition of internal control is that internal control is a process, not a one-time effort. This means that adequate internal control will not be established by implementing a system only once and then relying on that system for the remainder of the time.

3.4 Continuous assurance

In this paragraph we will discuss some important concepts in the auditing practice.

3.4.1 What is continuous assurance?

To achieve continuous assurance it is necessary to provide a definition. The following definition will be applied for continuous assurance:

> **Continuous assurance** means that at certain successive points in time the organization has to be able to provide reasonable assurance about the adequacy and effectiveness of controls and the integrity of information (Institute of Internal Auditors, 2005).

This definition is based on the jointly written report by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certifies Public Accountants (AICPA). Now that the definition is set, it is necessary to establish how continuous assurance can be achieved. There are different conceptual models that discuss the subject of continuous assurance. Continuous assurance as depicted in Figure 1 can be achieved through continuous monitoring and continuous auditing. These two are the main building blocks of continuous assurance. As we will see in the next two sections, the product of continuous monitoring and continuous auditing is very much alike. The key difference is that continuous monitoring process is owned by the management, as part of its responsibility to implement and maintain effective control mechanisms.

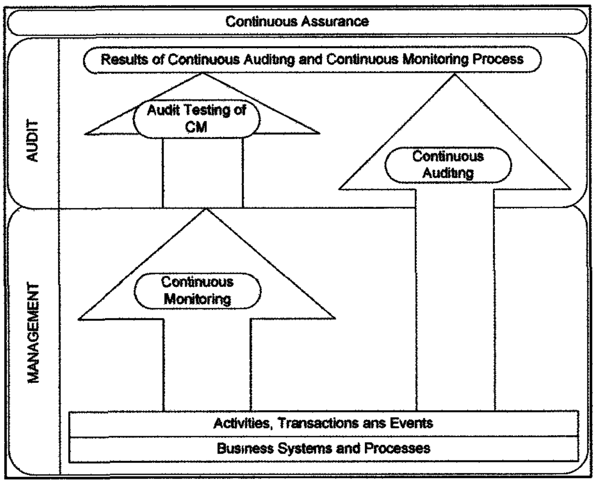

Continuous Assurance
Results of Continuous Auditing and Continuous Monitoring Process
AUDIT
Audit Testing of CM
Continuous Auditing
MANAGEMENT
Continuous Monitoring
Activities, Transactions ans Events
Business Systems and Processes

Figure 1: Conceptual Model Continuous Assurance (IIA, 2005)

3.4.2 What is continuous monitoring?

According to (Institute of Internal Auditors, 2005):

Continuous monitoring is the process that management puts in place to ensure that its policies, procedures and business processes are operating effectively through the course of time.

Management identifies critical control points and implements automated tests to determine if these controls are working properly. The continuous monitoring process typically involves the automated testing of all transactions and system activities, within a given business area, against a suite of control rules. The monitoring is typically put in place on a daily, weekly or monthly basis, depending on the nature of the underlying business cycle.

3.4.3 What is continuous auditing?

Continuous auditing is a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors' reports issued simultaneously with or a short period after the occurrence of events underlying the subject matter (Sarva, 2006).

An inverse relationship between the adequacy of management's monitoring and risk management activities and the extent to which internal auditors must perform detailed testing of controls and assessments of risk exists. If the effort put into continuous monitoring by management is limited, auditors should apply detailed continuous auditing testing methods. On the other hand, if management invests more effort in continuous monitoring, the internal audit activity does not need to perform the same detailed techniques that would otherwise be applied under continuous auditing. Auditors should then focus on procedures which determine if they can rely on the continuous monitoring process.

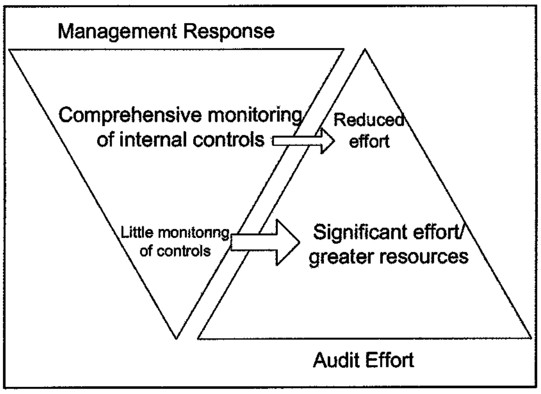

Management Response
Comprehensive monitoring of internal controls
Reduced effort
Little monitoring of controls
Significant effort/ greater resources
Audit Effort

Figure 2: The inverse relationship (IIA, 2005)

3.4.4 What are the benefits of continuous assurance?

According to (Head, 2005), continuous assurance has the following advantages:

- Validates continuous monitoring and risk assessment efforts: operational efficiency is enhanced and the bottom-results are improved because of cost savings and reduced revenue leakage and overpayments
- Identifies unknown or uncontrolled risks and monitors residual risks: the remark must be made that this advantage is not commonly present in current control frameworks, where risks are defined beforehand and controls are devised accordingly
- Resources are leveraged: less time is needed by internal auditors and management, this reduces costs (for management) and allow for a shift of attention to other important issues (internal audit)
- Timely meets regulatory monitoring needs, such as prescribed by the conformance legislation discussed in this chapter, while shortening the cycle time
- Promptly identifies "irregularities" and allows self reporting and proactive resolution: deviations are remarked a short time after they occur and don't have to wait for the next assessment, instances of error and fraud are severely reduced

3.4.5 What are CAATTs and CATs?

Computer Assisted Auditing Tools and Techniques (CAATTs) are techniques that assist an EDP-auditor in performing an audit. In our research, we will use a broader definition namely that these techniques not only support the auditor but also the manager in doing his work, including the continuous monitoring of processes, and the risk consultant in developing and implementing a general control framework for his clients. We will call them CATs, which means Continuous Assurance Techniques.

Continuous Assurance Techniques are the techniques used by the auditor and the manager in gaining assurance that the object under scrutiny is in control.

David Coderre, best known advocate of CAATTS, remarks that there is no purpose in having a technique without the tools, or the tools without the technique. The techniques are thus usually available in the form of a tool: an example is eQsmart, a Deloitte in-house developed tool specifically meant for gaining assurance by testing SAP configuration settings.

Within Deloitte, three classes of CATs have been defined. These are **process mining, data analysis** techniques and **automated testing**.

3.5 Continuous Assurance Techniques

In this chapter, we will discuss the abovementioned techniques and show how the application of these techniques is converging.

3.5.1 Process mining

New processes are emerging and existing processes are changing. The alignment of business processes and information systems requires continuous attention. It is important to detect deviations of the described or prescribed behaviour to maintain conformance. Process mining is a technique that has the prospects to evaluate and measure the performance of business processes. Process mining allows an IT auditor to extract information from event logs and collect data at runtime aiming at extracting unexpected and useful knowledge about the process. Process mining is based on pure facts. These facts can be runtime data, which means that there is no doubt possible about misperceptions, because it is based on factual data. Process mining could open a large variety of opportunities for the auditing of business processes because without or with limited prior knowledge about the structure of the process it is possible to infer a process model.

Process mining is the technique of distilling a structured process description from a set of real executions (event log) (van der Aalst, 2005;van Dongen *et al.*, 2004).

Also a definition of a process model is given:

A **process model** is defined as visual representation displaying the execution of relevant tasks in the business process, providing information on order of execution, timing and resources associated.

Process mining is based on Business process management (BPM):

Business process management is the field of knowledge at the intersection between Management and Information technology encompassing methods techniques and tools to design, enact, control and analyze operational business processes involving humans, organizations, applications, documents and other sources of information (van der Aalst *et al.*, 2003).

BPM itself is not system bounded, a BPM *system* however becomes system bounded. A BPM system can be process-aware, using a *structured*, a priori defined prescriptive process model. These are called workflow management systems (or WfM-systems), examples include Staffware and FLOWer. A BPM system can also be *unstructured* using no previously defined process model. An example of unstructured BPM systems are ERP packages such as SAP and Oracle (although also structured modules exist).

Process mining is closely related to BAM (Business Activity Monitoring), BOM (Business Operations Management), BPI (Business Process Intelligence), and data/workflow mining. Unlike classical data mining techniques the focus is on processes and questions that transcend the simple performance-related queries supported by tools such as Business Objects, Cognos BI, and Hyperion (www.processmining.org). Process mining is useful when diagnosing existing business processes, gathering information on all process executions and suggesting improvements for business process (re-)design.

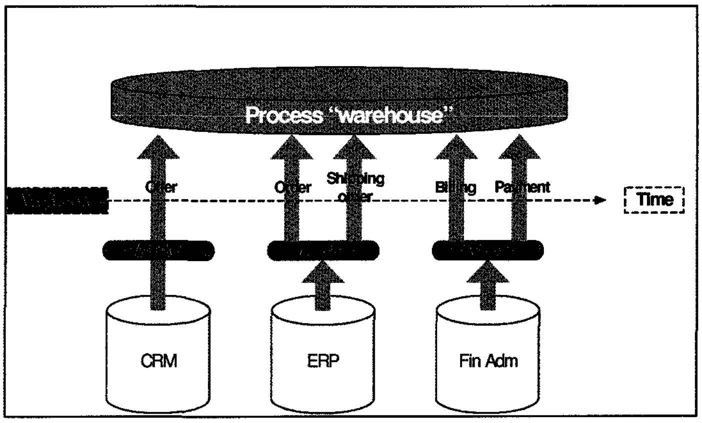


Figure 3: Process mining architecture

Process mining has three application areas (Figure 3):

- **Process discovery**: the audit trails of a workflow management system or the transaction logs of an enterprise resource planning system can be used to discover models describing processes, organizations, and products.
- **Delta analysis**: use process mining to detect deviations, comparing the observed events with predefined models. This application can be very useful for IT auditing in determining conformance.
- **Performance analysis**: in order to develop improvements to the business process.

Stated that process mining is the extraction of a process model using a set of real executions, how do we go about applying this technique? Figure 4 shows the simplified concept of process mining.

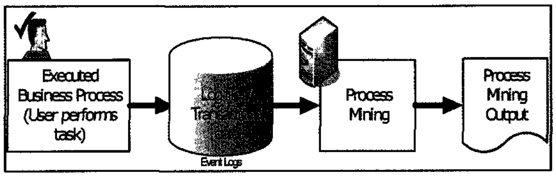


Figure 4: Process mining overview

A business process is a combination of several tasks from (different) users. An employee executes a specific task; information about this task is logged in the application. This log, called an event log, contains information about the execution of a process. The logs from the different tasks, which together form the complete business process, are gathered. The logs are adapted to a standard. Finally, via process mining algorithms the actual executed business process is determined. To find a process model on the basis of an event log, the log is analyzed for causal dependencies. The result of the process mining offers a wide variety of purposes. The available process mining algorithms are described in detail in (de Medeiros *et al.*, 2004) and (de Medeiros *et al.*, 2005). Before the logs from the different sources can be mined, they must be adapted to a generic format. The Mining-XML (M-XML) format is specifically developed for this purpose. Almost every system has its own way of logging the events, although the information logged during operation is quite similar. The M-XML format acts as an intermediate function between the source system and the process mining tools.

The minimum requirements for the process logs, and directly for process mining, are according to (van der Aalst & Weijters, 2004):

- Case ID - The Case ID indicates for which case (or process instance) the activities have been executed. Without the Case ID, we are not able to identify from executed logs whether new processes are started, or finished.
- Task ID - The Tasks ID indicates which activity has been executed. When a task is executed for a specific case, we refer to it as an activity. Tasks are "atomic" and cannot be partially executed.
- Tasks are ordered - The last requirement of process mining is that the tasks are ordered. In other words when an activity in the log appears before another activity in the log, it is known that the first activity was executed first.

In our research, we restrict the attention to ERP packages and leave CRM packages and Financial Administration packages out of scope. In order to be able to conduct process mining in an ERP package, three phases have to be undertaken. The preparation phase, the pattern discovery phase and the analysis phase. The latter two of these phases is generic, the first phase is dependent on the information system (ERP package or WfMS).

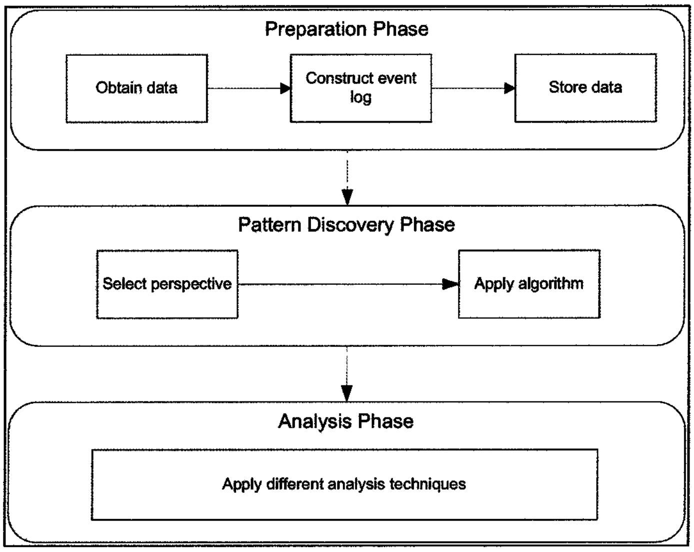


Figure 5: The phases of process mining

The preparation phase consists of the extraction of data from the source ERP system, converting this data to a usable event log in M-XML format and storing this data for later use. The pattern discovery phase entails the execution of the applicable algorithms, dependent on the selected perspective. The selected perspective in turn is dependent on the information that needs to be retrieved (for example, a process description or a social network). In the analysis phase several analyses can be executed to derive conclusions on the dataset. For example, using process discovery, models may be generated to explain the observed behaviour. Unfortunately, as we will see later on in the research, due to some strict requirements which the ERP logging is not conforming to, the process mining of models can be very difficult to intractable for many processes. However, for most processes one can formulate (un)expected/(un)desirable properties. (van Dongen *et al.*, 2004) These properties can be directly compared with the event log. Van der Aalst et al. proposed using the language called Linear Temporal Logic (LTL) to define certain properties and check these properties against an event log. Note, that in principle, no process model has to be mined to be able to do so. For example, for very complicated processes resulting in spaghetti-like diagrams it is easy to verify the 4-eyes principle using linear temporal logic. In Appendix VIII: LTL language applied to M-XML an overview is given of the LTL language definition.

In executing the first phase of process mining in ERP systems, the preparation phase, several problems arise:

- The trace mechanisms designed in ERP systems are not designed with the idea of supporting process mining, no standards on the structure of log and trace files on ERP systems exist
- ERP systems are traditionally designed from a data perspective, supporting the integration of data using relational databases (Kassem & Rautenstrauch, 2005)

Process mining has several advantages:

- The technique is based on pure facts
- Only basic knowledge of the underlying process is needed
- The whole process under scrutiny is assessed
- Conformance checking of the prescribed process model is possible

On the other hand, process mining has also some serious disadvantages that have to be overcome:

- The results of the analysis depend on profile input: event logs should be complete and available
- Logs should not contain too many tasks with no unique names
- Pre-processing of data is required, transforming the logs to the mineable M-XML format or a comparable alternative
- A process instance (Case ID) must be available (SAP R/3 logs for example do not have this ID readily available)

Concluding, we can say that process mining has several advantages but also some severe disadvantages that will have to be conquered before the technique can be put to auditing use. These disadvantages will be addresses in the rest of the research.

3.5.2 Automated testing

Traditionally, audits on samples of data were collected manually after financial year close, often very long after transactions had taken place. Although it took a lot of time to gather and assess all the documentation, this was offset by the fact that the audit was executed not very often and only by a few people. Nowadays, SOX has changed everything. Testing takes place during the whole year at all levels of an entity. The auditing of controls takes a lot of time and resources. It has been estimated that testing one control one time can cost up to $500. For a large organization with a thousand or more controls, very regular checking of controls can become quite a financial burden. For this reason, the audit of controls generally takes place on a multi-year rotation plan. Of course, advanced audit plans incorporate a differentiated approach, varying to the definition and auditing of some "key controls" versus standard controls, to a sliding scale of controls importance, where more important controls receive more attention than those which address risks with less likelihood and impact. The first step is to replace manual controls with automated ones. The reason is straightforward: automated controls are efficient, reliable and preventive. Furthermore, it provides a reduction in costs and an improvement in quality of the operational processes.

We will start out by setting a definition of automated testing:

Automated testing is the technique of reducing recurring manual compliance effort by replacing manual testing of automated controls with automated testing of controls.

Since the advent of controls monitoring, incentives have arisen regarding the automation of controls testing. By automation several advantages are achieved: internal auditor dedicated time is reduced, providing the resources to address other important issues. Furthermore: by continuous testing the cycle time of controls is greatly reduced which significantly improves the timeliness of detecting a failing control.

The advantages of automated testing are:

- Internal auditor dedicated time is significantly reduced, severely bringing down the associated costs
- The audit cycle can be reduced, serving timelier assurance to the stakeholders
- The client becomes aware of being the owner of monitoring role

On the other hand, the disadvantages of this technique are:

- The controls should be audited as well
- Not applicable to all types of controls (for example, entity level controls such as review of policies and procedures)
- Only applicable when processes, risks and applicable controls are well known

In Figure 6, a schematic representation of the automatic testing procedure is given. A GRC framework is a repository where all control objectives and procedures are stored.

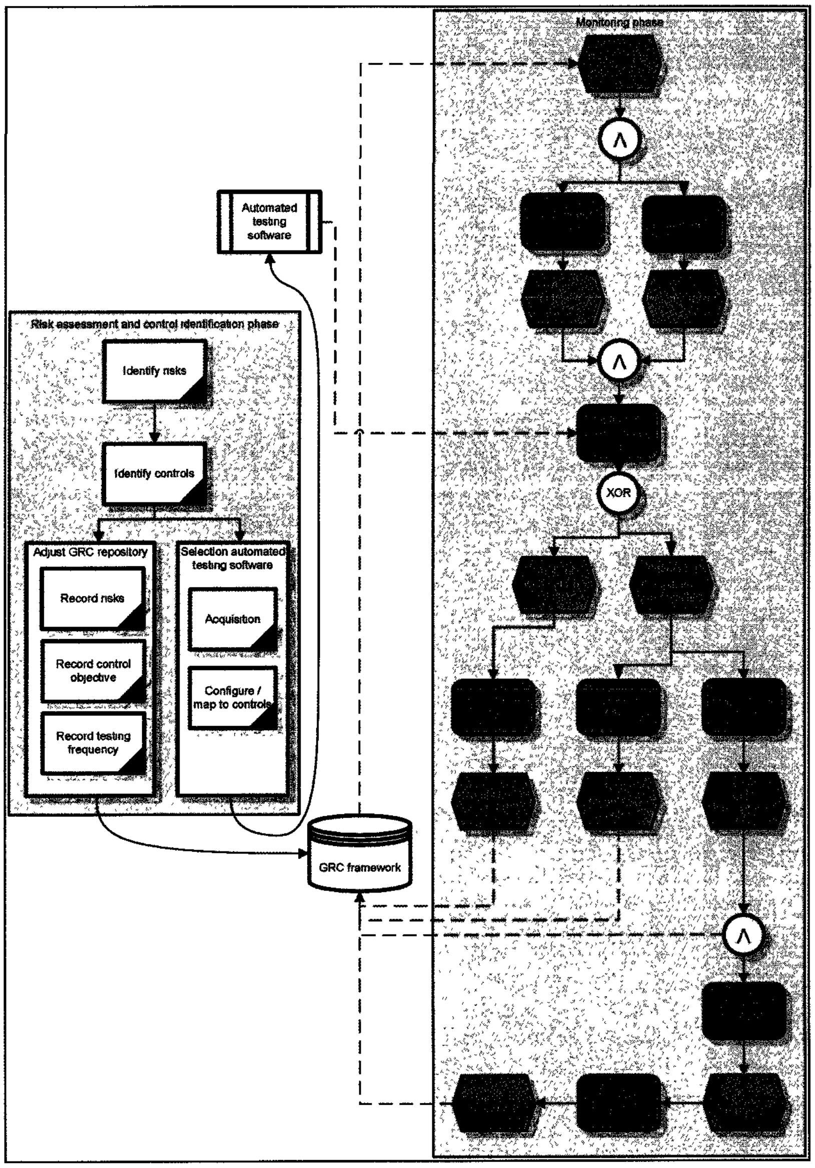


Figure 6: The automated testing process

3.5.3 Data analysis

The definition of data analysis is as follows:

Data analysis is the act of transforming data with the aim of extracting useful information and facilitating conclusions.

Data analysis has basically two application areas. The first application, called online analytical processing (OLAP) can be used to support a manager in making decisions, for example he would query the data warehouse for total amount of sales of a certain product group in a selected group of geographical areas over several time frames. He could then develop a trend forecast and allocate production to these regions for the coming month accordingly. Or more strategically, he could decide to stop serving a certain market. Otherwise, in auditing data analysis is usually executed in the form of a set of data being submitted to a series of queries in order to test a hypothesis. The example here is inspecting a table of employee salary payments and assuring that nobody got paid twice a month. In this case the query is clear and a conclusion can be drawn. If not, then further inspection will be necessary.

The advantages of data analysis are presented here:

- Great flexibility in devising the on-demand substantive test
- Supreme computer power allowing 100% testing deletes the need for sampling
- Most tools have no trouble importing data in a big array of formats
- Most tools provide a visual API for easy scripting

Data analysis is a great technique to use on an ad-hoc basic, piercing datasets with the right queries to give the auditor the assurance needed. Caution must be taken though in devising the right queries.

3.5.4 Relation of the techniques

It is clear that the three mentioned techniques cannot be discussed in isolation. Where data analysis and continuous testing converge, software tools emerge which use a predefined set of queries to test on a cyclical basis if the data still conforms. We will discuss a few of these tools in the next chapter. Data analysis and process mining also overlap, for example the two split decision in process models is often based on data attributes. Data analysis and process mining converge here to discover the unique data attribute that causes the decision on the two split and so help discover business rules. Finally, we expect that process mining which is used on a continuous basis can also be applied to assess and define KPI's. In the next chapter we will discuss a tool that already uses process mining to support management in decision making. For the sake of clarification we have decided to split up these three techniques and use this as a guidance in discussing the shortlist of software in the next chapter. In Figure 7 can be seen how the techniques are developing, becoming more and more continuous and along the way catching the interest of new stakeholders.

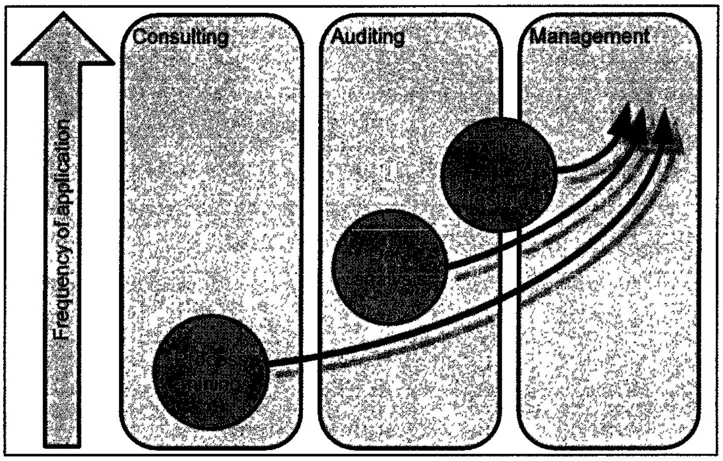


Figure 7: The development of the CATs

3.6 The audit process

Although the previous sections discussed internal control measures, it is not yet clear how these are tested. This paragraph discusses the audit methodology. The first subsection reviews the theory of the audit process. Then we will briefly discuss the ERS audit methodology.

3.6.1 Theory

In the preceding sections we discussed the need for internal control. Controls are put into place to mitigate risks. These controls have to be assessed for design, existence and operating effectiveness. This is the work of the EDP auditor. The definition of the tasks of the EDP auditor have been taken from the book "Inleiding EDP Auditing" (van Praat & Suerink, 1992), EDP auditing is defined as follows:

> EDP auditing is the discipline which concerns the analysis of an organizations information and computer systems in order to evaluate the integrity of its productions systems as well as potential security breaches. The goal is to improve and contribute to the adequate organization of the information provisioning.

Van Praat en Suerink distinguish the following phases:

- Assignment formulation
- Establishing the audit plan
- Executing the audit
- Formulating the judgment
- Reporting

The audit process begins with the assignment formulation. In the audit assignment the entity of research, the aspects which will be the object of the research and the standards that will be enforced are recorded. Then the audit plan is formulated:

> The audit plan is a systematic and structured definition of the activities which have to be executed in order to determine the existence and the operating effectiveness of control measures which are put into place to ensure the quality of the entity under research.

Proof to reach an assessment is gathered during the execution of the audit. Methods applied can vary from interviews (the most applied technique) or observation to internal and external proofs of evidence, such as documentation of third party installed software. All findings are registered in a record, which can be used to later substantiate the conclusions. Reporting contains the judgment of the auditor, based on the difference found between the standards used and the encountered situation.

3.6.2 Deloitte ERS practice

The Deloitte Audit Approach Manual details the Deloitte uses the in-house developed system called AS/2. AS/2 contains an audit approach, general documentation and software technology. AS/2 is also suitable for creating the dossiers needed to reach a substantiated conclusion. The audit process is visualized in Figure 8.

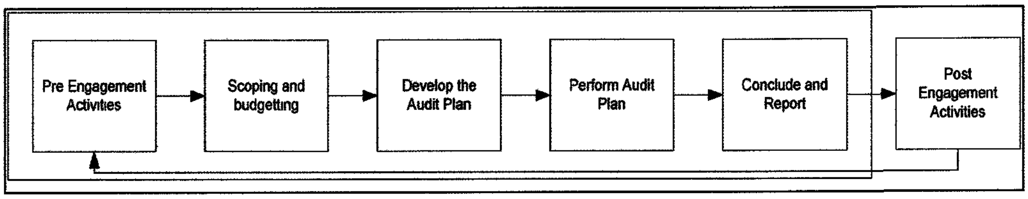


Figure 8: Deloitte ERS Audit Process

ERS executes two different types of assignments. These can be assignments that support the accountant in financial year closing (or so-called integrated audit-assignment) or individual assignments.

Based on the amount of dependency on IT of the entity being audited, the help of the EDP auditor is called in to support the accountant in his audit, called the integrated audit assignment. The classification of IT dependency can be either minimal, significant, or dominant, depending on the amount of manual controls, IT dependent controls and fully automated controls. In The Netherlands, the support of an EDP auditor is called upon when the classification is significant or dominant in the entity. The IT auditor participates from the beginning stages of the audit. The expertise of the IT auditor is needed to verify that control measures are correctly set up and working effectively in order to prove that the financial information generated by the system is reliable. The intake, with the EDP auditor and the accountant, the scoping and the budget is determined. The scoping contains an overview of the components of the IT infrastructure that have to be tested. A work program is formulated by the auditor. After conducting the audit, the EDP gives feedback to the accountant in the form of a report which concludes if the process can rely on the IT infrastructure. The accountant takes these conclusions in consideration. The IT auditor provides analyses for each audit assignment involved over several layers of IT. The auditor has to check all the layers, because control in one layer does not have to mean the entire entity is in control. For example, an application can be in control but if the underlying data can be modified outside the application, for example directly in the database used, the application controls would be useless. Therefore the IT auditor has to check all levels in order to attest the in-control statement regarding IT.

The **individual assignments** concerns the testing of a new system or application or the selection of a new software package. The ERS IT auditor will execute an audit to reach assurance about the object. During the intake, the level of assurance and the amount of budget the client is willing to allocate are determined. The client and the auditor define the scope of the research and then the auditor formulates a work program. The work program is submitted to the client. After acceptance, the auditor performs the audit and gives feedback to the client in the form of a report with results and recommendations.

3.7 Legislation

Over the years, many legislation was created to regulate corporate governance. These movements came into existence as far back is the 70s, when the Watergate Scandal shocked the world. This event led to the Foreign Corrupt Practices Act in 1977. This law was devised to prevent unlawful payments by the implementation of internal control mechanisms. In Figure 9 can be seen which events led to the attention given to internal control and corporate governance. Of these events, we will discuss the most impacting legislation here, the Sarbanes-Oxley Act.

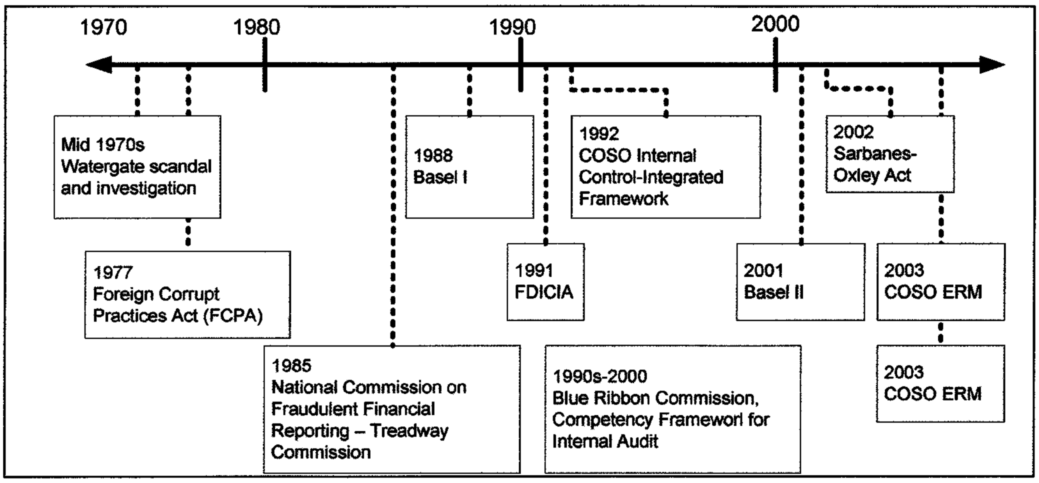

1970
1980
1990
2000
Mid 1970s Watergate scandal and investigation
1977 Foreign Corrupt Practices Act (FCPA)
1985 National Commission on Fraudulent Financial Reporting – Treadway Commission
1988 Basel I
1991 FDICIA
1992 COSO Internal Control-Integrated Framework
1990s-2000 Blue Ribbon Commission, Competency Frameworl for Internal Audit
2001 Basel II
2002 Sarbanes-Oxley Act
2003 COSO ERM
2003 COSO ERM

Figure 9: Timeline directives issues

3.7.1 The Sarbanes Oxley Act

A bulk of Deloitte ERS projects over the last years concerned the Sarbanes-Oxley legislation (SOX), with the Enron scandal being particularly responsible for the final push needed to pass the Sarbanes-Oxley law. The law is intended "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes" (Sarbanes-Oxley act of 2002). A non-profit, non-governmental and independent organization to oversee auditors of publicly traded companies was created. The board was selected by the SEC and so the Public Company Accounting Oversight Board (PCAOB) came into being. The SOX sections 302 and 404 have far reaching consequences for the financial reporting of big international companies and those companies were obliged to be "SOX-proof" by Januari 2007. We will discuss these two sections here in some detail.

Section 302 handles corporate responsibility. Certifying officers such as the CEO and CIO have to certify the accuracy of financial statements and the existence and the effective operation of disclosure controls and procedures in the periodic report. They must also certify that those statements accurately represent the financial condition and operations of the issuer. Furthermore, information used to create financial statements must be retained and made publicly available. This section makes internal control over financial reporting mandatory.

Section 404 requires management to report annually about the establishment and maintenance of adequate internal control over financial reporting. It requires an assessment of the controls and the identification of the framework used for the assessment. It concerns the processes that have been put in place to ensure the reliability of financial reporting.

The difference between the two sections is that section 302 obliges management to **establish an internal control system** and section 404 obliges to **enforce a systematic approach to the establishment of an internal control system** by identifying the framework used. Section 404 requires an explicit statement about whether the internal control system was actually effective.

This leads to a review of existing internal control systems and testing to see if these provide reasonable assurance. Management is forced to think thoroughly about risks and control before designing and implementing a control structure. Furthermore, new 404 audits are needed when material processes are changed, such as when implementing a new ERP package. In the first year, SOX required companies to report about the effective working of the internal control system on the day of the fiscal year end. Currently, the legislation forces companies to report about the effectiveness of the internal control systems throughout the entire year. SOX compliance and the auditing of the in control statement is an ongoing process which has to be managed effectively and efficiently, instead of a one-time effort. Requiring reporting on the effective working of the internal control systems, the Sarbanes-Oxley legislation can be seen as a driver for continuous assurance.

3.8 Summary

In this chapter, several relevant definitions have been put forward. Also three different CATs have been discussed, presenting the workings, the advantages and disadvantages of the several techniques. Concluding, we can say that each technique has several advantages but also some severe disadvantages. Furthermore, the techniques are not to be seen in isolation, but are of most practical use when applied in concordance. In the next chapter several tools will be discussed that apply these techniques.

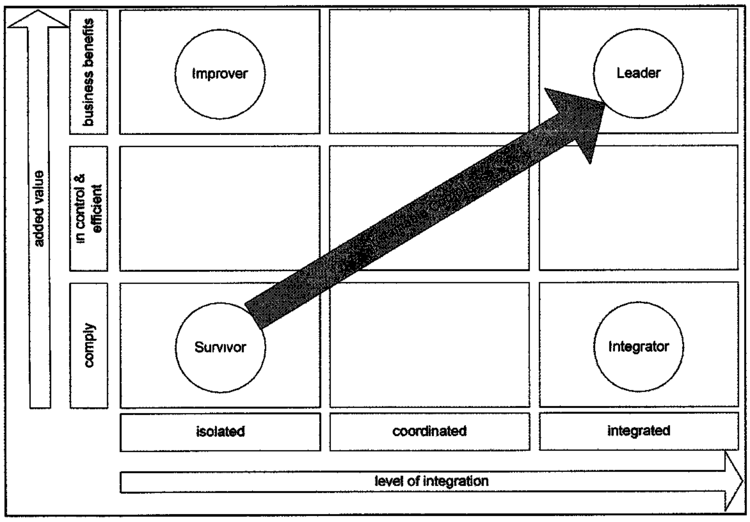
4 Market and tool analysis

In this chapter, we give an overview of the compliance market landscape. Here we will discuss what the trends are and what types of software vendors are operating in the market. Keep in mind that there is no clear way to divide the software market for enterprise and compliance software perfectly. Secondly, it is not our intention to review all the compliance software available on the market. But we think it is necessary to provide a context of the software market before we assume a specific focus. When comparing software, we decided to take the continuous assurance techniques approach, the CATs have already been described in the preceding chapter. Again, this is an approach, and many other attributes of the software under scrutiny could have been compared.

4.1 Developments in the market

After the initial wave of SOX-compliance software and implementation projects, the market is starting to mature. Two major trends are occurring along with this maturation. First, the integration of on the one side specific compliance software to suites that address compliance in general can be seen. The second trend is the leveraging of compliance software to actually improve business performance. These two trends are clearly shown in Figure 10.

Figure 10: Compliance strategies (adapted from van Brummelen et. al., 2006)



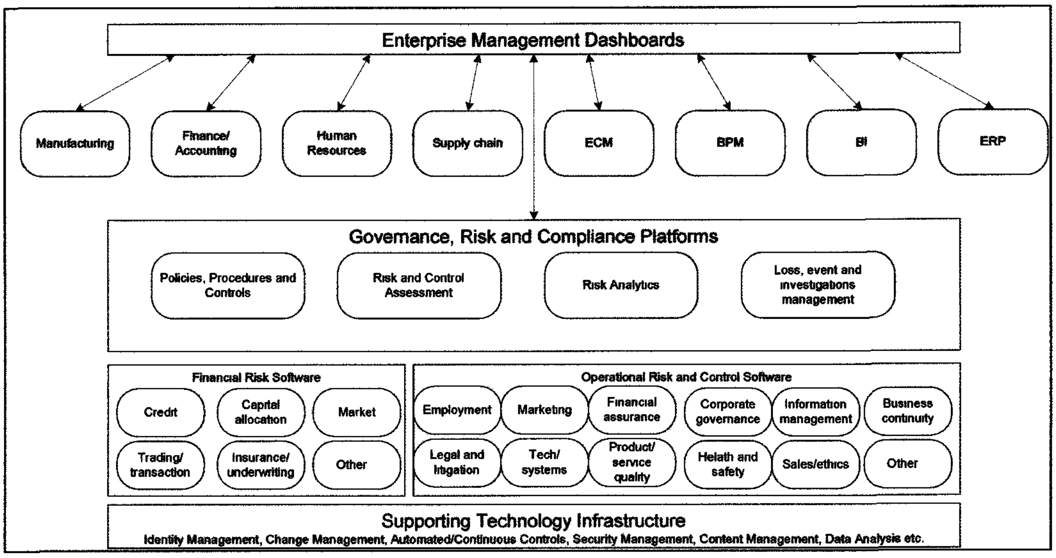
Currently, integration of different compliance domains is taking place. Formerly the compliance on a certain area was reached by executing a compliance program according to the regulations and organizational unit under study. This way of working is very inefficient because it creates a significant amount of duplicate work. This can more and more be supported by using tools that share the same process and organizational models, sharing controls where applicable and applying the same way of working. Most of the Sarbanes-Oxley compliance software offered by vendors relies heavily on the ERP package that is in use. The ERP vendors patiently waited to see which software vendors survived. Now that the contours amongst vendors are becoming clear, partnerships, mergers and acquisitions are occurring at a fast pace. The focus is moving from a siloed approach to integrated solutions labelled with names as Global Risk and Compliance suites.

For example, SAP recently bought Virsa, while Oracle took over Hyperion in March of this year. SAP announced the launch of a new integrated suite called SAP GRC, an initiative in partnership with DTT.

The second development is that companies start to realize that compliance is not only a nuisance, but is also an enabler for business improvement (van Brummelen *et al.*, 2006). Given the fact that a big investment has to be made to comply on all fronts, these major investment are more and more being used to leverage business process performance and improve while complying.

In Figure 11 a overview of the compliance market is given. This overview is adapted from (Rasmussen, 2007). Starting at the bottom, software gets more complex as it gets to the top. We will call this upward integration of software functionality.

Figure 11: The risk and compliance market landscape (Rasmussen, 2007)


Enterprise Management Dashboards
Manufacturing
Finance/ Accounting
Human Resources
Supply chain
ECM
BPM
BI
ERP
Governance, Risk and Compliance Platforms
Policies, Procedures and Controls
Risk and Control Assessment
Risk Analytics
Loss, event and investigations management
Financial Risk Software
Credit
Capital allocation
Market
Trading/ transaction
Insurance/ underwriting
Other
Operational Risk and Control Software
Employment
Marketing
Financial assurance
Corporate governance
Information management
Business continuity
Legal and litigation
Tech/ systems
Product/ service quality
Helath and safety
Sales/ethics
Other
Supporting Technology Infrastructure
Identity Management, Change Management, Automated/Continuous Controls, Security Management, Content Management, Data Analysis etc.

4.2 Overview of available tooling

The research started by collecting an overview of the common tools available in the market. The market is very turbulent, many vendors are available in the market and as we speak, new vendors are being established or merging. Furthermore, tools are very diverse. Some tools are very generic, offering broad functionality, others are very specific, tailored to meeting specific requirements. When comparing the software packages, we first have to face the fact that we are restricted to Deloitte knowledge and desk research. We cannot address the vendors of the software directly because Deloitte considers itself a competitor and has made the strategic decision to avoid contacting the vendors directly. Furthermore, in doing literature research the best of material one can get is often whitepapers written by the vendors themselves and reports issued by market research institutes such as Gartner and Forrester. The reports produced by the latter often refer to the abovementioned whitepapers or don't follow a very scrutinizing approach and simply take the whitepaper characteristics. Because the goal of this thesis is not to provide an exhaustive list comparing all vendors on all measurable attributes, we will restrict myself here to discussing a shortlist of thirteen vendors. This shortlist was established together with Deloitte ERS.

4.3 Software assessment criteria

The software is compared on the basis of the CATs characteristics discussed in the preceding chapter. We am investigating how the software supports data analysis functionality, process mining functionality and continuous testing functionality.

4.4 Discussion of compared software

Except for Hyperion System 9 and SAS all packages typically support the documentation and communication of policies and procedures. Furthermore all packages support the definition of controls and have a template library or repository structure to store these controls. A library or repository is a database in which identified risks and according control activities are recorded, and this can be customized to meet the needs of the client. In Table 1, a comparison is made between the thirteen software packages. Support for this assessment is given in the software descriptions, which can be read in Appendix V: Software description and evaluation.

Table 1: Software evaluation

	Process mining	Data analysis	Automated Testing
ACL Continuous Controls Monitoring	0	2	2
Applimation Integra Apps	0	1	2
Approva Enterprise Controls Management	0	1	2
Aris Process Performance Manager	2	1	1
Bwise	0	1	1
eQsmart	0	0	1
Hyperion System 9	0	2	2
OpenPages	0	1	0
Paisley Enterprise GRC, GRC on Demand	0	1	0
ProM Framework	2	1	0
Protiviti Governance Portal	1	0	0
SAP GRC Process Control	0	0	2
SAS Enterprise Intelligence	0	2	2
0 = Does not support 1 = Supports 2 = Integrated			

What stands out is the fact that only ARIS PPM uses process mining functionality. This clearly is a topic of further research. ACL is the only package that uses advanced data analytics to support compliance programs. Most GRC software restricts its attention to streamlining the compliance process itself and leaving the (automated) tests to other parties. In continuous testing, Approva and ACL are the most versatile tools, offering adapters for all ERP packages. Applimation, Hyperion and SAP GRC are ERP specific software packages and are the least versatile. eQsmart is custom made for SAP and focuses on settings which are in effect at the moment the data is extracted. ProM is a tool which allows for mining event logs to identify process models.

4.5 Auditing with process mining

As seen in this chapter, few solutions are available using the power of process mining. In this paragraph we will elaborate on how process mining can be applied in auditing.

The application of process mining is twofold:

- Understand the entity
- Gather audit evidence

Process mining is able to discover a process model. In the pre-engagement phase of an audit project, process mining could be applied to create a basic understanding of the business process at hand.

Another application of process mining can be found in gathering audit evidence. This can be done in several ways, executing a delta analysis and analyzing the social network. In doing a delta analysis, the discovered process model can be compared to the prescribed model and deviations can be inspected. In order to apply this form of process mining, a prescribed process model must be available at the client, which is almost always not the case.

The other approach lies in executing a social network analysis. A gap exists in enforcing **segregation of duties**. Each user of an ERP system has several rights at the transaction level. Auditing an ERP system means inspection of user transaction rights and verifying if these rights are in accordance with their responsibility clearances in the organization. For example, a purchaser can only execute purchasing transactions and a sales manager only has the right to record sales transactions. One can imagine that conflicting transactions exist in an ERP system, for which it is better that a user is not allowed to execute both. The way ERP packages typically handle this problem is to enforce application controls that prohibit users from executing conflicting behaviour.

Deloitte has developed a tool called eQsmart which tests the settings for conflicting occurrences of user transaction rights. In the case of eQsmart the ERP package is SAP. Let us take an example in purchasing. A purchaser is allowed to create a purchase order and pay the invoice to that purchase order. Allowing this user to execute both transactions in the system creates a security breach. He could order goods for personal use and authorize the reimbursement to the purchase order. Therefore, these two transactions are often strictly separated in an ERP system.

Another drawback is that eQsmart only uses the actual settings in SAP and does not take into account the history of these settings. When eQsmart is installed and reports are run on a regular basis, this does not have to be a problem.

Process mining has the potential to enforce segregation of duties at the case level instead at the transaction level. A user can have rights to execute both transactions, as long as they do not handle the same case (in our example, the purchase order). An additional advantage of applying process mining is that the test uses historical information, so conflicting transactions executed in the past are also detected.

4.6 Summary

The software market is gradually maturing, having more integrated offerings and adding value for the client. Continuous testing and data analysis are improving and getting integrated, with the software often focussing on either of these characteristics. Of the discussed software, only one offering (ARIS PPM) is using process mining but even here the functionality is very dependent on the initial implementation of the software.

From a clients perspective, interoperable offerings would be much more attractive because of two reasons. First of all supplier dependency would be much lower. Secondly, interoperable components would better drive the market, optimizing at the component level and not at the integrated offerings level. If the market would be organised in this way, we expect qualitatively better solutions to be offered at more competitive pricing. Unfortunately, a very rigid upwards integration movement is taking place. This is mainly effected by the strong ERP vendors, who control the market and initiate these practices to better serve their own interests.

From the CATs perspective, the process mining technique is the least applied. Opportunities to use process mining exist in checking and enforcing segregation of duties.

5 Diagnosis

Based on the preceding analysis, this chapters formulates the final assignment which will lead to the design project to be performed at Deloitte ERS. After positioning the problem and the final assignment, several design directions and the according action plan are discussed.

5.1 Problem identification

In general, a stakeholder can face problems, opportunities and directives. When the current situation is preventing us to reach our goals, we are speaking of a **problem**. When the current situation is perfectly fine, but there is a feeling that it can still be improved, then we are talking about an **opportunity**. If our environment is forcing us to respond, thus driving the cause for change, we speak of a **directive**. Each of these forces can be the reason for a redesign project. We will start by discussing the issues that we encountered during the interviews for each of the stakeholders and come to a problem formulation that will lead to the final assignment.

The **client** is facing increasing governmental regulations forcing him to comply. These trends resulted in big investments in compliance software. Now that the architecture is installed for external compliance, the incentive for internal compliance is arising, i.e. conforming to *own* stated business rules. The problem is that often business rules are implicitly baked into an ERP system. Process mining can help the client make (recorded) business processes explicit and define his business rules. Furthermore, gaining insight in the real working of a business process creates a window of opportunity for process improvement.

For the **Deloitte ERS Auditor**, in planning an audit, understanding the business process is very important. Process mining can help him get an overview of how things are working. In executing the audit, the auditor can also be served by process mining because it is possible to detect anomalous process executions and process conformance. Unfortunately, no auditing tools are in the market that can help him with this approach. Furthermore, no business case exists where process mining in auditing practice has been practically proven.

According to the **public** perspective, many data analysis tools are available and trends are that these are increasingly being automated. This area of research is of less interest than the topic of process mining. After market research, we can conclude that process mining is an approach that is a relatively new concept and not yet society-wide embraced. Further research of a practical application is therefore important to further the understanding of this specific continuous assurance technique.

As agreed upon in the start of the project, one of the CATs would be selected to improve upon in order to move continuous assurance forward. In the analysis phase, we discovered that the eQsmart tool focuses on settings which are in effect at the moment the data is extracted. This means that eQsmart does not take into account the history of the transaction settings. A malicious user with enough rights could change his transaction access settings, execute conflicting behaviour and change the settings back. eQsmart would not discover this. Furthermore, by forcing a user to **not be able** to execute two transaction codes, his flexibility can be severely impaired. In most workflow management systems, users are indeed able to execute two conflicting activities, as long these don't relate to the same case. Process mining provides opportunities to develop a control objective that can test a historical event log for conflicting behaviour. This method releases the transaction level user restrictions and makes user rights much more volatile.

We therefore formulate the problem as follows:

> Process mining has been introduced as a promising new concept for improving the auditing function by testing control objectives using historical data. Until now, it has had a limited use in ERP systems because the lack of an appropriate technique that is able to extract trace event log data from the ERP systems. A gap between the theoretical approach of process mining and the benefits of practical application in real situations exists which has to be solved.

5.2 Problem analysis outcome

Research showed that process mining is not ready for continuous application, simply because the practical realization is not proven. Therefore, and because of abovementioned issues, the definition of the final assignment reads as follows:

> Develop a model describing the application of process model extraction and control objective testing using process mining in a general business cycle. Elaborate on the requirements of these applications using the expenditure cycle and application in the SAP R/3 environment.

The assignment is aimed at developing a work system for the auditing function. By creating a model in the context of which process model extraction is developed and following a case based approach, successful application can easily be expanded. That is why the assignment is explicit on two choices. First, a decision is made to study the purchasing process. The reason that this process is chosen is that this is an often studied process and literature is available. Furthermore, this process is expected to provide for a diverse set of controls and thus creating the chance to investigate which type of controls the technique will be suitable for and which type not. Second, the decision is made to choose the SAP R/3 ERP system. This decision is based on the fact that SAP is the leading ERP vendor amongst Deloitte clients and SAP expertise is available at Deloitte ERS.

5.3 Design approach

In order to address this assignment, three design directions are defined:

- Feasibility of testing control objectives
- Feasibility of executing process mining
- Feasibility in the SAP R/3 environment

Feasibility of testing control objectives

First of all, we will investigate for which controls process mining is a useful approach. From RACK, the Deloitte Risk and Control Knowledge Base, the typical purchasing controls must be chosen and mapped to the expenditure process, delivering a **control objectives model.**

Feasibility of executing process mining

The second aspect is the technical feasibility of process mining in an ERP package. Several attempts have been undertaken to apply process mining in ERP packages but these were unsuccessful. We will describe the problems encountered and design a **requirements model** which describes the prerequisites in order to be able to extract the correct data from an ERP system and transform it to be used in ProM, the process mining framework suitable for processing M-XML files. Two aspects are considered, applying ProM in order to extract the process model and applying ProM in order to test control objectives.

Feasibility in the SAP R/3 environment

Here we will consider the application of the requirements model in a real SAP system. In the expenditure context, what data must be extracted? What are the issues encountered when converting this data to usable ProM format?

To address this assignment, we will define a modelling approach on how to address the problem. Then the research model for the design phase is presented.

5.3.1 Modelling approach

According to (Whitten *et al.*, 2004), the life cycle of an IS-reliant work system can be split into two stages:

- Systems Development
- Systems Operations and Maintenance

First a system is developed and then it is operated and maintained. In Figure 12 the relation between system development and system operation can be seen.

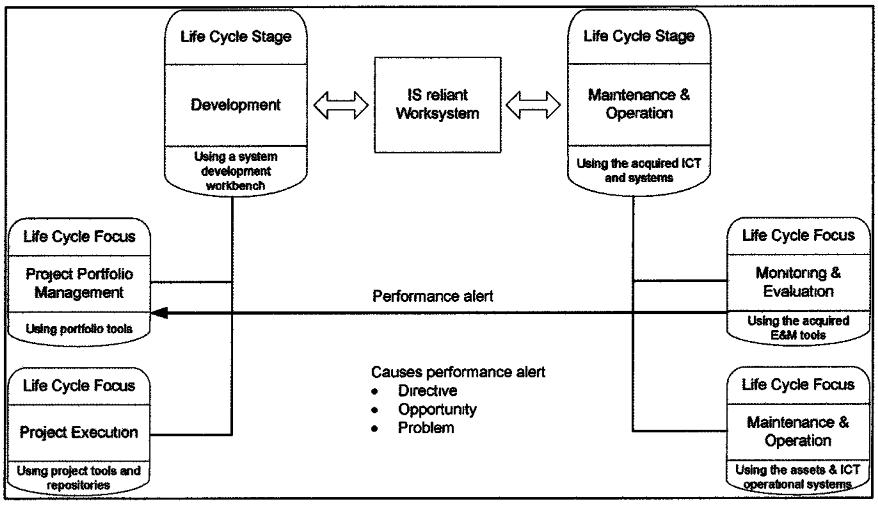


Figure 12: The life cycle of an IS Reliant Work System (Whitten et al, revised by Goossenaerts)

In this assignment, the performance alert is the opportunity to apply process mining in the audit process. This assignment comprises the first part of a system development project. Several approaches towards system development exist. The COMET methodology is a structured approach to developing or redesigning an IS reliant work system. We choose to use elements of the COMET design methodology because of its characteristics (Berre et al, 2004-2007).

COMET is:

- Object oriented
- Component based, meaning that the methodology is based on the belief that information systems can and should be assembled from components
- Architecture driven
- Model driven
- Iterative and incremental

In Appendix VI: Overview COMET methodology, an overview of the methodology is given.

5.3.2 Research model

In order to develop a business scenario, the following additional research will have to performed:

- Research on purchasing theory
- Research on controls in the purchasing cycle
- Research on process mining in SAP

First the work system is articulated., a Value and Risk model mutually relating the concepts in the work system. In this model, instantiations are selected for developing an example business scenario. This delivers a platform independent model (PIM model) for the purchasing cycle in chapter 7. This model is further filled in using instantiations of the classes specified. The focus is on creating a continuous assurance work system that aids the developers in defining the control objectives for a specific cycle and package that are feasible for testing using process mining techniques.

5.4 Work plan

Within continuous assurance, process mining is not a goal but a way to help the auditor in attaining his goal: performing the IT audit. The work plan for the design phase will contain elements of the development of the COMET models applied at different levels of abstraction, which is unusual for a typical technology management thesis. Therefore, we will discuss the Business Model in chapter 6 and 7. Chapter 6 discusses the Value and Risk Model, defining the context and the goal of the design and Chapter 7 will deal with the Business Operations Model, discussing the expenditure cycle and the control objectives in the expenditure cycle. Chapter 8 will then discuss the Requirements Model for the expenditure cycle, discussing the requirements for mining a process model from an ERP event log and the requirements for applying process mining in order to test control objectives in the expenditure cycle. Chapter 9 discusses the status of process mining in SAP and the requirements which will have to be met in order to successfully execute process mining. Chapter 10 discusses a case, where the ideas developed in the preceding chapters are applied to an extracted expenditure dataset at a Deloitte client. Chapter 11 presents an implementation plan to convert the methods proposed into a tool that can be used in the audit process. Chapter 12 presents the conclusions and the recommendations for further research.

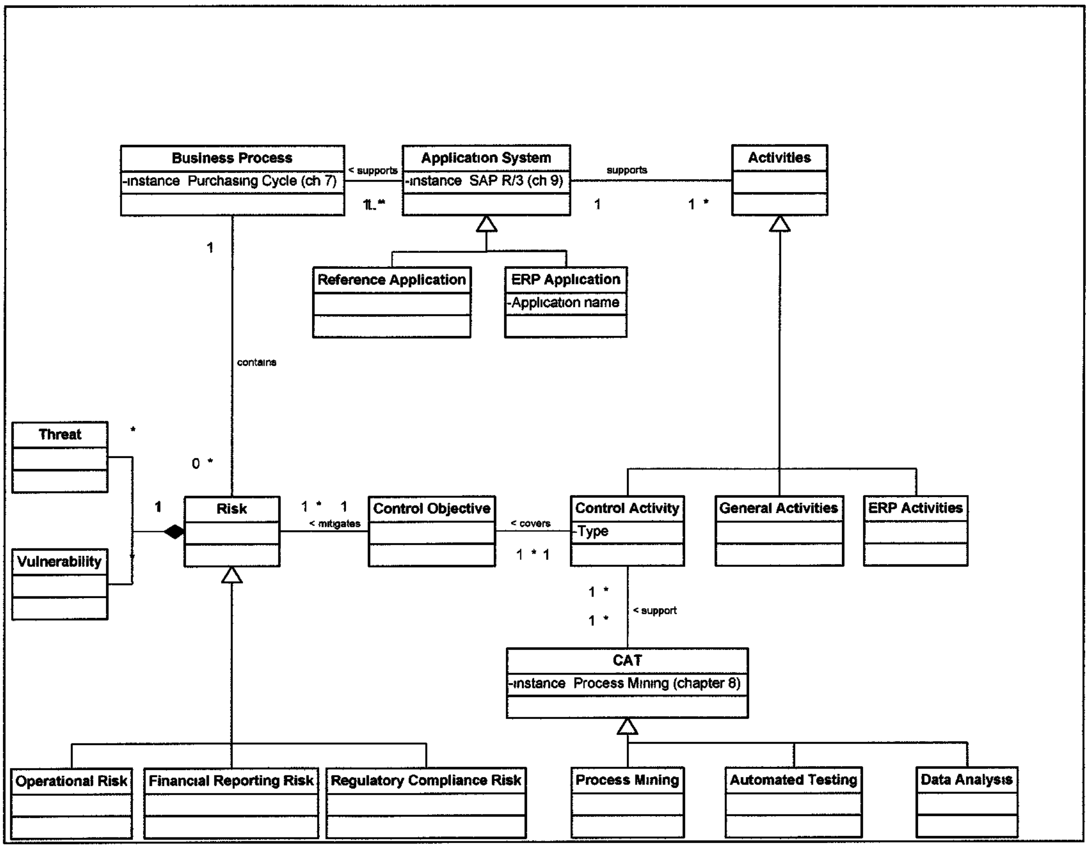
6 Value and risk model

The business model describes the part played by the product being developed in the context of the business that will fund its development and use it. It contains the context statement, the vision statement and the risk analysis. The scope of the model is any part of the world that is defined as interesting for the company, organization or others, and which has some impact on the required behaviour or other characteristics of the product. The goal model describes the business goals that will be met by implementing and using the product. The community model contains the roles and artefacts are involved in the work system. This chapter discusses the scoping statements, consisting of the context statement and the vision for change.

6.1 Context Statement

The context statement describes the scope of the design. First we developed a domain model, using the UML modelling language. Within the domain of application controls, the mission of Deloitte ERS is to provide control assurance regarding business processes. A business process is the set of activities the organization executes to add value for their customers. An example of a business process could be the purchasing process or the sales process. Each business process is subjected to risks (a result of threats and vulnerabilities) and these are countered using control objectives. The business process is supported by application systems and the control objectives are enforced by deploying control activities. In Figure 13 the domain model of the control assurance process is seen. These control objectives and the according control activities is what we are interested in, proposing a new method of achieving assurance using process mining (process mining being a method to execute a control activity).

Figure 13: Business resource model for the assurance process (Janmaat, 2006)



6.2 Vision Statement

As discussed in §4.5, in performing the audit plan the following activities are generally executed:

- Understanding the entity (pre-engagement phase)
- Gathering audit evidence (audit plan execution phase)

Process mining can be used to extract a process model using an event log. This can be very useful in understanding the entity.

The most approaches towards auditing focus on verification of a design rather than analyzing the actual behaviour. The vision is that a process mining tool can be designed that can support control activities for a number of control objectives in the purchasing cycle. A direct application of process mining is by testing control objectives on the event log. In this way, control objectives such as segregation of duties can be tested against a log of real events. In order to test controls using process mining, a control framework specifying the controls is needed. As a case, in the next chapter the purchasing cycle will be discussed. The method can be repeated as a work system to evaluate other business cycles and specify for each cycle which controls are feasible for process mining.

6.3 Summary

The successful execution of process mining in auditing can lead to less auditing effort, the release of restrictions on internal application controls and the automation of several auditing routines. The impact on the continuous assurance work system depends on leveraging the procedure on other business cycles and on rolling out the approach at different clients. This last remark means that a certain standardization of the approach is necessary in order to apply the procedure at other clients. In order to develop an approach for process mining, a close inspection of the control objectives applicable is needed. When a repository is filled with these control objectives and according control activities are devised, the approach can be expanded to other business cycles. The next chapter discusses an instantiation of the class Business Process, which is the Expenditure Cycle. For this Business Process, the control objectives are discussed (instantiations of the class Control Objectives). The control objectives which can be enforced using process mining (instantiation of the class Control Activity) are then discussed in the chapter.

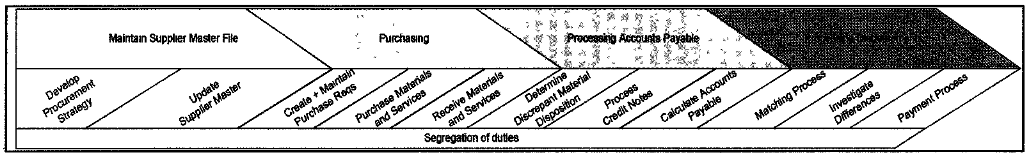
7 Business operations model

This chapter discusses the platform independent considerations regarding the application of process mining in continuous assurance. We will discuss an instantiation of the class of business processes, being the expenditure cycle. We will also specify the risks and according controls that are present in this cycle and we will discuss which of these controls are applicable for testing using process mining.

7.1 The expenditure cycle

The expenditure cycle is an instance of the class "Business Processes" represented in Figure 13. In Figure 14 the steps in the expenditure cycle are shown. In the expenditure cycle, four main steps are identified. These are: maintaining the supplier master file, purchasing, processing accounts payable and processing disbursements.

Figure 14: The expenditure cycle


Maintain Supplier Master File
Purchasing
Processing Accounts Payable
Develop Procurement Strategy
Update Supplier Master
Create + Maintain Purchase Reqs
Purchase Materials and Services
Receive Materials and Services
Determine Discrepant Material Disposition
Process Credit Notes
Calculate Accounts Payable
Matching Process
Investigate Differences
Payment Process
Segregation of duties

Maintaining the supplier master file constitutes of two tasks, developing the procurement strategy and updating the supplier master file. In the procurement strategy, the specifications in terms of quality and quantities of the goods and services that need to be bought are defined. Also, the vendor selection process and the results of the negotiations are defined in this part of the purchasing process, resulting in an agreement and a contract with the supplier. Accordingly, the supplier master file defines with which suppliers the company is doing business, which suppliers are the preferred vendors for certain products and what kind of purchasing agreements are set (pricing, standing orders, vendor-maintained inventories etc). This is the strategic part of the purchasing process.

Purchasing is the tactical and operational part of the purchasing process. In this part of the purchasing process, purchase requisitions for goods and services are created and maintained. These purchase requisitions are converted into purchase orders which are placed with the selected supplier and the purchased materials and services are received.

Processing accounts payable takes care of determining the amount that has to be paid to the supplier. The purchase orders are matched with the delivery notes recorded at the moment goods and services are received and the discrepant material disposition is corrected. Also applicable credit notes for returned goods are handled after which the amount which is due can be calculated.

In **processing disbursements**, the invoices received from the supplier are matched with the own information. The invoice is compared with the purchase order (is the invoice in accordance with the initial purchase order) and with the goods receipt (is the invoice in accordance with the goods received in the inventory). Also pricing is checked, is the supplier invoicing the agreed price. After all differences are investigated and resolve, the invoice is cleared for payment. After the due period, the invoice is paid to the supplier.

7.2 Verification of properties: using temporal logic

In the next chapter, we will describe the requirements for mining a process model and for checking event log properties. We will give an example of a definition of a control objective in LTL. After the objective is defined, it can be tested against a real event log using a ProM plug-in called LTL-checker. First, we will now disucss the expenditure control objectives and discuss why or why not these objectives are feasible for testing using LTL.

7.3 The expenditure control objectives

Deloitte uses the InfoBase as the repository to specify the risks and control objectives per cycle. Extracted from InfoBase, the main risks and according control objectives in the expenditure cycle are shown in Figure 15. Not all controls are feasible for testing with process mining. Feasibility is dependent on several factors:

- Is the data needed for testing the control objective logged in the system?
- Can an appropriate event log with enough detail be generated?
- What is the type of the control objective?

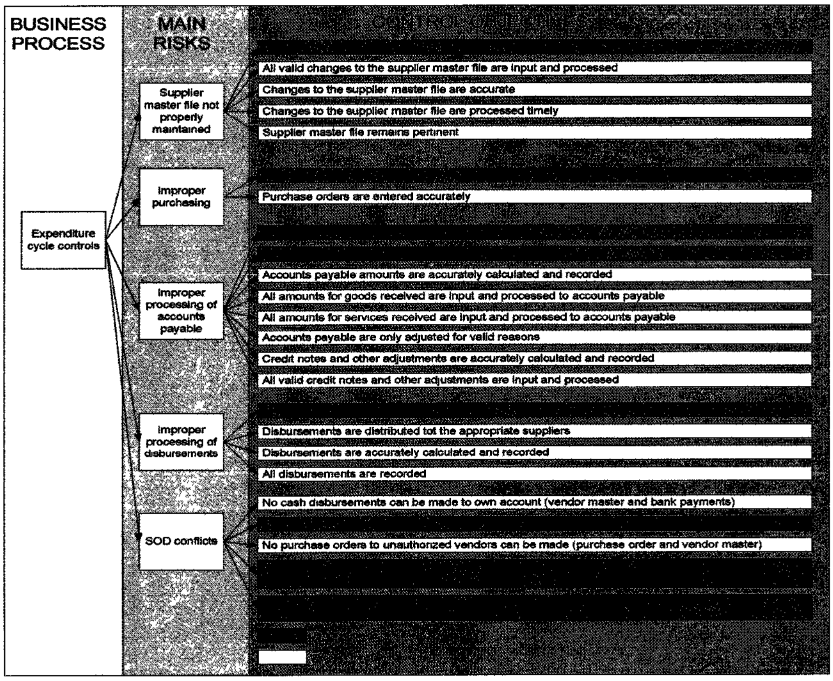
Transaction-level controls serve to prevent, identify and/or detect inappropriate, inaccurate or unauthorized transactions. As individuals perform day-to-day business processes, key steps and milestones are recorded as transactions and can take the form of entries in the financial system, e-mails or even conversations. This type of control objectives is very feasible for process mining because logging takes place at the transactional level.

Business processes and corporate policies are comprised of a prescribed sequence of tasks, events and transactions. Configurable controls ensure that processes are executed as intended. When business processes are highly automated, **configurable controls** ensure that the workflow which drives key processes is never circumvented. Configurable controls are mostly integrated in the ERP package. eQsmart can be used to detect deviations from these configurable controls. Process mining could be used to detect historical deviations.

Master data is the core information about an organization's customers, vendors, employees, raw materials and chart of accounts that is fundamental to the execution of mission-critical business processes. **Master data controls** ensure the integrity of this data so that mistakes are not compounded as transactions reference the data when business processes are executed. Process mining is of little use to check these control objectives, because often the controls involve the authorization of users to change master data.

We will give some examples to address each factor. The control objective "purchase orders are entered accurately" can not be tested using the data in the system. This objective refers to en employee taking an order and correctly inputting this into the system. The control objective must be tested using other means, such as inspection by observation or interviewing the employees. Another example of a control objective is "purchase orders are placed for approved purchase requisitions only". When applying process mining, the extracted process model will tell us the flow of the purchase orders. Based on an event log, a process model can be extracted which will make clear what the flow of purchase orders was, both in size and in order. So, this objective can be partly tested using process mining. Additionally, inspection of whether the authorized personnel is actually authorized to perform this activity (approving the purchase requisitions and converting these into purchase orders) must be done using other means. In Figure 15, the control objectives are colour-coded to indicate if the control objective is feasible for testing with process mining. All control objectives are discussed in detail in Appendix VII: Expenditure control objectives for PM. It can be seen that the three columns represent instantiations of classes in the business resource model for the assurance process (Figure 13).

Figure 15: Expenditure cycle control objectives


BUSINESS PROCESS
MAIN RISKS
CONTROL OBJECTIVES
Expenditure cycle controls
Supplier master file not properly maintained
Improper purchasing
Improper processing of accounts payable
Improper processing of disbursements
SOD conflicts
All valid changes to the supplier master file are input and processed
Changes to the supplier master file are accurate
Changes to the supplier master file are processed timely
Supplier master file remains pertinent
Purchase orders are entered accurately
Accounts payable amounts are accurately calculated and recorded
All amounts for goods received are input and processed to accounts payable
All amounts for services received are input and processed to accounts payable
Accounts payable are only adjusted for valid reasons
Credit notes and other adjustments are accurately calculated and recorded
All valid credit notes and other adjustments are input and processed
Disbursements are distributed tot the appropriate suppliers
Disbursements are accurately calculated and recorded
All disbursements are recorded
No cash disbursements can be made to own account (vendor master and bank payments)
No purchase orders to unauthorized vendors can be made (purchase order and vendor master)

7.4 Summary

In this chapter, we have discussed the control objectives in the expenditure cycle in a platform independent manner. We have identified control objectives which can be tested using process mining. In the following chapter, we will discuss the requirements for mining a process model and propose a method for the verification of properties based on temporal logic.

8 Requirements model

Now that the operations model is identified, the requirements have to be specified in order to map the platform independent approach to an IS-enabled approach. To be able to test the control objectives using process mining, we will first discuss the requirements for mining a process model. in §8.1 In §8.2, the requirements for checking control objectives using LTL-checker is presented.

8.1 Requirements for mining an event log

To be able to mine an event log and generate a mathematically sound process model, a dataset must be extracted that meets the criteria set forward by the process mining theory. General requirements and requirements for mining the expenditure cycle event logs is discussed here.

To be able to mine an event log, the log has to meet several requirements:

- The event log with audit trail entries must be extractable or otherwise compiled
- Activities should be uniquely identifiable
- Each audit trail entry should refer to a specific process instance

The first requirement defines that the event log minimally contains the process instance using a case ID (what), the activity executed (how), the time stamp (when) and the originator (who). These are the minimal requirements to mine a model.

We will discuss the last two requirements and reason why these have to be released in order to be able to mine an ERP-generated event log.

The second requirement means that an activity that is recorded in the audit trail entry always represents the same amount of work done. If an activity can mean the execution of several tasks, the mining of a sound process model becomes inoperable. We will give an example to illustrate this problem.

Consider the generic ERP package X with the process Y under scrutiny. Let us consider a general purchasing process, depicted such as in Figure 16, where the process instance is the purchase order. In Figure 17, the platform independent model object classes and their attributes are depicted.

Figure 16: Example purchasing process

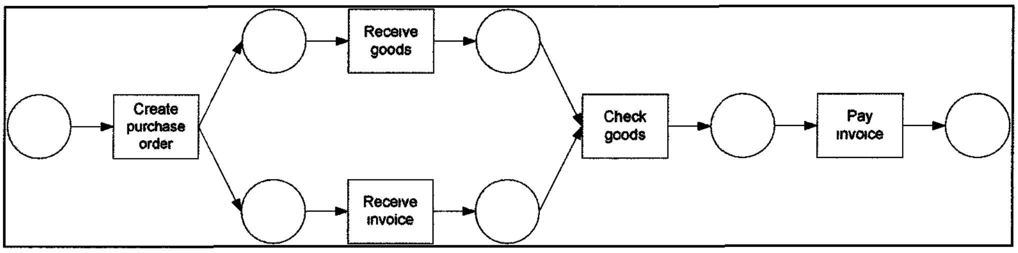
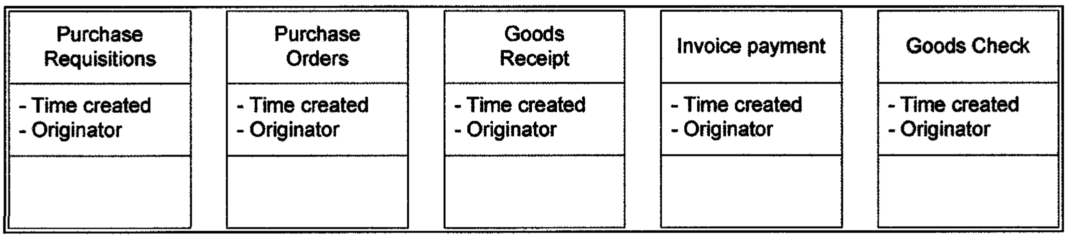
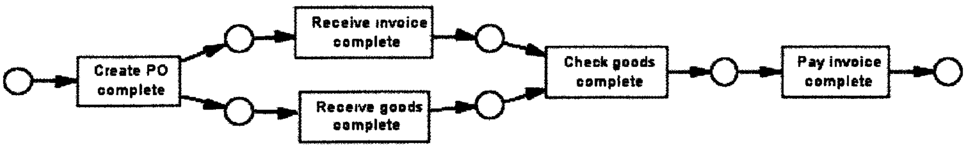


Figure 17: PIM classes in the expenditure cycle



The log can be found in Table 4: Stable event log, in Appendix IX: Two event logs. The logs contain three process instances. Based on the information shown and by making some assumptions about the completeness of the log (i.e. assuming that the cases are representative and a sufficient large subset of possible behaviours has been observed)[2] the model can be mined using alpha miner algorithm and a model as seen in Figure 18 is generated.

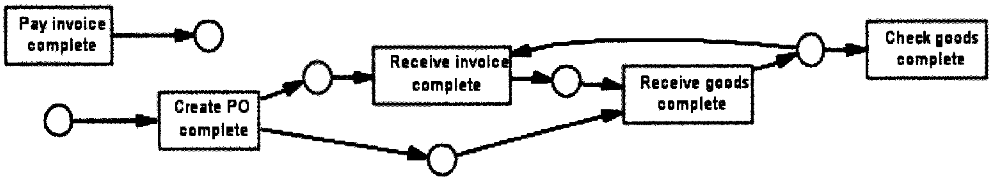
Figure 18: Mined petrinet of a sound event log using alpha miner



Now, suppose we add to the event log a few audit trail entries that can be perfectly fine in an ERP package. The modified event log is seen in

Table 5, the added entries are bold. In this log, goods can be received in parts and invoices are paid in several instalments. The alpha mined model is presented in Figure 19.

Figure 19: Mined petrinet of an unsound event log using alpha miner



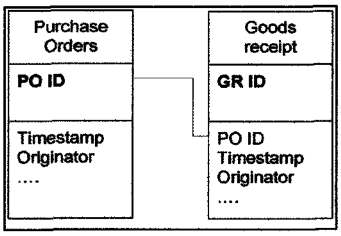
This model can not be used for interpretation. The explanation is that the activity "pay invoice" is executed several times. In constructing a petrinet, this is a problem, because the token before pay invoice is consumed after the first payment. To be able to execute the second (and subsequent) payments, a token should be put back in the place before the activity "pay invoice". This regeneration of a token is dependent on some kind of attribute that is defined as the remainder of the invoice after the last payment. Since the process mining algorithm is not able to generate

[2] Obviously the number of events in Table 1 is too small to establish these assumptions accurately. However, real event logs will contain thousands or more events.

dummy activities and dummy places, this property is not taken into account. The result is that no correct model is mined using the alpha miner plug-in.

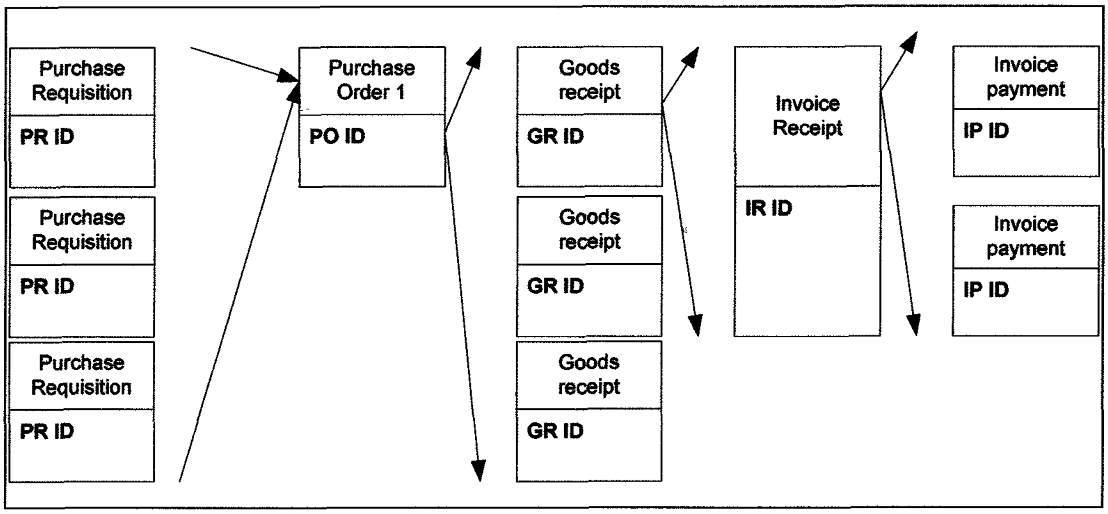
Now consider the following two actions: "create purchase order" and "goods receipt". Suppose the documents are kept in two different tables which display the following relation:

Figure 20: Example relation two documents



It is clear that no unique identifier is kept for both documents at the same time. A goods receipt could be a part of a purchase order, because some goods are delivered later. In this way, one purchase order can result in many different goods receipts, and so forth. So what should be taken as the case ID? If the PO ID is taken and the first time a goods related to a specific order are received, the activity goods receipt is fired. Then no purchase order can be created anymore for the same PR ID (because the token is gone). What can be done, is define the identifier of the process instance as **the combination of the two key fields**. This approach will lead to the expansion of the event log by generating dumourentries (see Figure 21).

Figure 21: The relation of the documents



We will call the property of this event log **divergence**:

A **divergent event log** contains audit trail entries which execute the same activity on one process instances several times. In a database structure, this is presented as 1:n cardinality. For example the goods receipt in several parts of a purchase order

The third requirement is that each audit trail entry should refer to exactly one process instance and this process instance must be recognizable. In WFMS systems, the identifier of the case is mostly the same throughout the process. In ERP packages, this case identifier tends to change throughout the process because each process step generates a new key field. Here, actually the opposite of divergence is the case:

A **convergent event log** contains audit trail entries which execute one activity on several process instances at once. In a database structure, this becomes clear as n:1 cardinality. For example the payment of several invoices related to several purchase orders

Note that the occurrence of convergence and divergence is dependent on the choice of process instance. In this example, if the purchase order is chosen as the process instance, divergence occurs because more receipt are happening related to the purchase order. On the other hand, say that we chose the goods receipt as the instance, convergence is happening because later in the process one payment is made for several goods receipts.

Alpha miner has proven to be useless if convergence and divergence is occurring in a log. If we use HeuristicsMiner (Weijters *et al.*, 2003), we get the result shown in Figure 33 (Appendix XIV). Note that this figure can be used for interpreting the process under study. The figure clearly shows the flow of orders. The fraction depicted at each arc represents the fraction of the audit trail entries in the event log that can be correctly parsed by replaying the log.

8.2 Requirement for checking controls using LTL-checker

The requirements for checking controls using LTL checker are less strict ((van Dongen *et al.*, 2004):

- An event log must be available
- A control objective translated to LTL language must be available

Divergence is no problem, because for every audit trail entry, a check is run to see if a violation of the decision rule is occurring. Convergence can be a problem, because then a check has to be done on a piece of data that does not have a specific case ID. For example, a user pays several cleared invoices at the same time. The payment is then related to several goods receipt, but it first must be clear if these goods receipt belong to the same purchase order. If this not the case, the payment can not be related to a unique purchase order ID and thus process instance. In the next paragraph we will give an example of a check performed using the event log presented in the previous paragraph and a control objective translated to LTL.

8.3 Testing a control using LTL checker

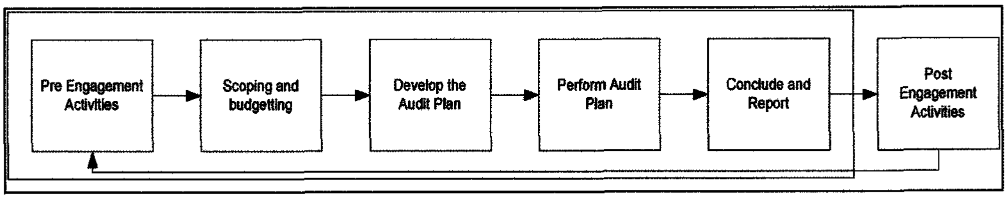
Let us again take the example proposed in §8.1 and use the unsound event log. Now propose that we want to test the SOD control objective "No user can purchase an item, mark it as received and enter and pay the invoice". This control objective is also called the "three-way match". The according LTL formulae are presented in Appendix X: Example LTL Control Objective. After using ProM to test the control objective, we can safely conclude that the three-way match is correctly enforced in this event log. This can be also concluded after visual inspection of the event log, but this gets harder when checking large event logs.

8.4 Integrating process mining in the audit approach

Now that two applications of process mining have been discussed, how do these applications fit in the audit process?

As can be seen in Figure 22, the application of process mining to visualize a process is useful in developing the audit plan and performing the audit plan. The testing of control objectives can be applied in performing the audit plan. In developing the audit plan must be defined which control objectives will be tested and how these will be tested. In performing the audit plan, the control objectives can be tested using the method proposed in the last paragraph. The application of the techniques proposed is dependent on the ERP package and the structure of the data extracted.

Figure 22: Process mining and the audit process



8.5 Summary

In this chapter, we discussed the requirements of applying process mining in generating the process model and testing control objectives. Generating the process model is a difficult process because the data models of ERP packages do not allow for easy process instance identification, due to problems with convergence and divergence. The application of testing control objectives is technically feasible because of the fact that less restrictions on the log exist. The feasible controls for testing control objectives are those which involve an originator, time based aspects and process instance information. The feasible controls are highlighted in Figure 15. In the following two chapters, we will discuss the application of the designed concepts in an ERP environment. In chapter 9, we will first present the basic concepts of the SAP ERP package and issues that arise in defining the dataset that needs to be extracted. In chapter 10 will apply the concepts on a real dataset.

9 Process mining in SAP R/3

In this chapter, we will discuss the application of process mining in the expenditure cycle in SAP R/3. This is a platform specific application of the model proposed in this thesis. According to Figure 13, this involves an instantiation of the First we will explain in short how SAP works by introducing the system wide concepts and objects. Then we will discuss the design of the expenditure cycle in SAP and the relevant objects for the expenditure cycle. Paragraph 9.4. will deal with testing a control objective in SAP and paragraph 9.5 will then give an example of a control objective and the LTL formulae that will be used to test the control objective.

9.1 How does SAP work?

SAP R/3 is basically a combination of a huge relational database and an application interface to change and use this database. All the information in the R/3 system is stored in **tables**. A table consists of **records**, entries in the table. The table furthermore contains **fields**. A field is a part of a record which defines a relevant attribute of the table record. About 90.000 tables are used in R/3. Whenever a user wants to execute a part of the business process, or a task, he can call a **transaction code**. A transaction code creates, changes or deletes records in the tables. An executed transaction code can updated one or more tables at the same time. Furthermore, a table can often be updated by one or more transaction codes. More than 10.000 transaction codes exist in the SAP R/3 environment. For example, in order to create a purchase order, the user can call transaction code ME21N. This will open a form where the user can specify all the details of the purchase order. The PO is assigned a unique **document number** and stored in the purchase order table (EKKO). This document number will denote the purchase order. All tables are linked using **foreign keys**. A field in the dependent table is referenced in the check table. For example, a purchase order is addressed to a specific vendor. A record in the table EKKO will contain a field called LIFNR, specifying the vendor account number. The reference table is LFA1 where more details about the vendor are recorded. A record in a table can be changed, resulting in an updated record and not in a new record. The changes are recorded in two other tables, called CDHDR (change document header) and CDPOS (change document items).

SAP R/3 is split up in three main **business areas**, called Logistics, Accounting and Human Resources. Every business area is split up in several **application modules** and every application module is split up in several **application components**. For example, Logistics contains Materials Management (MM), which is split up in materials requirement, purchasing, inventory management , warehouse management and invoice verification. Based on the needs of the company, the according application modules are selected, configured and implemented.

9.2 Obtaining the data in SAP: two approaches

As defined in the literature study: two approaches are proposed to process mine in ERP packages:

- Using transaction records
- Using table records

SAP is, as most ERP systems are, designed from a data perspective, supporting the integration of data using relational databases (Kassem & Rautenstrauch, 2005). This practically means that the execution of transaction codes in an ERP package is based on function logic, executing complex routines and often involving several activities or tasks.

We will illustrate the two approaches. Let us assume a user in an ERP environment creates a certain purchase order by executing a transaction code or completing a form. The fact that the transaction code is executed will result in an update of the table with the purchase orders. This table contains a unique key for the purchase order, which can be used as the case ID. Some other things will also be specified, such as the products that are ordered, (probably with a selected preferred supplier) and delivery terms. Now let us assume the purchase order is delivered. The user will execute another transaction code, called goods receipt, and the order is added to inventory. Then the supplier will send an invoice. The invoice is received, matched with the purchase order and paid to the vendor. Each of these activities are done by executing transaction codes and result in updates in database tables. New keys are generated, but the audit trail entries can be related to the initial purchase order.

So how will the audit trail entries be extracted? The first approach would look up the record of the user executing the transaction codes in a so called transaction monitor (the CDHDR table in SAP). Transaction codes are executed for all process steps and, if logged, can be extracted. The second approach would inspect the purchase order table and conclude that a purchase order is created and thus the activity create purchase order must have occurred. The same applies for the other tables, each table is updated and the update can be linked to the initial purchase order.

Let us discuss the problems for the first approach. When logging at the transaction level, the audit trail entries do not always refer to a unique activity. That would not be a problem, IFF (if and only if) the execution of a transaction code would mean that a certain set of tasks is executed AND those tasks are only executable by that transaction code. In that case, one would be able to derive a process model using the transaction level event log, because the WorkflowModelElement (transaction code) would denote a finite set of activities always executed by that transaction code. Process mining on the basis of transaction codes does not render a useable process model, because the transaction code denotes a set of tasks that may, or may not have been executed. The functionality of the ERP system is not revolving around how the purchase order is specified, it is revolving around how the work can be done most efficiently. That means that a transaction code can execute the payment of the invoices of several purchase orders. Or just a part of an invoice of a purchase order, but we don't know.

When using the table update approach, it is noted that the table purchase orders can contain a purchase order that is called upon by several goods receipt records in the goods receipt table. These records can either be the result of several goods receipt actions each booking in the goods receipt table a part of the purchase order (divergence), or the result of one goods receipt action, booking in several purchase orders at the same time (convergence).

We will explore the expenditure cycle in SAP to see if data logged in tables can be used to extract a process model and test control objectives.

9.3 The expenditure cycle in SAP

When discussing the expenditure cycle, in SAP several modules are important. Let us consider the whole process, from creating the purchase requirement until payment of the invoice.

The creation of the purchase requirement is done in the application module MM (materials management) in the application component PUR (purchasing). The used transaction code is ME51N for creating purchase requirement. This purchase order can be created individually (ME21N: vendor unknown and ME25: vendor known) or by converting purchasing requirements to purchase orders (ME58 and ME59). A purchase order consists of a header and line items. The header presents basic information about the purchase order and the line items are the products that are being ordered by the PO. After the PO is issued, an invoice is received and booked in (using transaction code MIRO: enter invoice) and goods are received (using transaction code MIGO: goods receipt for purchase order). Of course, goods and invoices don't have to arrive at the same time or in the same quantities. That is why the GR/IR account exists where invoices and goods receipts are parked. After the invoice is received, the invoice must be booked to accounts payable in the Financials module (RB60: invoice). After the documents are cleared (matched), a payment request is issued.

9.4 Testing a control objective

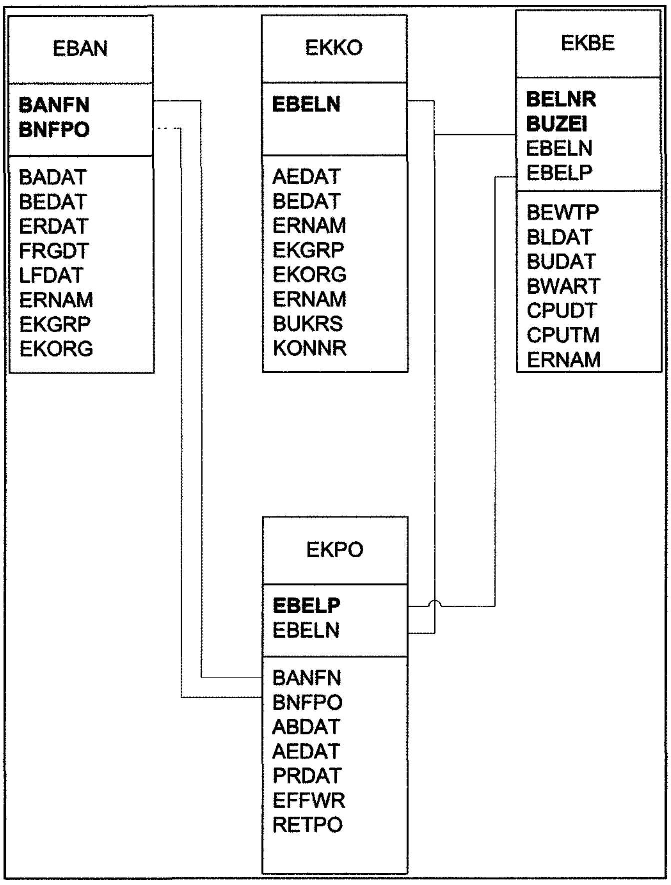
Suppose we want to test the control objective that no user is creating a purchase order and receiving the goods. Using the definition of the above described format, we need data on the creation of purchase orders and data on the goods receipt. When this data is gathered and formatted in the correct way, the event log can be built, loaded and checked. As a verification for checking control objectives with LTL checker, we will conduct a case in chapter 10. But first, we will have to sort out where the relevant data is hiding in the SAP database.

9.5 Obtaining the data: relevant tables and relationships

Depending on the scope of the audit, data must be extracted form the ERP pacakage. Van Giessel (Van Giessel, 2004) executed a research in order to identify the data needed for process mining in SAP and came to the conclusion that extracting the needed data is very laborious and case-dependent.

Let us assume that we are to audit the expenditure cycle in an SAP environment. Let us discuss the first activities of the purchasing process: create purchase requisition, create purchase order, receive goods and receive invoice. The execution of a transaction code cause an update of one or more tables. The tables, the fields and the relations between the tables are important for our approach because they contain the relevant information for applying process mining. Here we will inspect the relevant tables for the first part of the expenditure cycle, which are EBAN, EKKO, EKPO and EKBE. The table EBAN logs all the purchase requisitions. The table EKKO logs the purchase order headers, while the table EKPO contains the line items. The table EKKO and EKPO are related by the key field EBELN (purchase order number). The table EBAN and EKPO are related by the field BNFPO. A requisition is made on an item basis. Not all entries in the EKPO table have a value for the field BNFPO, because an item can also be ordered directly (without the purchase requisition). The table EKBE logs all the goods movements and associated invoices sent. The field BEWTP is de identifier of the type purchasing document history and is dependent on the transaction code. For example, when someone runs MIRO, goods receipt, an entry is made in this table and BEWTP fill become "Q", denoting "Goods receipt" in the enumeration table T163B (purchasing history category) . When a user executes transaction code MIGO, the field denotes the letter "E" representing goods receipt. In Figure 23 the tables and their relations are displayed. This is a platform specific representation of the object classes discussed in chapter 8 (Figure 17). For the sake of clarity, the description and the mapping of all the fields is added in Appendix XI: Overview tables and attributes.

Figure 23: Relation between the tables



Before a model can be mined, the requirements as specified in chapter 8 must be resolved. First of all, the architecture of the event log is required defining which records are needed and where they originate. As the process instance ID we chose the purchase order number.

Now that the data sources are determined, we have to build up the event log. The event log can be translated using the format presented in Table 2. An extract from SAP is used to select the relevant fields and convert these to an event log in Access format. This file can then be imported in ProM for analysis.

Table 2: Event log conversion format

PI-ID	Source	WFMElt	Originator	Timestamp	EventType
	EBAN	Create PR	ERNAM	ERDAT	Complete
EBELN	EKKO	Create PO	ERNAM	BEDAT	Complete
EBELN	EKPO	"Create PO line item" IF RETPO.EKPO="x"	ERNAM	AEDAT	Complete
EBELN	EKPO	"Return PO line item" IF RETPO>EKPO=""	ERNAM	AEDAT	Complete
EBELN	EKBE	"Goods receipt" if "BEWTP.EKBE=E"	ERNAM	CPUDAT	Complete
EBELN	EKBE	"Account Maintenance" IF BEWTP.EKBE="K"	ERNAM	CPUDAT	Complete
EBELN	EKBE	"Delivery Note" IF BEWTP.EKBE="L"	ERNAM	CPUDAT	Complete
EBELN	EKBE	"Subs deb log IV" IF BEWTP.EKBE="N"	ERNAM	CPUDAT	Complete
EBELN	EKBE	"Invoice Receipt" IF BEWTP.EKBE="Q"	ERNAM	CPUDAT	Complete
EBELN	EKBE	"Goods issue" IF BEWTP.EKBE="U"	ERNAM	CPUDAT	Complete

The records in EKPO do not have an originator. The originator is actually the person who makes the purchase order so the attribute is inherited from the table EKKO. Furthermore, the records in the table EBAN do not have the case ID because they are indirectly linked to the table EKKO. These are generated using a query.

9.6 Summary

Before an event log can be extracted from SAP, it must be clear what data is needed and identified how and where this data is logged in the system. This is dependent on the scope of the audit and the control objectives that are to be tested.

Identifying an explicit workflow model in ERP systems is very difficult, as the identification of such explicit workflow model requires a deep understanding of the enterprise structure. It is already clear in this piecewise application in SAP with regard to the expenditure cycle. This conclusion is supported by Kassem & Rautenstrauch (2006).

When the scope and the control objectives are defined, it is possible to extract the data and run a control objective testing routine on SAP data, as long as every audit trail entry in the event log contains a case ID. With 1:N cardinality (divergence) this is no problem, with N:1 cardinality it is (convergence).

10 The case discussion

In this chapter, we will test the methods we described in the previous chapters. First we will provide a description of a case. Then we will describe the extraction of the needed data. Paragraph 10.3 describes the conversion of the extracted dataset to a mineable format. Then, §10.4 will discuss the extraction of the process model based on the data. Respectively, alpha miner is used and heuristics miner is applied. In §10.5 the testing of a control objective based on the data is done. In the last paragraph, conclusions are drawn on the basis of this exercise.

10.1 Description of the case

The case data is extracted from a running SAP R/3 environment at a client of Deloitte ERS. The client has indicated to not be named in the report, but company background information is not needed to interpret the results. The data represent a generic purchasing cycle.

10.2 Preparation phase

The preparation phase consists of obtaining the data, constructing the event log and storing the data.

10.2.1 Obtaining the data

Based on the information presented in chapter 9, a direct download was made from the SAP database. The scope was data ranging from January 1st until June of this year. The database tables that were queried, were the following:

- EBAN (purchase requisitions)
- EKKO (purchase orders)
- EKPO (purchase order line items)
- EKBE (purchase order history)

Of these tables, the fields that were exported are shown in Appendix XI. Not all the extracted fields were used in the analysis.

10.2.2 Constructing the event log

Of the dataset we received, we decided to only take into account the purchase orders that were created in the month March. This resulted in 1892 process instances and 33261 audit trail entries. The dataset was converted using the format presented in Table 2: Event log conversion format. The description of the conversion steps are described in Appendix XIII. Note that in the log the activities “Subs deb log IV” and “Account Maintenance” do not occur. We deleted 24 audit trail entries that contain the first activity and 302 audit trail entries containing the second. We do not know what these activities are and regard them as noise.[3]

Three event logs are created:

[3] Mind you: these records are very interesting from an auditor point of view! What impact do they have on the expenditure cycle?

Event log 1: all records

This is the event log as created in the description, containing 33261 audit trail entries.

Event log 2: no PR

Because of the fact that of the 1892 purchase orders only 112 are based on a purchase requisition, we delete these from the event log, in order to analyze what kind of a process model is extracted. The log contains 33149 entries.

Event log 3: no PO line items

In this log, we remove the PO line items in order to study the relation between the purchase order, goods receipt and invoice receipt. This yields an event log with 26896 audit trail entries. This event log will be discussed in this chapter as an example.

10.3 Pattern discovery and analysis

Now that the event log is created, a process model can be extracted. We will apply two different mining algorithms, as we argued in chapter 8, using Alpha Miner is not applicable on an event log with divergence and convergence. We will use HeuristicsMiner to create a process model.

10.3.1 Analyzing the dataset using ProM HeuristicsMiner

The event logs are loaded into ProM HeuristicsMiner. Two runs are made on each event log, one using a high threshold and one using a low threshold. A high threshold means that a relation between two activities has to be strong to show up in the process model (i.e. the relation must be seen at many audit trail entries). The reverse is true when mining with a low threshold: every interaction between activities is represented. For more information on thresholds, we refer to (Weijters *et al.*, 2003). The process models rendered on the basis of the event logs are presented in Appendix XIV. We will discuss the results of the process model extraction process.

Event log 1: all records

From the process model generated by this log can be concluded that most purchase orders follow the path create purchase order, goods receipt, invoice receipt. Points that can be remarked:

- In 63 cases a purchase order line item is returned even before the line item is created
- Only 112 of the purchase orders are created on the basis of a purchase order
- In 24 cases, the purchase requisition is also created after the purchase order is placed. This order flow must be subjected to closer inspection.

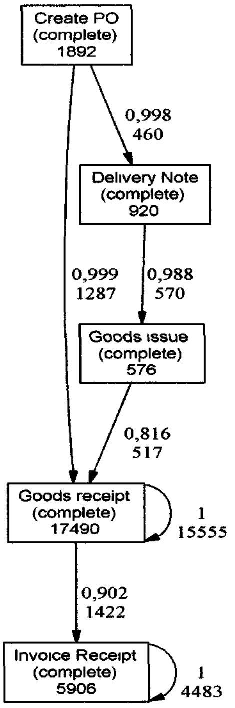
Event log 2: no PR

In this run, we delete the purchase requisitions from the log because they only occur in 112 process instances. This model yield no improvements.

Event log 3: no PO line items

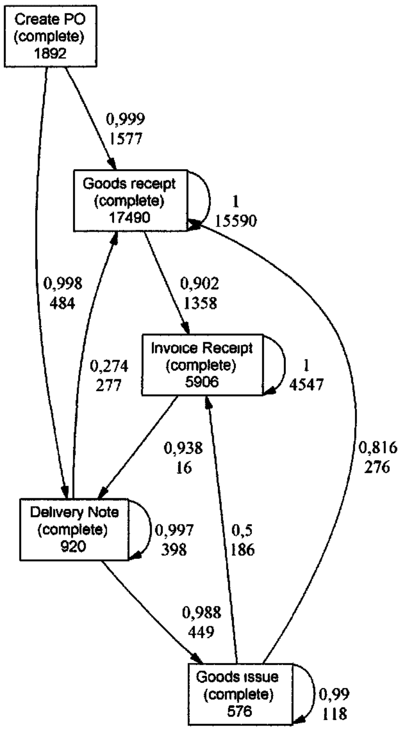
In this run, we delete the PO line items and PO line item returns to see how the purchase orders, the goods receipt and the invoice receipt interact. The high threshold process model yields a diagram on the basis of which can be concluded that about ¾ of the orders is recorded as a goods receipt and ¼ is recorded as a delivery note. It makes sense to inspect the data structure in order to conclude when a delivery note is recorded and when a goods receipt.

Figure 24: HeuristicsMiner process model based on event log 3, high treshold



If we inspect the low threshold version of the model, we easily see which deviant arcs are present in the process that need inspection. For 276 orders, goods are received after the goods issue is recorded. This should not be possible and should be further inspected.

Figure 25: HeuristicsMiner process model based on event log 3, low treshold

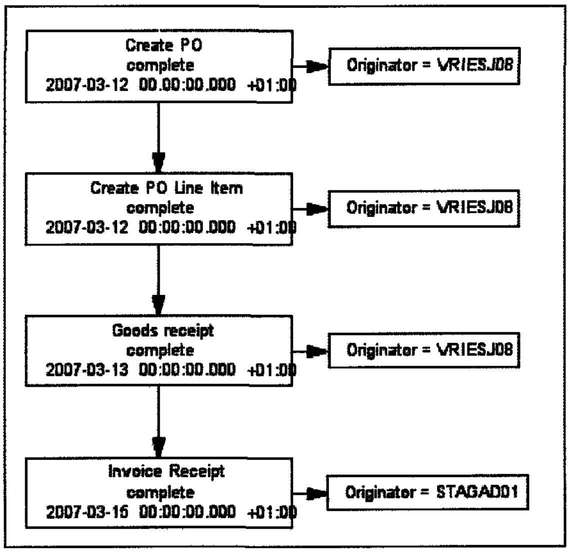


HeuristicsMiner can be used to mine a process model from a dataset. The great advantage of HeuristicsMiner is the possibility to create a threshold. If a high threshold is chosen, the main process steps are presented. Conversely, for the auditing function choosing a low threshold shows the ways the process is executed. Small order flows can quickly be recognized and subjected to a closer inspection.

10.3.2 Testing a control objective using LTL checker

Here we will test the application of testing a control objective using LTL checker. Let us use the control objective presented in §9.4 where no user can create a a purchase order and mark it as received. The formula name of the check is: "exists_person_doing_task_A_and _B". We ran the routine on the dataset and came to the conclusion that of the 1892 process instances, in 351 cases these two activities is done by the same user.

Figure 26: LTL checker result



These process instances can then be subjected to a closer inspection. In this manner, several control objectives can be formulated and tested against the log. The most feasible type of control is in the category of SOD control objectives.

10.4 Summary

Once known which tables and which fields are needed for the analysis, extracting the dataset from SAP is straightforward. Defining which tables and fields are needed is the difficult part. After the data is extracted, some tricks and ploys have to be executed to get the data in a mineable format. Mining the dataset with alpha miner yield nothing useful. The explanation for this is that alpha miner cannot cope with the released restriction of allowing an activity to execute more than once on a process instance. HeuristicsMiner is able to handle loops, so executing heuristics miner gives an overview of how the order flows. For ad hoc inspection of the expenditure cycle this is a useful exercise. Testing a control objective using LTL checker has been done with an example: the process instances where the property does not holds are filtered perfectly. This application has proven to be of significance for the audit routine.

11 The implementation

In this chapter, I introduce an implementation plan for developing the tool for the audit function, taking into account the fact that the tool must be expanded, continuously developing new applications using the continuous assurance domain model as a reference. The implementation of an information system can be seen as a project. In §11.1 the System Implementation Method (Kruithof & Poll, 1991) is used as the basis for creating an implementation plan for further developing the tool at Deloitte ERS. The System Implementation Method is further explained in Appendix XV. The method distinguishes seven key aspects.

11.1 Implementation plan audit routine

In this section the seven aspects of the System Implementation Method will be applied on the tool improvement project at ERS. The seven aspects are:

- The project approach
- The project phasing
- The project organization
- The project crew
- The project facilities
- The project budget
- The project planning

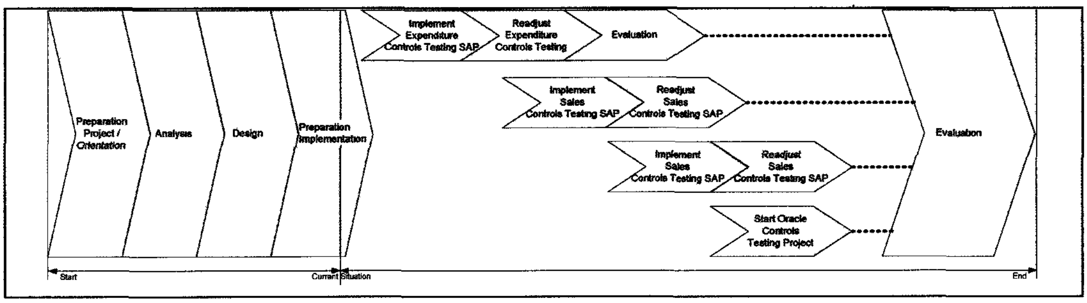
11.1.1 The project approach

By automating controls testing routines using event logs and LTL formalisations in the expenditure cycle and by expanding the approach to other cycles in SAP, the tool can be further improved. Because the conclusion is that testing is feasible but needs to be evaluated on a per cycle basis, no clear end date of the development process is proposed. Also, no direct external pressure exists (other than the general need to innovate). Therefore a process approach is being followed.

11.1.2 The project phasing

At this moment the project has reached the phase of preparation implementation. This concerns the creation of an automatic tool that can transform SAP expenditure data into event logs which can be parsed with LTL control objective routines. After the creation and successful use of such a tool, an evaluation can take place and the application can be expanded to other business cycles and ERP systems.

Figure 27: Overview of phases of implementation


Preparation Project / Orientation
Analysis
Design
Preparation Implementation
Implement Expenditure Controls Testing SAP
Readjust Expenditure Controls Testing
Evaluation
Implement Sales Controls Testing SAP
Readjust Sales Controls Testing SAP
Implement Sales Controls Testing SAP
Readjust Sales Controls Testing SAP
Start Oracle Controls Testing Project
Evaluation
Start
Current Situation
End

11.1.3 The project organization and crew

The project organization will consist of a project team that has one project leader, which is Marc Verdonk. The members of the teams will be either key users of the tool (SAP IT auditing staff form the SSG group) and programmers from the WebServices group.

11.1.4 The project facilities

All activities in this project plan can be executed at Deloitte ERS, facilities are available.

11.1.5 The project budget

A budget is allocated to the project in the form of the Continuous Monitoring Team (x-monitoring team), under the leadership of Willem Ypma. This team is responsible for allocating financial resources and human resources (indirect hours) to projects. Sufficient resources are available within his team to support the team of Marc Verdonk.

11.1.6 Project planning

Below is an initial milestone-based project plan for the development of the first automated tool. The presented project planning is a concept version and has yet to be approved by the stakeholders.

Table 3: Project planning

Major project milestones	Start date	End date	Team lead	Execution
Introducing ProM and LTL to the programming staff	03-sep	07-sep	M. Verdonk	Marc Verdonk
Programming the automated testing tool	10-sep	21-sep	M. Verdonk	WebServices team
Introducing the tool to users and training	End of year		W. Ypma	Techweeks
Applying the tool in audits	Begin 2008		M. Verdonk	SSG group
Readjusting the tool	Begin 2008		M. Verdonk	WebServices team
Evaluating the tool	Begin 2008		M. Verdonk	X- Monitoring Team
Deciding on the expansion of the tool	Begin 2008		M. Verdonk	Marc Verdonk

11.2 Risk Analysis

Applying process mining provides a means to test the controls directly on the recorded events. The successful execution of process mining in auditing is dependent on the quality of the data that can be extracted from the information system. This means that the choice to use process mining in the audit approach should be explicitly made in the engagement phase. Furthermore, this extraction of data should be done using a information-system-dependent standard adapter. This adapter should be insensitive to information system configurations and/or customizations.

11.3 Summary

This chapter proposes an implementation plan to gradually expand the application of the functionality to other business cycles within SAP and other ERP packages. Because this trajectory will need specialized resources and programming skills, the project will fall under the umbrella of the x-monitoring team.

12 Conclusions and recommendations

In this chapter, we will draw conclusions about the research. The research objective as proposed in chapter 5 reads as follows:

> Develop a model describing the application of process model extraction and control objective testing using process mining in a general business cycle. Elaborate on the requirements of these applications using the expenditure cycle and application in the SAP R/3 environment.

Applying process mining in ERP systems certainly is feasible, although some academic mathematical restrictions will have to be released. This is the direct result of the fact that ERP packages are functionally designed, not directly supporting mining initiatives. Using the tables available in an ERP package it is possible to extract a mineable dataset. Because of the above-mentioned restrictions, using this dataset to extract a process models is rather hard, but possible. The more interesting application is to build LTL routines in order to check predefined control objectives. The first advantage of the proposed method using the LTL checker over the eQsmart tool is the fact that historical data is used. A user changing the settings in between eQsmart checks is noted. The second advantage is that control objectives can be enforced at the process instance level instead of the transaction level, creating flexibility in allocating work to employees.

Conclusions on feasibility of testing control objectives

The testing of control objectives has been proven feasible. The most interesting class of control objectives are the segregation of duties control objectives. When the control objective is specified, the dataset can be used to test these objectives and conclude if conflicting behaviour has occurred. Because a thorough knowledge of the data structure of an ERP application is needed, the ad-hoc application for SOD control testing is not very attractive.

On the other hand, the data structure of an ERP application is rather static. If a tool is built that specifies which data from which tables is needed and directly runs a LTL check using specified LTL control objectives, the application becomes very interesting. An additional advantage is that the auditor just needs to make a data download and doesn't have to change data or settings at the client. For this application, an implementation plan is proposed.

Conclusions on feasibility of executing process mining

The technical feasibility of process mining in an ERP package has been proven as well but is less interesting for a straightforward approach. Problems with convergence and divergence exist, making the definition of a process instance very laborious. Furthermore, process mining in an ERP package does require a thorough knowledge of the data structure of the ERP package, which renders the application less interesting. It can be a handy tool to quickly inspect a specific cycle. A process model using heuristics miner can be generated and visual inspection can aid the auditor in identifying defecting behaviour.

Conclusions on feasibility in the SAP R/3 environment

In SAP, extraction and conversion of a dataset in a narrow scope has been executed and proven feasible. In our research, we conducted a process mining project manually to experience which problems arise. Setting up an extraction and conversion mechanism in order to create an event log has been proven to be very dependent that on the data structure. In order to test SOD control objectives, per cycle a clear data extraction and conversion script must be made before easy testing of control objectives is feasible.

In order to develop a useful tool for the audit, we have designed a continuous assurance domain model that covers the areas of interest in developing new tools for the audit function. Because the tool will have to be developed on an incremental basis, we have proposed a plan of attack to gradually transform the platform independent principles discussed to an IS-enabled audit execution supporting functionality, starting with the expenditure business cycle in SAP, extending to other business cycles and other ERP packages, CRM packages and financial administration software.

It is clear why no standard adapter from SAP to ProM has yet come into existence. For every cycle, process mining based on data available in ERP databases is dependent on the way the data is stored in the tables. The approach based on developing procedures for specific cycles can help overcome this problem.

The drawbacks of the approach is that the assumption is made that the data extracted is complete and correct. This drawback is recovered by the fact that the approach is intend to contribute to the level of assurance based on the evidence received.

The reason why we scoped the case to one month of purchase orders is because of the fact that Excel is not capable of handling large files. Our recommendation is to develop a ProM adapter import plug-in for the ACL package. ACL can work with extremely large exports of database records, making the testing of control objectives over larger time frame more feasible.

Bibliography

Reference List

1. Amato,R.A. & Eysink,W.T. (2005) Young Deloitte. In.

2. Becht,M., Bolton,P. & Roëll,A. (2003) *CORPORATE GOVERNANCE AND CONTROL.*

3. Berre,A.J., Elvesaeter,B., Aegedal,J.O., Oldevik,J., Solberg,A. & Nordmoen,B. (2004-2007) COMPONENT AND MODEL-BASED DEVELOPMENT METHODOLOGY: METHODOLOGY HANDBOOK. https://modelbased.net/comet/index.html

4. Committee on the Financial Aspects of Corporate Governance (1992) THE CADBURY REPORT. In: London.

5. de Beer,H.T. (2004) THE LTL CHECKER PLUGINS: A REFERENCE MANUAL. In: Eindhoven University of Technology, Eindhoven.

6. de Medeiros,A.K., van der Aalst,W.M.P. & Weijters,A.J.M.M. (2005) USING GENETIC ALGORITHMS TO MINE PROCESS MODELS: REPRESENTATION, OPERATORS AND RESULTS. *BETA Working Paper Series.*

7. de Medeiros,A.K., van Dongen,B.F., van der Aalst,W.M.P. & Weijters,A.J.M.M. (2004) PROCESS MINING: EXTENDING THE A-ALGORITHM TO MINE SHORT LOOPS. *BETA Working Paper Series.*

8. Deckers,F.B.M. & van Kollenburg,J.C.E. (2002) *ELEMENTAIRE THEORIE ACCOUNTANTSCONTROLE.* Wolters-Noordhoff, Groningen.

9. Demneri,A. (2005) A NEW LOOK. In.

10. Eisenhardt,K.M. (1989) AGENCY THEORY: AN ASSESSMENT AND REVIEW. *Academy of Management Review,* 57-74.

11. Head,K.M. (2005) CONTINUOUS ASSURANCE: PROACTIVE MONITORING FOR ERRORS AND IRREGULARITIES. In.

12. Institute of Internal Auditors (2005) INFORMATION TECHNOLOGY CONTROLS (GLOBAL TECHNOLOGY AUDIT GUIDE (GTAG) NO.3, Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment. *Internal Auditing,* **20**.

13. Kassem,G. & Rautenstrauch,C. (2006) IMPROVEMENT OF ENTERPRISE WORKFLOW IN ERP SYSTEMS BY MEANS OF USAGE MINING METHODS: SAP R/3 AS EXAMPLE OF THE PAPER. In: *Interactive Mobile and Computer Aided Learning Conference.*

14. Kassem,G. & Rautenstrauch,C. (2005) PROBLEM OF TRACING WORKFLOW INSTANCES IN ERP-SYSTEMS. In: *2005 International Business Information Management Conference,* pp. 123-131.

15. Kruithof,E.J.D. & Poll,H.K. (1991) *SYSTEEM IMPLEMENTATIE METHODE: METHODISCHE AANPAK VAN DE IMPLEMENTATIE VAN INFORMATIESYSTEMEN.* Academic Service.

16. Rasmussen,M. (2007) WILL THE REAL RISK AND COMPLIANCE VENDOR PLEASE STEP FORWARD? In: Forrester.

17. Sarva,S. (2006) CONTINUOUS AUDITING THROUGH LEVERAGING TECHNOLOGY. *Information Systems Control Journal,* **2**.

18. van Brummelen,H., Coban,S., Dollieslager,D., Lakenman,E., Rogers,T., Tukker,M. & Verstegen,G. (2006) SOX AND COMPLIANCE TOOLS - KEY FINDINGS. In: Capgemini.

19. van der Aalst,W.M.P. (2005) BUSINESS ALIGNMENT: USING PROCESS MINING AS A TOOL FOR DELTA ANALYSIS AND CONFORMANCE TESTING. *Requirements Engineering Journal,* **10**, 198-211.

20. van der Aalst,W.M.P., Ter Hofstede,A.H.M. & Weske,M. (2003) BUSINESS PROCESS MANAGEMENT: A SURVEY. In: *International Conference on Business Process Management,* pp. 1-12. Springer-Verlag, Berlin.

21. van der Aalst,W.M.P. & Weijters,A.J.M.M. (2004) PROCESS MINING: A RESEARCH AGENDA. *Computers in Industry,* **53**, 231-244.

22. van Dongen,B.F., de Beer,H.T. & van der Aalst,W.M.P. (2004) PROCESS MINING AND VERIFICATION OF PROPERTIES: AN APPROACH BASED ON TEMPORAL LOGIC. In.

23. Van Giessel,M. (2004) PROCESS MINING IN SAP R/3. In: Master Thesis, Dept of TM, University of Technology, Eindhoven.

24. van Praat,J.C. & Suerink,J.M. (1992) *INLEIDING EDP-AUDITING,* 5th edn. Ten Hagen & Stam.

25. Weijters,A.J.M.M., van der Aalst,W.M.P. & de Medeiros,A.K. (2003) PROCESS MINING WITH THE HEURISTICS ALGORITHM. In.

26. Whitten,J.L., Bentley,L.D. & Dittman,K.C. (2004) *SYSTEMS ANALYSIS AND DESIGN METHODS,* 6th edn. McGrawHill.

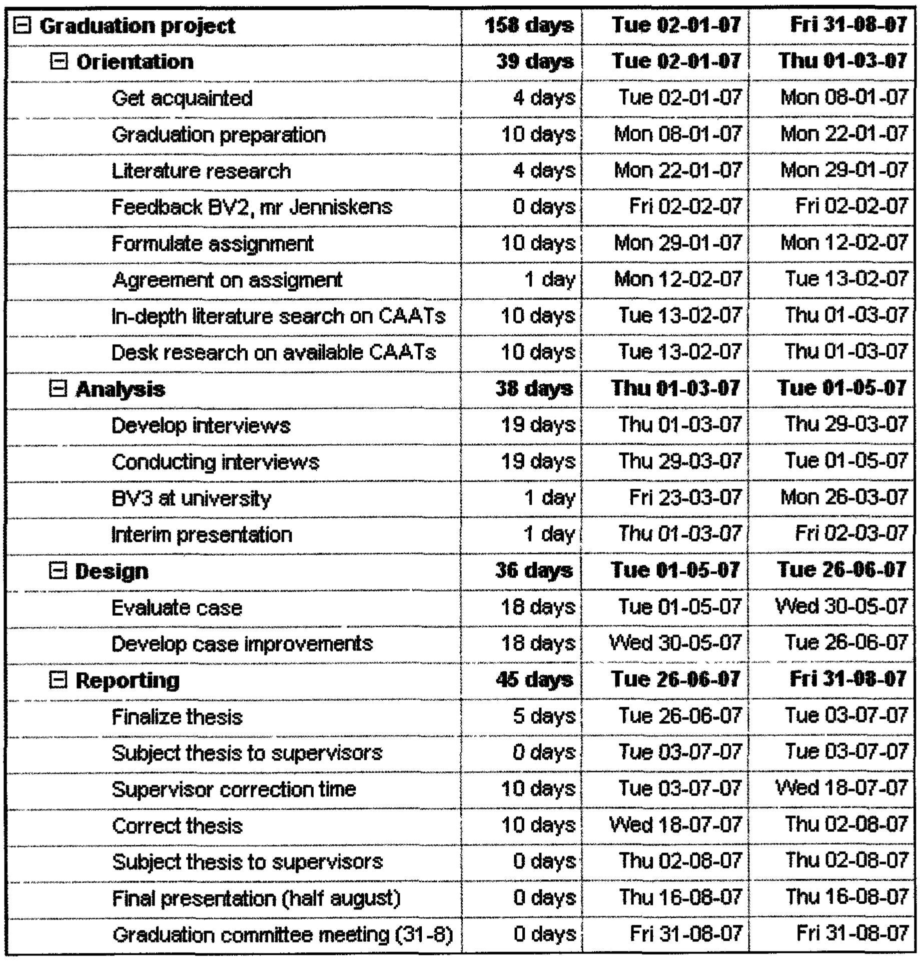
Deloitte Enterprise Risk Services

Investigating the application of process mining for auditing purposes

Appendices

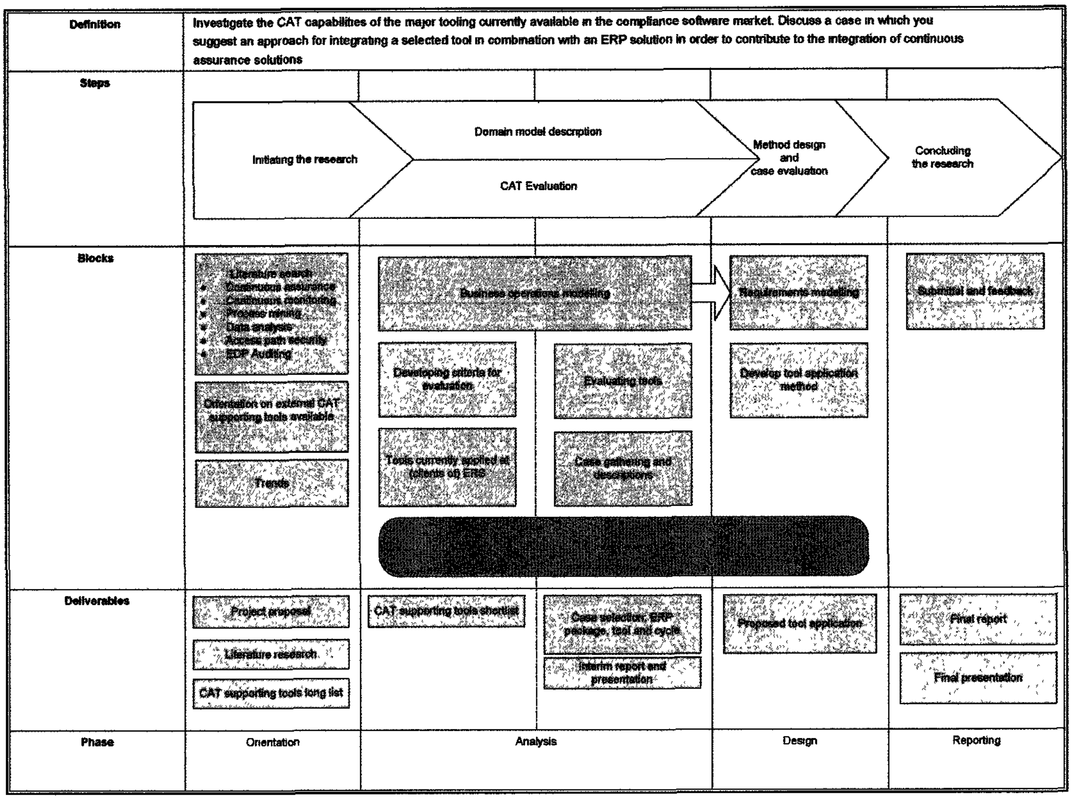
Appendix I: Project planning and schematic represenatation

Figure 28: Planning overview



⊟ **Graduation project**	**158 days**	**Tue 02-01-07**	**Fri 31-08-07**
⊟ **Orientation**	**39 days**	**Tue 02-01-07**	**Thu 01-03-07**
Get acquainted	4 days	Tue 02-01-07	Mon 08-01-07
Graduation preparation	10 days	Mon 08-01-07	Mon 22-01-07
Literature research	4 days	Mon 22-01-07	Mon 29-01-07
Feedback BV2, mr Jenniskens	0 days	Fri 02-02-07	Fri 02-02-07
Formulate assignment	10 days	Mon 29-01-07	Mon 12-02-07
Agreement on assigment	1 day	Mon 12-02-07	Tue 13-02-07
In-depth literature search on CAATs	10 days	Tue 13-02-07	Thu 01-03-07
Desk research on available CAATs	10 days	Tue 13-02-07	Thu 01-03-07
⊟ **Analysis**	**38 days**	**Thu 01-03-07**	**Tue 01-05-07**
Develop interviews	19 days	Thu 01-03-07	Thu 29-03-07
Conducting interviews	19 days	Thu 29-03-07	Tue 01-05-07
BV3 at university	1 day	Fri 23-03-07	Mon 26-03-07
Interim presentation	1 day	Thu 01-03-07	Fri 02-03-07
⊟ **Design**	**36 days**	**Tue 01-05-07**	**Tue 26-06-07**
Evaluate case	18 days	Tue 01-05-07	Wed 30-05-07
Develop case improvements	18 days	Wed 30-05-07	Tue 26-06-07
⊟ **Reporting**	**45 days**	**Tue 26-06-07**	**Fri 31-08-07**
Finalize thesis	5 days	Tue 26-06-07	Tue 03-07-07
Subject thesis to supervisors	0 days	Tue 03-07-07	Tue 03-07-07
Supervisor correction time	10 days	Tue 03-07-07	Wed 18-07-07
Correct thesis	10 days	Wed 18-07-07	Thu 02-08-07
Subject thesis to supervisors	0 days	Thu 02-08-07	Thu 02-08-07
Final presentation (half august)	0 days	Thu 16-08-07	Thu 16-08-07
Graduation committee meeting (31-8)	0 days	Fri 31-08-07	Fri 31-08-07

Figure 29: Schematic representation of the research



Definition

Investigate the CAT capabilities of the major tooling currently available in the compliance software market. Discuss a case in which you suggest an approach for integrating a selected tool in combination with an ERP solution in order to contribute to the integration of continuous assurance solutions

Steps
Initiating the research
Domain model description
CAT Evaluation
Method design and case evaluation
Concluding the research
Blocks
Literature search
Continuous assurance
Continuous monitoring
Process mining
Data analysis
Access path security
EDP Auditing
Orientation on external CAT supporting tools available
Trends
Business operations modelling
Developing criteria for evaluation
Evaluating tools
Tools currently applied at (clients of) ERS
Case gathering and descriptions
Requirements modelling
Develop tool application method
Submittal and feedback
Deliverables
Project proposal
Literature research
CAT supporting tools long list
CAT supporting tools shortlist
Case selection, ERP package, tool and cycle
Interim report and presentation
Proposed tool application
Final report
Final presentation
Phase
Orientation
Analysis
Design
Reporting

Appendix II: Additional information on the principal

II.1 Founders

William Welch Deloitte

William Welch Deloitte was one of the fathers of the accountancy profession. Deloitte, a grandson of a Count de Loitte, started his career at the age of 15. He became an assistant to the Official Assignee at the Bankruptcy Court in the City of London where he learned the business. In 1845, at the age of 25, Deloitte opened his own office opposite the Bankruptcy Court in Basinghall Street. Three momentous Companies Acts created joint stock companies, laying the foundation for modern company structures, and Deloitte was in his element. As president of the newly created Institute of Chartered Accountants, Deloitte found a site for its headquarters in 1888. In 1893, he opened offices in the United States and soon after started to audit a growing soap and candle business. Over a century later, Procter & Gamble is still a client. In 1952, Deloitte's firm in the United States merged with Haskins & Sells.

George Touche

Financial disasters in the new and booming investment trust business gave George Touche his business opportunity. His reputation for flair, integrity, and expertise brought him a huge amount of work setting these trusts on the straight and narrow. A similar flair for saving doomed businesses from disaster and restructuring them led to the formation of George A. Touch & Co. in 1899. In addition, in 1900, along with John Niven, the son of his original Edinburgh accounting mentor, he set up the firm of Touche, Niven & Co. in New York. Offices spread across the United States, United Kingdom and Canada. Meanwhile Touche himself took his reputation for probity to the electors, became MP for North Islington in 1910, and was knighted in 1917. He died in 1935.

Nobuzo Tohmatsu

After Tohmatsu qualified as a certified public accountant at the age of 57 in 1952, he became a partner in a foreign-affiliated accounting firm and a director of a private corporation. In 1967, he became president of the Japanese Institute of CPAs. The key to Tohmatsu's growth was the decision to send a substantial number of partners and professional staff overseas to gain experience. From the beginning, this meant the firm was internationally focused, and it is reflected in its long-standing international clients.

II.2: Deloitte ERS Service Industries and Competency Groups

A couple of years ago industry programs have been implemented at Deloitte ERS in order to facilitate industry specific knowledge provided by the different competency groups to reinforce their competitive position by focussing more on specific client needs. These industry programs are specifically designed for the following industries:

- Aviation & Transport Services
- Consumer Business
- Energy & Resources
- Financial Services
- Life Sciences & Health Care
- Manufacturing
- Public Sector
- Real Estate
- Technology, Media & Telecommunications

In the multidisciplinary world of risk management and control, Deloitte ERS delivers broad services at every level of a company. It provides services in the form of expert strategic, functional, and operational support and implementation. Five service groups, also called competency groups, provide these services:

- Risk Consulting/Internal Audit (RC/IA)
- Control Assurance (CA)
- Security Services Group (SSG)
- Data Quality & Integrity (DQI)
- Web services

(a) Risk Consulting/Internal Audit (RC/IA)

Risk Consulting / Internal Audit helps clients establish sustainable, internal capability to identify, assess, and manage risks to the achievement of their objectives, and the integrity and effectiveness of their processes. The participative approach develops ownership, accountability, and the support of each department and business unit in the organization. It builds an end-product that helps organizations manage risks to the achievement of their objectives within a simple-to-understand risk framework. Risk frameworks map an organization's universe of risk and control, including strategic, operational, financial, and compliance risks. Using the combination of structured risk frameworks, workshops, awareness programs, reporting and accountability processes, RC/IA enthuse and enable people - from members of the Board and management, to front line employees, team leaders, and supervisors - to develop a sustainable capability to assess and manage risk and control across an organization.

(b) Control Assurance (CA)

Control Assurance helps clients to identify, develop, and test internal control policies and procedures within business process and information technology environments. CA provides these services as part of a stand-alone audit or audit of financial statements, or as part of individual projects following from major organizational changes or implementation of new technologies. Work is often done in conjunction with ERS and Deloitte consulting service lines. Control Assurance reviews design and operating effectiveness of general IT controls and application controls. This is done by providing monitoring and independent assessment. By pursuing a value-added audit strategy, CA is able to identify new or more effective controls as a result of changes in client's system or technology, and to identify more efficient, automated controls that are designed to eliminate or reduce manual effort. Specific knowledge areas for the competency CA are methodologies like ITIL and COBIT.

(c) Security Services Groups (SSG)

SSG provides customers with an end-to-end service offering that addresses the organization's need to better assess and manage risk in IT-environments. They typically provide IT security services such as application security, IT-infrastructure security and attack and penetration testing. Implementing effective security can help drive down costs by reducing accidental errors and deliberate errors such as fraud and is therefore of the main focus points for SOX. The Security Services Group is divided into two subgroups. Application Integrity (SSG-AI) mainly focuses on business processes as it provides end-to-end integrity of business transactions and enables the effective use of new technologies. It includes security and controls in ERP and e-Business application implementations, including SAP, Oracle, PeopleSoft, and JD Edwards. SSG can help clients achieve adequate risk management within their ERP environment by providing:

- An assessment of the ERP environment, focusing on business process and security controls and providing practical recommendations as to how to remedy deficiencies identified in these areas.
- Design and implementation of business process and security controls as part of an ERP implementation.
- Reengineering of business process and security controls after an implementation has occurred.

Technology Infrastructure (SSG-TI) is a technical oriented group of professionals that has a primary focus and knowledge expertise on the security of Operating Systems, Databases, Networks, and Firewalls. They support application integrity with in depth knowledge on technical issues.

(d) Data Quality & Integrity (DQI)

The mission of the DQI group is to apply mathematical and statistical expertise and software skills to assist clients in questions relating data by providing effective and efficient methods and tools. DQI has the statistical expertise to advice auditors to decide on the benefits of a statistical approach to their audit as a whole and to apply tools and techniques that are fit to, effectively and efficiently, provide the required audit assurance and evidence.

(e) Web Services

Deloitte INVision is an advanced Internet platform designed to provide clients with key insights into processes, systems, and trends. It effectively and safely transforms data into transparent and accessible information. Both small and large companies successfully use Deloitte INVision solutions for:

- Audits: supports audits by capturing and linking all relevant audit information:

- Risk management: determine and manage business risks and meet the Basel II risk management requirements
- Corporate Governance and Internal Control implementation: be consistent with the policies and procedures as outlined by COSO and Tabaksblat
- Compliance: comply with regulatory requirements such as SOX
- Benchmarking: measures client's company's performance
- Surveys: create questionnaires and process them efficiently and reliable.

The Deloitte INVision platform is an innovative framework enabling the retrieval, sharing, and analysis of data through the Internet. The flexible platform architecture allows for fast development and deployment of new tailor-made solutions.

Appendix III: the COSO framework

(from www.coso.org)

The Committee Of Sponsoring Organizations (COSO) of the Treadway Commission was originally formed in 1985 in the US to sponsor the National Commission on Fraudulent Financial Reporting. This is an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions. COSO is dedicated to improve the quality of financial reporting through business ethics, effective internal controls and corporate governance. COSO is considered the 'de facto' standard in the world nowadays, for the goal mentioned above. The PCAOB refers to this as follows: (PCAOB, 2004)

> Management is required to base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework established by a body of experts that followed dueprocess procedures to develop the framework. In the United States, the Committee of Sponsoring Organizations ("COSO") of the Treadway Commission has published Internal Control Integrated Framework. COSO's publication (also referred to simply as COSO) provides a suitable framework for purposes of management's assessment

COSO distinguishes three internal control area's. In the COSO framework, internal controls are designed to assure:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with laws and regulations.

The internal-control-integrated-framework consists of five components. Monitoring, Information & Communication, Control Activities, Risk Assessment and Control Environment. These five component are/must be designed to ensure the reliability of the three internal control areas mentioned earlier. Additionally, COSO recognizes that these components can be active at different organizational levels. COSO internal controlintegrated- framework is depicted in figure 34. Thereupon the five components will be explained briefly to get a grip on their specific meaning and goal.

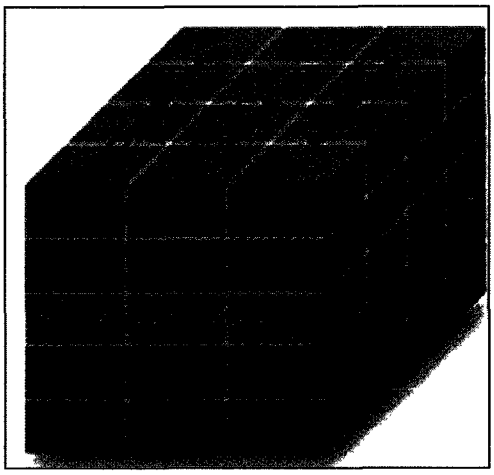


Figure 30: Internal Control - Integrated Framework

Control Environment – The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of

directors.

Risk Assessment – Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Control Activities – Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Information & Communication – Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

Monitoring – Internal control systems need to be monitored by viz. a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board. There is synergy and linkage among these components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons. Internal control is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise. 'Built in' controls support quality and empowerment initiatives, avoid unnecessary costs and enable quick response to changing conditions. There is a direct relationship between the three categories of objectives, which are what an entity strives to achieve, and components, which represent what is needed to achieve the objectives. All components are relevant to each objectives category. When looking at any one category – the effectiveness and efficiency of operations, for instance – all five components must be present and functioning effectively to conclude that internal control over operations is effective.

The internal control definition – with its underlying fundamental concepts of a process, effected by people, providing reasonable assurance – together with the categorization of objectives and the components and criteria for effectiveness, and the associated discussions, constitute this internal control framework.

Appendix IV: The Deloitte ERM approach

In this part the ERM practice of Deloitte will be described. The Deloitte approach is based on five steps that make up the whole risk management process.

Step 1: Identify Risks

The identification of risks is done through internal interviews with middle and higher management, desk research and a workshop. During this identification both the internal as well as the external environment is being considered. The questions asked are about what management considers the most important risks to achieve their goals in the upcoming year(s). Taking the goals and missions as a starting point, risks are events that are a potential danger for the achievements of these goals. Normally a time period for one or two years is considered. Important to remember is the fact that risk is a deviation from a goal and therefore has two sides: a down-side risk is a potential negative outcome and an upside-risk is a potential positive outcome (Groenland 2005).

Step 2: Prioritize Risks

After the identification of a comprehensive set of risks, the risks must be prioritized. This is done during a workshop in which the top risks are identified or by using an internet application. Prioritizing in a workshop is done by voting. During the risk assessment workshop, senior management vote on the likelihood that a risk will occur and on the impact that the risk will have on the organization. Because the voting process is executed with the facilitation of software, the participants can not influence each other. First the participants rank the risk on the likelihood of occurrence. This is measured on a scale from one to nine, with a one indicating a very low likelihood and nine indicating a very high likelihood. This process is repeated for the impact a risk can have on organizational goals. The same process of prioritizing the risks is also being executed with an internet application. Deloitte has an in-house developed internet platform called Survey Web. With this application surveys are easily being built and put online, all in a secure environment. The same voting process can be done with this application and is anonymous. This way the respondents can not influence each other which in turn provide more objective data. An outcome of this process is a risk map where the likelihood and impact are plotted in a matrix.

During a typical risk assessment conducted by Deloitte, the existing control effectiveness in an organization is also taken into consideration. Assessing the control effectiveness is similar to the assessment of the risks. Instead of voting about the impact and likelihood of the risk, the level of control is identified. This way the residual risk is identified. When there is a risk with a high score on impact and likelihood, but there is a high level of control effectiveness, there will not be a big problem for the organization. The only action a company should take is to get assured that their controls are really effective against the risk. If a top risk is identified that has high impact/likelihood but the control effectiveness is low, action should be taken change this. In the situation that the risk and the level of control effectiveness are low, the company should only monitor these risks to make sure the situation is not changing. Another situation is overcontrol. In this situation effective controls are in place, but the significance of the risk is low. This can be an indication that the company is putting to much effort in controlling a certain type of risk and it might be wise to evaluate the control to see if control efforts can be focused on other risks. The four possible scenarios are presented in the control effectiveness/risk significance matrix.

Step 3: Analyze Root Causes

Sourcing helps in determining action strategy and steering based on cause-and-effect analysis.

Step 4: Develop Risk Strategies

There are several risk strategies which can be developed. In his book Doherty (2000:5) identifies four different actions toward risk. He states that risk can be: 1. Transferred to a counter-party by purchase of an insurance policy or financial hedge. 2. Retained in either an active or passive way. Simply not insuring is retaining risk. But the firm can mimic the insurance process by self insuring with internal pricing, reserving, and loss settlement. 3. Reduced by investing in sprinklers, smoke alarms, inspections and other safety measures. 4. Avoided by not undertaken activities that are risky or by substituting less risky processes. According to Amato and Eysink (2005), Shell uses a comparable classification of actions toward risk: Take, Treat, Transfer, Terminate. The real foundation for the development of risk management strategies is to understand why risk is costly to the firm in the first place (Doherty, 2000). When risk is costly to the firm it will destroy income and thus will have a negative effect on shareholders value. Not only understanding the risks, but also being able to form a strategy to counter these risks, will create value for the firm. The strategy to treat risk will result in the creation of internal controls or other actions to diminish either the likelihood or the impact for the organization. This can be done by taking actions so that the company can be assured that it will be unlikely that a risk will happen. An example is being compliant to government rules. If a company investigates their compliancy following new rules and regulations, it can judge the potential problems that can arise in the future and by doing so avoid penalty fees or worse, shutdown of operations. If a company knows it is not compliant, it can change this by restructuring and therefore diminish the likelihood of this risk drastically. Another good example on how to diminishing the impact of a potential risks is about the supply of raw materials. If a company has just one supplier to rely on for its raw materials, the dependency on this supplier is big. If this supplier stops delivering its raw materials, the company must stop its operations. By exploring the possibility to buy raw materials from other suppliers will diminish the dependency and therefore the impact of this risk.

Step 5: Implement and Monitor

- There are a few important elements to have Risk Management successfully embedded in the current management structure (Demneri 2005).
- Define a risk management policy and specific guidelines within which the Risk Management will be executed aligned with the existing business policies.

- A common risk language contributes to a common understanding and communication of risks across the organization (Funston 2003:59-63).
- Establish a structure with the purpose to define and communicate the accountabilities for managing risks in a structured manner.
- Develop a risk management process. This to identify, prioritize and act upon risks on a continuous basis and in an integrated manner with other business activities aligned with the planning and control cycle.
- Enhance management reporting with the purpose to provide management with information on risks, "what if" scenarios and trends in risk causes as part of the regular management reporting.
- Develop supporting tools to support the execution of the process, generation of reporting and communication.
- Progress of Risk Management and its implementation has to be monitored for a clear status for internal and external responsible.
- Risk Management is an ongoing and iterative process. Trends and new risk scenario's have to be mapped for timely intervention and anticipation.

Appendix V: Software description and evaluation

ACL Continuous Controls Monitoring

ACL Continuous Controls Monitoring (CCM) combines the flexible and powerful data analytic capacity of ACL with developing and implementing a control framework. ACL CCM conducts point-in-time analysis and interrogation of data performed during traditional audit reviews, incorporate additional sophisticated analytics, and embed them in an organization's day-to-day operations. Run automatically on a continuous basis, ACL CCM solutions identify suspicious activity, errors, and exceptions that may be disguised through the structuring and processing of transactions over time or hidden within high data volumes. After designing the framework, where parameters such as the entity level, the queries, the required datasets, the period of time and frequency of test running is determined, the system is operational. CCM uses a copy of the database and executes the analytics, after running the results are presented in an exception report. The first advantage of ACL CCM is that flexible custom made tests can be developed, varying for example from a deviating stock levels to suspect double salary payments to an employee. The second advantage is that the tests can be automated, requiring less human intervention except for the review of the exception reports. ACL services multiple platforms including ERP Systems such as Oracle and SAP and legacy systems. Tests can only be designed during implementation, so care must be taken that during the implementation phase all required tests are incorporated. We conclude that ACL CCM has strong automated testing functionality and strong data analytics. The approach is data focuses, the application is not process aware. Process mining is a technique which has not been used in this application.

Applimation Integra Apps

Applimation Integra Apps is a controls solution suite specifically designed for Oracle and Peoplesoft. It has measures to prevent segregation of duties violations and unauthorized changes to sensitive data, code and objects. It typically comes along with standard tests, these can be slightly configured but it does not offer the flexibility that ACL CCM does in designing custom tests. Because of the Oracle and Peoplesoft focused approach, Integra Apps is a very strong package in terms of preventive SOD and GCC controls in that field. When controls are correctly set up, these tests can be automated. In terms of user controls, Approva does provide a framework where results of control tests can be recorded. The specific data analytics are not supported in Approva. Approva also does not use process mining capabilities to test controls.

Approva Enterprise Controls Management Solution

The Approva Enterprise Controls Management Solution is split up in three parts. The BizRights Platform is the unified platform for addressing enterprise wide-controls business controls. In contrast with Integra Apps, Approva made the decision to be broadly oriented. It's solutions support several ERP vendors' solutions using standard adapters, but custom made adapters can be developed by the companies' consultants. The Application Controls Suite aids in managing application access and security controls, including aspects such as segregation of duties, user activity, configuration settings. The Process Controls Suite monitors business processes, giving insight a.o. in the financial closing, procurement-to-pay cycle and the order-to-cash cycle. Although the tests can be automated, Approva comes with a predefined set of tests and it is not possible to develop custom tests. Data analytics are not possible and process mining is not supported.

ARIS Process Performance Manager

The ARIS Process Performance Manager (PPM) is part of the ARIS platform, a Germany-based software vendor specialised in modelling and redesigning business processes. ARIS PPM is the only commercial package explicitly employing process mining. PPM is coupled to ERP systems using XML adapters and is able to chart the running processes, even across different ERP packages and legacy systems. Using this interface, benchmarks can be executed such as the throughput time of order to delivery, categorised to sales districts. Here the advantage of process mining in performance management becomes clear, because throughput times are statistics with which data analytics has trouble to identify (van der Aalst, 2005). PPM server uses a relational SQL database to import runtime data. The intervals of data import can be determined by the user. Historic data is compressed and archived. This repository can be seen as a warehouse. When a client is acquisitioning PPM, ARIS consultants come in and identify the business processes under scrutiny. These are modelled in the ARIS BPM modelling language (EPC) and the XML adapters are defined. That means that process instances and transition activities are generally fixed, an assumption that is valid in a stable business process environment. A disadvantage is that when the process undergoes big changes, for example, when new process activities and new process instances are introduced to the system. In that case, PPM will have to be reconfigured because the XML adapter does not fit the ERP software anymore.

BWise

The Bwise application includes testing of key controls to be executed by business managers or internal auditors. The testing functionality includes scheduling of control testing, as well as the documentation save function and auditable storage of collected evidence. Bwise offers amongst others a COSO and CobiT template. The package enables policy and procedure development and maintenance. It provides support for modelling business processes. BWise does not offer workflowmanagement support and no process mining abilities. Although an interface is developed and tested for active control monitoring, this does not belong to the main functionality of BWise and is very limited. Furthermore, a repository with standard test methods comes along with BWise, but data analysis techniques are not supported in BWise. The results of data analysis techniques mainly have to come from other tools.

eQsmart

eQsmart is an internally developed tool used for testing certain control objectives in SAP. This tool loads the configuration settings and issues a report regarding the status of the settings in SAP. Using control objectives, specific queries can be loaded and the control objective is tested. An example of a typical control objective that is tested using eQsmart, is the status of SOD issues in SAP. Conflicting transaction codes can be input and then a list of users can be generated who have access to a set of transaction codes which are conflicting. This tool is custom made for SAP and focuses on security settings which are in effect at the moment the data is extracted. eQsmart does not take into account the history of the configuration. A malicious user could change his access settings, do bad things and change everything back. eQsmart will not detect this deviation.

Hyperion System 9

Hyperion was recently acquisitioned by Oracle. That means that Hyperion lacks multi-platform applicability. Hyperion is mainly focused on business analytics. System 9 has several modules. System 9 Foundation Services is the meta application for implementing the several System 9 modules, including BPM Architect for modelling business processes, Workspace the web interface and Shared Services, a framework to centrally create and maintain users and access security. The rest of the modules are Financial Applications, Business Intelligence and Data Management Services. Enterprise Analytics forms the data analysis side of System 9, providing very powerful OLAP functions tailored to the clients needs. Enterprise Metrics is the dashboard functionality of System 9, delivering KPI's online to the clients need. Concluding, System 9 delivers strong online data analytics. The data analytics of Hyperion could be used for compliance and testing of controls purposes. However, hyperion does not supply a control framework for risk and control assessment.

OpenPages

OpenPages develops enterprise governance, risk and compliance management (GRCM) solutions that optimize internal controls, reduce risk exposures and empower effective corporate oversight. OpenPages Governance Platform contains a suite of modules for Financial Controls Management, Operational Risk Management, IT Governance and General Compliance Management. OpenPages solutions improve corporate accountability, reduce disclosure process costs, assure organizational performance and increase stakeholder confidence via a unified system of record for every significant process, risk and control throughout the enterprise. The company's portfolio of solutions includes SOX Express, the market-leading enterprise application for automating the compliance requirements of Sections 404 and 302 of the 2002 Sarbanes-Oxley Act, and OpenPages ORM, an enterprise risk management software solution that enables entities to identify, analyze and manage operational risk on an integrated, company-wide basis. OpenPages FCM claims to be the market-leading software solution for compliance with the Sarbanes-Oxley Act and similar worldwide financial reporting regulations. It automates an organization's entire compliance lifecycle – from design and documentation, through test, review, approval and certification. Combining full document management, powerful workflow and interactive reporting capabilities, OpenPages FCM makes compliance procedures more efficient while providing executive management with assurance that the organization is meeting its compliance requirements. Although the compliance lifecycle is automated, data analysis is not supported and process mining is not employed. Automated testing of controls is currently not possible.

Paisley Enterprise GRC and GRC on Demand

Paisley has two service offerings, Enterprise GRC and GRC on Demand. The latter is tailored for mid-sized clients. Also Paisley advocates a top down approach. Manual recording of risk and controls status is allowed, not automated tests can be run. They talk about a "process level risk assessment approach that analyzes business processes across the organization", but unfortunately, as with a lot of the vendors, the exact workings of this proposition remains a big mystery. Paisley Enterprise GRC provide the basic GRC functionality encountered at all the software inspected, which is comprehensive audit management functionality with risk assessment, planning, scheduling, preparation, review, report generation, global issue tracking and administration functionality. It also enables the sharing of audit findings, key risk areas, and recommendations across the compliance, IT governance and risk management processes. No automated tests can be run and data analyses is not supported within the tool, except for the recording of test results generated with external data analysis software.

Protitivi Governance Portal

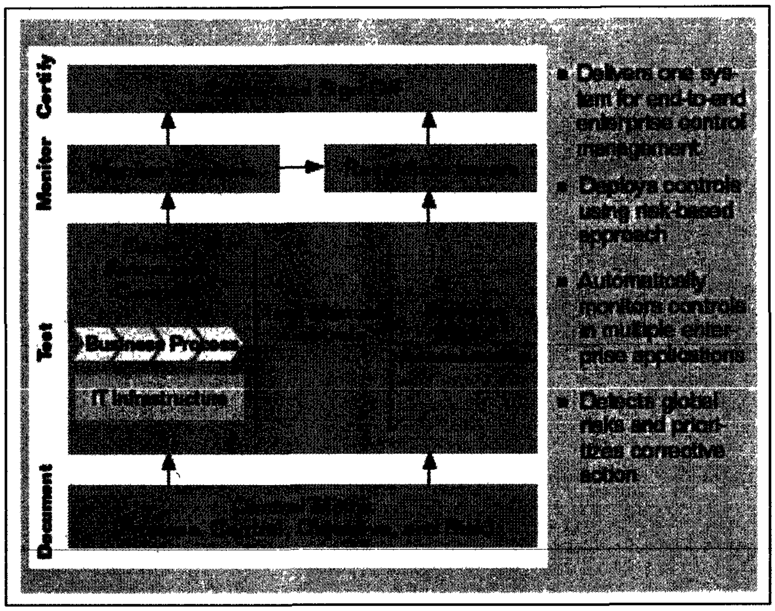
Protiviti's approach assists organizations in building a sustainable assessment process. The Protiviti Governance Portal™ (PGP) is a web-enabled process and knowledge management solution designed to improve corporate governance, comply with Sarbanes-Oxley requirements, and enhance business performance. Its extendible framework also provides a strategic platform for broader compliance, governance and risk management initiatives. The PGP provides a complete framework to facilitate the documentation, testing, and mitigation activities to manage all phases of a Sarbanes-Oxley compliance program. Protiviti has a partnership with TIBCO, a workflow management software vendor. TIBCO provides a software infrastructure that is capable of extending the compliance program throughout the enterprise. By integrating TIBCO's workflow management system with the PGP, clients establish structure in the risk mitigation process by alerting management of all process exceptions and utilizing a proven framework in which gaps are reviewed, mitigated and closed. The extended features offered through TIBCO provide an enterprise backbone for messaging, monitoring, and event management. Specifically, organizations have the ability to track system changes and monitor key risks across multiple platforms including ERP systems, firewalls, and intrusion detection systems. Such events may trigger advanced workflow, update PGP details, and populate a real-time dashboard. The PGP SarbOx Portal assists the client in risk and control assessment, structuring test programs, and recording control status. No mention is made of automated testing capabilities, nor integration with external vendors. The interesting part of the Protiviti solution is the workflow oriented approach of compliance procedures. Although workflow management is used to coordinate the compliance-related business process, process mining is not used to analyze business processes at the client itself.

SAP GRC Process Control

SAP provides an integrated suite called SAP GRC. This solution contains three areas: Governance, Risk and Compliance. Each area contains several modules. The Compliance area consists of five modules:

- SAP GRC Access Control
- SAP GRC Process Control
- SAP GRC Global Trade Solutions
- Sap Applications for environmental compliance
- GRC Composite applications by SAP and Cisco

The SAP GRC Process Control application allows the automation of monitoring, testing, assessment, remediation, and certification of enterprise-wide business processes. Visibility into business process controls is gained to ensure that they are operating as designed and that the data that is reported to regulatory bodies can be trusted. SAP GRC advocates continuous monitoring of controls using automated testing. Data analysis is not part of the module and process mining is not applied.



- Delivers one system for end-to-end enterprise control management
- Deploys controls using risk-based approach
- Automatically monitors controls in multiple enterprise applications
- Detects global risks and prioritizes corrective action

Figure 31: SAP GRC Process Control

SAS Enterprise Intelligence

SAS is propositions the same selling principles as Hyperion. It identifies the need of timely and high quality information, generated from data extracted from several data sources such as ERP systems and legacy software. In this sense, SAS is not a GRC solution, but an Enterprise Management Dashboard. SAS has strong data analytic capabilities, but does not use process mining concepts. SAS also does not use a risk and control framework and no automated testing of controls.

Appendix VI: Overview COMET methodology

Adapted from: (Berre *et al.*, 2004)

The COMET methodology involves building a set of models and their associated work products, following the iterative and incremental process paradigm. Except for some work products in the business model and the other requirement work product, the work products are UML-based, and each work product is presented with one or more UML diagrams. Figure 32 depicts this and shows the Development Process in a nutshell.

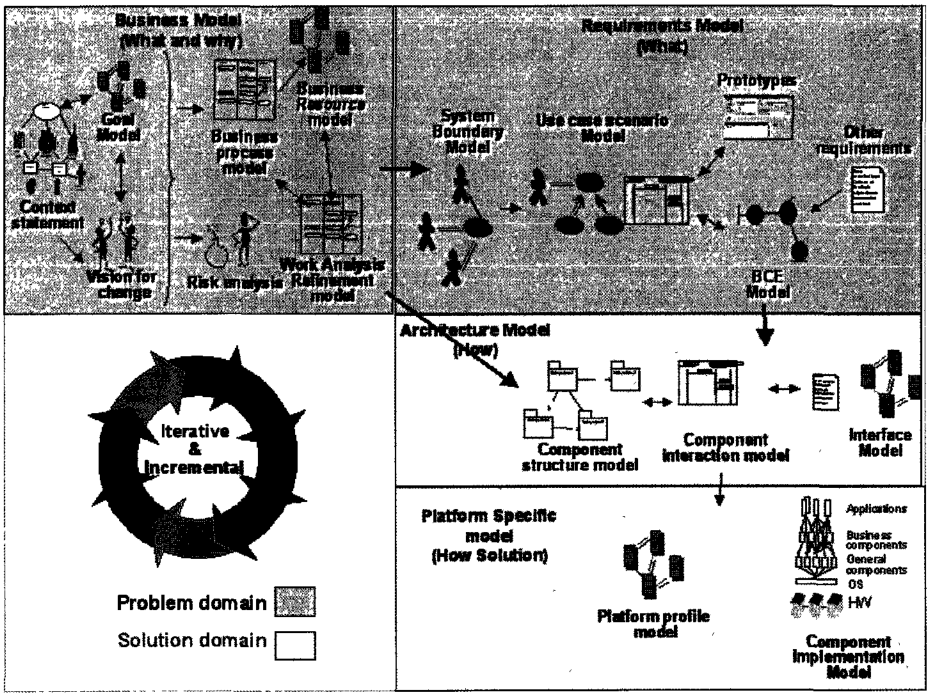


Figure 32: COMET Development process in a nutshell

The figure shows all Component Centre development process work products. The icons indicate the associated UML diagram(s) or nature of deliverable for each work product and the arrows show the most common path through the set of work products within an iteration.

Starting from the upper left we have the Business model which includes the context statement, vision for change, and risk analysis as well as more formal models of the goals, processes & roles and business resources. The icons indicate use of UML class diagrams for modelling goals and business resources, and UML activity graphs and collaborations for modelling business processes and roles. The Work Analysis Refinement model (WARM) is a refinement of the business process & roles model to identify the required behaviour of the Product under development.

In the Requirements model, the use case diagrams are associated with both the system boundary model and the use case scenario model. UML sequence diagrams or activity graphs are used for detailing the use case scenarios. Prototypes might be might be developed for various reasons, such as HCI mock-ups, as a vehicle to get fruitful interaction with end users, or for testing the architecture etc. The Other Requirements work product is typically expressed in text. The BCE model is modelled using UML class diagram with the boundary, control and entity stereotypes.

In the Architecture model, the component structure model uses the package concept of UML and UML class diagram. The component interaction model defines the component interaction using UML sequence diagram and/or UML collaboration diagram. The interface model specifies the interface signatures, pre and post conditions for the operations and the abstract information model represented by the interface. These are modelled using UML class diagram, as well as using prose text and/or OCL.

The platform specific model is typically expressed using UML class diagram and programming languages as well as documentation in various forms (user manual, reference guide, comments within the code etc).

Appendix VII: Expenditure control objectives for PM

In this appendix, we will discuss which control objectives of the expenditure cycle are feasible for process mining and which are not.

Maintaining supplier master file

Only valid changes are made to the supplier master file: in order to enforce this control objective, it has to be determined which changes are valid and which are not. Valid changes are those which are made by users that are authorized make them. Verifying if the ERP authorized personnel is also organizationally legitimate is done by comparing authority clearance from the organizational model with the users available in the ERP system. This part can not be tested using PM. PM can be used to verify if users exist who changed master files but are not authorized to so, by comparing the originators in the change master file log with the list of users authorized to change the master files

All valid changes to the supplier master file are input and processed: changes to master files have to be compared against manual logs of change request. This information is not recorded in the ERP data and can not be verified using process mining

Changes to the supplier master file are accurate: the same as above, changes to master files have to be checked with (manual) source documents which renders the control infeasible for checking with process mining

Changes to the supplier master file are processed timely: reports of changes to vendor master records have to be compared to authorized source documents and/or a manual log of requested changes to ensure that all valid changes were input accurately and timely, not feasible for process mining

Supplier master file data remains pertinent: reports of changes to vendor master records have to be compared to authorized source documents and/or a manual log of requested changes to ensure that all valid changes were input accurately and timely, not feasible for process mining

Purchasing

Purchase orders are placed only for approved requisitions: this control can be checked using process mining. A requisition can be approved using an ERP release strategy and manually by persons who are approved to do so. Users who approved requisitions can be compared against a list of users who are authorized to approve purchase requisitions

Purchase orders are entered accurately: purchase order entries have to be compared to authorized source documents and/or a manual log to ensure that all purchase orders were input accurately and timely, not feasible for process mining

Processing accounts payable

Amounts posted to accounts payable represent goods received: usually, the ERP packages restricts to authorized personnel the ability to input vendor invoices that do not have a purchase order and/or goods receipt as support. PM can be used to check if the log contains a goods receipt that does not refer to a purchase order.

Amounts posted to accounts payable represent services received: usually, the ERP packages restricts to authorized personnel the ability to input vendor invoices that do not have a purchase order and/or goods receipt as support. PM can be used to check if the log contain services which were not signed of against a purchase order

Accounts payable amounts are accurately calculated and recorded: calculation of accounts payable is dependent on the exchange rates. These exchange rates are recorded in a master table and can only be changed by approved personnel. These changes can not verified using PM

All amounts for goods received are input and processed to accounts payable: in order to achieve this, management should proactively monitor the goods receipt/invoice receipt account. This control objective can not be tested using process mining

All amounts for services received are input and processed to accounts payable: in order to achieve this, management should proactively monitor the goods receipt/invoice receipt account. This control objective can not be tested using process mining

Accounts payable are only adjusted for valid reasons: adjustments to accounts payable must be approved by authorized personnel. PM is not able to test the control objective

Credit notes and other adjustments are accurately calculated and recorded: calculation of credit notes is dependent on the exchange rates. These exchange rates are recorded in a master table and can only be changed by approved personnel. These changes can not verified using PM

All valid credit notes and other adjustments related to accounts payable are input and processed: also this control objective can not be tested using process mining because the information does not reside in the system. Employees must be interviewed to verify all credit notes are processed.

Processing disbursements

Disbursements are only made for goods and services received: PM is able to make a match between the goods received account and the disbursements that have been made. The event log can be checked if a disbursement is made for which no matching goods receipt is present

Disbursements are distributed to the appropriate suppliers: PM could be used to verify this control objective (compare the payee with the preferred vendor). In the context of the purchasing cycle, this is not applicable

Disbursements are accurately calculated and recorded: correct calculation of disbursements must be verified using source logging and cannot be verified using PM

All disbursements are recorded: not recorded disbursements are not remarked. An event log can be inspected for redundant process instances, i.e. process instances that do not reach the end state. These could indicate reimbursements that were not recorded

SOD Controls

No cash disbursements can be made to own account (vendor master and bank payments): PM could be used to compare employee bank accounts and vendor bank accounts. A simple query is better suited

No fictitious purchase orders and receipt can be processed (purchase order and goods receipt): PM can be used to inspect if the log contains audit trail entries where the originator of both activities matches

No purchase orders to unauthorized vendors can be made (purchase order and vendor master): PM is not applicable. Rather, the purchase orders should be inspected to check if the order is issued to a vendor is used that is not specified in the master data

No user can purchase an item, mark it as received and enter and pay the invoice (purchase order and vendor master): PM can be used to check if the originators of the activities issue purchase order, goods receipt and invoice payment are the same

No entry of a fictitious vendor, purchase order and goods receipt can be made (vendor master, purchase order and goods receipt): PM can be used to check if the originators of the activities create or change vendor master data, create purchase order and goods receipt are the same

Appendix VIII: LTL language applied to M-XML

The notation `ate.x` is used to refer to some attribute of an audit trail entry (`ate`) i.e. an event in an event log. `pi.x` is used to refer to an attribute of a process instance (pi). Several predefined attributes exist, `ate.WorkflowModelElement` refers to the activity (or other process elements) being executed. `ate.Originator` is the resource executing it. `ate.Timestamp` is the timestamp of the event. `ate.Eventtype` is the type of the event (schedule, start, complete, reassign etc.). The first 7 lines define the attributes and their domains. The rename function is used for easy scripting. The formula function is used to define the properties to which the log should conform.

```
1 set ate.WorkflowModelElement;
2 set ate.Originator;
3 set ate.EventType;
4
5 date ate.Timestamp := "yyyy-MM-dd";
6 string ate.result;
7 string pi.title;
8
9 rename ate.Originator as person;
10 rename ate.Timestamp as timestamp;
11 rename ate.WorkflowModelElement as activity;
```

An example of a formula is as follow:

```
23 formula not_the_same_reviewer() :=
24 forall[p:person |
25 (((!(execute(p,"get review 1")) \/ !(execute(p,"get review 2"))) /\
26 (!(execute(p,"get review 1")) \/ !(execute(p,"get review 3")))) /\
27 (!(execute(p,"get review 2")) \/ !(execute(p,"get review 3")))) ];
```

This formula is applicable to a process where three reviewers should check an article for approval. This formula verifies the property if a process instance exists in the log where one person is doing more than one review of the same article, a property that is undesirable in this typical process.

For more information, read the reference manual written by article written by de Beer (de Beer, 2004).

Appendix IX: Two event logs

Table 4: Stable event log

ATE-ID	PI-ID	WFMElt	EventType	Timestamp	Originator	Amount
1	1	Create PO	Complete	8:00	Tim	
2	1	Receive invoice	Complete	13:00	Jan	1000
3	1	Receive goods	Complete	15:00	Tom	
4	1	Check goods	Complete	16:00	Tim	
5	1	Pay invoice	Complete	17:00	Jan	1000
6	2	Create PO	Complete	9:15	Tim	
7	2	Receive goods	Complete	10:15	Tom	
8	2	Receive invoice	Complete	12:15	Jan	2000
9	2	Check goods	Complete	15:15	Tim	
10	2	Pay invoice	Complete	16:15	Jan	2000
11	3	Create PO	Complete	10:30	Tim	
12	3	Receive invoice	Complete	11:30	Jan	5000
13	3	Receive goods	Complete	13:30	Tom	
14	3	Check goods	Complete	14:30	Tim	
15	3	Pay invoice	Complete	17:30	Jan	5000

Table 5: Unstable event log

ATE-ID	PI-ID	WFMElt	EventType	Timestamp	Originator	Amount
1	1	Create PO	Complete	8:00	Tim	
2	1	Receive invoice	Complete	13:00	Jan	1000
3	1	Receive goods	Complete	15:00	Tom	
4	1	Check goods	Complete	16:00	Tim	
5	1	Pay invoice	Complete	17:00	Jan	1000
6	2	Create PO	Complete	9:15	Tim	
7	2	Receive goods	Complete	10:15	Tom	
8	2	Receive invoice	Complete	12:15	Jan	2000
9	**2**	**Receive goods**	**Complete**	**13:15**	**Tom**	
10	2	Check goods	Complete	15:15	Tim	
11	2	Pay invoice	Complete	16:15	Jan	1500
12	**2**	**Pay invoice**	**Complete**	**17:15**	**Jan**	**500**
13	3	Create PO	Complete	10:30	Tim	
14	3	Receive invoice	Complete	11:30	Jan	5000
15	3	Receive goods	Complete	13:30	Tom	
16	3	Check goods	Complete	14:30	Tim	
17	3	Pay invoice	Complete	15:30	Jan	2000
18	**3**	**Pay invoice**	**Complete**	**16:30**	**Jan**	**2000**
19	**3**	**Pay invoice**	**Complete**	**17:30**	**Jan**	**1000**

Appendix X: Example LTL Control Objective

The control objective is: “No user can purchase an item, mark it as received and enter and pay the invoice”. Basically, we want to test if a user exists in the log who executed the activities “Create PO”, “Receive goods” and “Pay invoice”. The code is as follows:

```
set ate.WorkflowModelElement;
set ate.Originator;
set ate.EventType;

date ate.Timestamp := "yyyy-MM-dd";
string ate.result;
string pi.title;

rename ate.Originator as person;
rename ate.Timestamp as timestamp;
rename ate.WorkflowModelElement as activity;
```

The according formula is defined as follows:

```
formula three_way_match() :=
forall[p:person |
(((!(execute(p,"Create PO")) \/ !(execute(p,"Receive Goods"))) /\
(!(execute(p,"Create PO")) \/ !(execute(p,"Pay Invoice")))) /\
(!(execute(p,"Receive Goods")) \/ !(execute(p,"Pay Invoice")))) ];
```

Appendix XI: Overview tables and attributes

	Attribute	Atrribute description	Key	Reference Table
EBAN: purchase requisition				
	BANFN	Purchase requisition number	Yes	EBAN
	BNFPO	Item number of purchase requisition	Yes	EBAN
	MANDT	Client	Yes	T000
	BADAT	Requisition (request) date	No	
	BEDAT	Purchase order date	No	
	EKGRP	Purchasing Group	No	T024
	EKORG	Purchasing Organization	No	T024E
	ERDAT	Date of Last Change	No	
	ERNAM	Name of person who created the object	No	
	FRGDT	Purchase requisition release date	No	
	LFDAT	Item delivery date	No	
EKKO: purchase orders				
	EBELN	Purchasing Document Number	Yes	EKKO
	MANDT	Client	Yes	T000
	AEDAT	Date on which the record was created	No	
	BEDAT	Purchasing document date	No	
	BUKRS	Company Code	No	T001
	EKGRP	Purchasing Group	No	T024
	EKORG	Purchasing Organization	No	T024E
	ERNAM	Name of person who created the object	No	
	KONNR	Number of principal purchase agreement	No	EKKO
EKPO: purchase order line items				
	EBELN	Purchasing Document Number	Yes	EKKO
	EBELP	Item Number of Purchasing Document	Yes	EKPO
	MANDT	Client	Yes	T000
	ABDAT	Reconciliation date for agreed cumulative quantity	No	
	AEDAT	Purchasing document item change date	No	
	BANFN	Purchase requisition number	No	EBAN
	BNFPO	Item number of purchase requisition	No	EBAN
	EFFWR	Effective value of tiem	No	
	PRDAT	Date of price determination	No	
	RETPO	Returns item	No	
EKBE: history per purchasing document				
	BELNR	Number of material document	Yes	EKBE
	BUZEI	Item in material document	Yes	EKBE
	EBELN	Purchasing Document Number	Yes	EKKO
	EBELP	Item Number of Purchasing Document	Yes	EKPO
	MANDT	Client	Yes	T000
	BEWTP	PO history category	No	T163B
	BLDAT	Document date in document	No	
	BUDAT	Posting date in the document	No	
	BWART	Movement type	No	T156
	CPUDT	Accounting document entry date	No	
	CPUTM	Time of entry	No	
	ERNAM	Name of person who created the object	No	
	BELNR	Number of material document	Yes	EKBE
	BUKRS	Company Code	Yes	T001
	BUZEI	Item in material document	Yes	EKBE
	MANDT	Client	Yes	T000
	AUGDT	Clearing date	No	
	EBELN	Purchasing Document Number	No	EKKO

Appendix XII: Example LTL Control Objective in SAP

The control objective is: "No user can purchase an item and mark it as received. Basically, we want to test if a user exists in the log who executed the activities "Create PO" and "Goods receipt". The code is as follows:

```
set ate.WorkflowModelElement;
set ate.Originator;
set ate.EventType;

date ate.Timestamp := "yyyy-MM-dd";
string ate.result;
string pi.title;

rename ate.Originator as person;
rename ate.Timestamp as timestamp;
rename ate.WorkflowModelElement as activity;
```

The according formula is defined as follows:

```
formula two_way_match() :=
forall[p:person |
(((!(execute(p,"Create PO")) \/ !(execute(p,"Goods receipt")))];
```

Appendix XIII: Description data conversion

The goal is to create an event log which can be mined. This means the event log has to contain a case ID (the process instance ID), a workflow model element (the activity), an originator, a timestamp and an event type. As described, we inspect the orders created in March, resulting in 1892 process instances and 33587 audit trail entries.

First we take a look at the table EKKO, containing all the purchase orders orders. For the case ID the field EBELN, the purchase order number, is chosen. The activity is create purchase order. The originator is defined as the field ERNAM, or the person who created the object. Two other organizational elements are available, EKORG and BUKRS, but at Friesland Foods these are not used. 93 different originators are creating purchase orders. For the timestamp, two dates are available, the field AEDAT and the field BEDAT. AEDAT is the date of creation, BEDAT is the date of the last change (if any). We chose the field BEDAT, because this refers to the most recent information. The event type is default complete, because the activities only registration dates are available. The table EKKO has been reduced to orders with the purchase order number (EBELN) posted only in March.

The table EKPO contains all the purchase order line items. We looked up all the line items which had a purchase order number related to the selection made in the previous step. Then we added these records to the event log. The EBELN is the case ID, the activity is create PO line item. In this table, some dates are recorded, such as the reconciliation date for the cumulative quantity and the date of price determination. We are interested in AEDAT, which is the timestamp. There is no originator recorded in the table, but the originator is the creator of the associated purchase order. The activity create purchase order line item is performed 6128 times.

The table EBAN contains purchase requisitions. Purchase requisitions are not directly linked to purchase orders, but they are linked to purchase order line items, which in turn are linked to purchase orders. We looked up purchase requisitions which were associated with purchase order line items that were in our scope of March-purchase orders. Then we added the purchase order number to the purchase requisition records. Not all purchase orders are associated with a purchase requisition. And not all purchase requisitions are converted to a purchase order (yet). So only 112 Audit trail entries with the activity create purchase requisition exist.

The table EKBE contains the history per purchasing document. Again several dates are posted such as BLDAT (document date in the document) and BUDAT (posting date in the document) but the date we use is the CPUDT, the date of posting the date in SAP system. BEWTP is PO history category. This is an enumeration class, the letters in this field refer to a master data table containing the associated activities: E: goods receipt, 100427, K: account maintenance, 2094, L: Delivery Note, 5818, N: subs deb log IV, 359, Q: invoice receipt, 34058, U: Goods issue. The originator is again ERNAM.

Now that all the tables and their relations have been defined, the event log is built up in excel. Important is to consider the order and the name of the fields:

- Ate-ID (an autonumber)
- PI-ID (the field EBELN)
- WFMElt (the activity)
- Eventtype
- Timestamp
- Originator

Because we use the Access import filter, we import the event log access and use the ProM import framework to convert the event log to M-XML format. In order to convert an Access database, the root of the database must be referred in the system DSN, specify an ODBC for the Access database. Two important aspects must be considered: the format of the timestamp field must be Date/Time and the format of the PI-ID field must be Long Integer, otherwise the import framework will not function.

Appendix XIV: Process models heuristics miner

Figure 33: Heuristics process model based on unstable event log

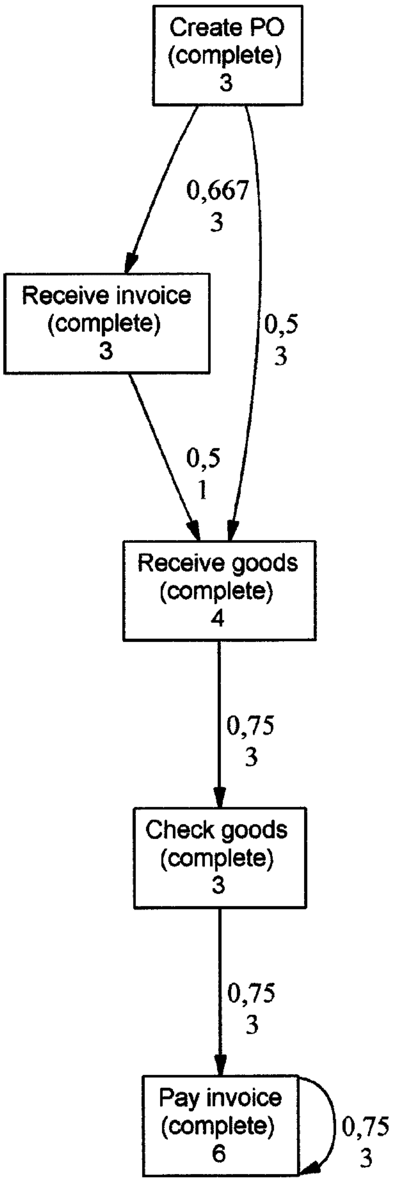


Figure 34: HeuristicsMiner process model based on event log 1, high treshold

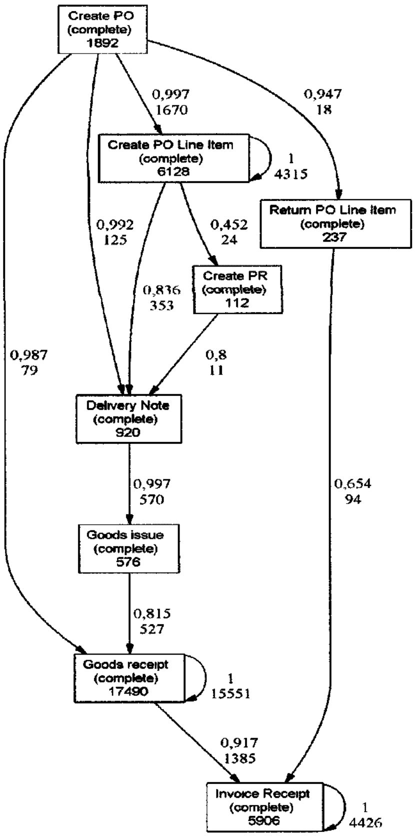


Figure 35: HeuristicsMiner process model based on event log 1, low treshold

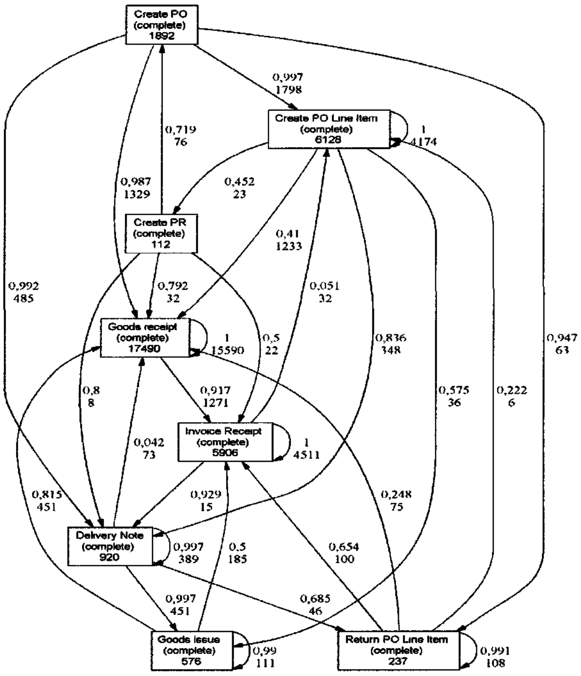


Figure 36: HeuristicsMiner process model based on event log 2, high treshold

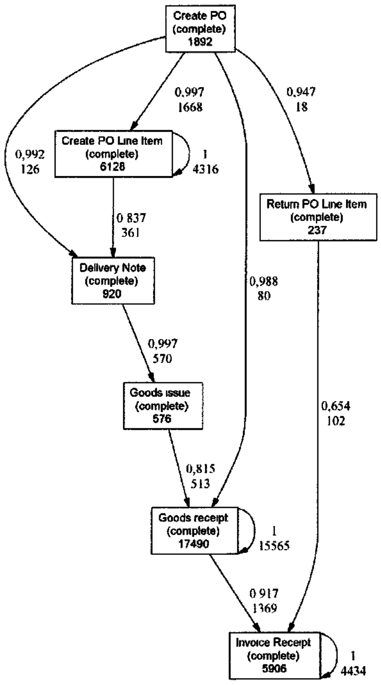


Figure 37: HeuristicsMiner process model based on event log 2, low treshold

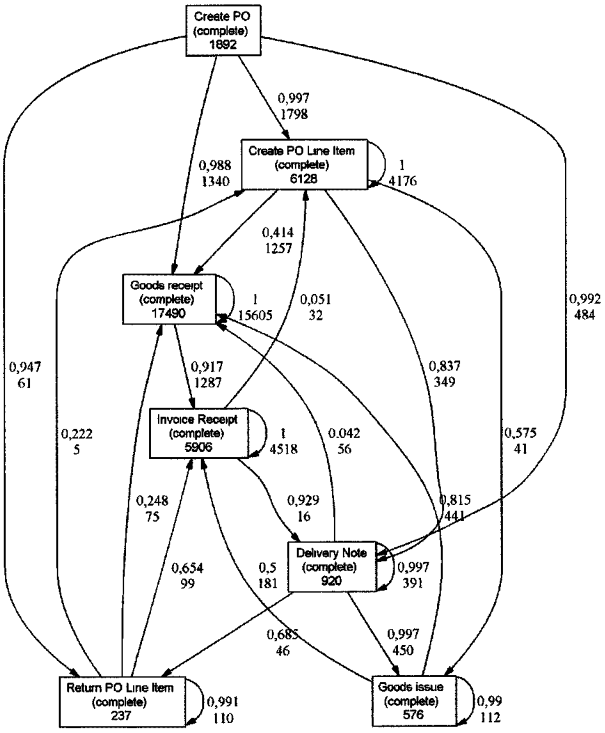


Figure 38: HeuristicsMiner process model based on event log 3, high treshold

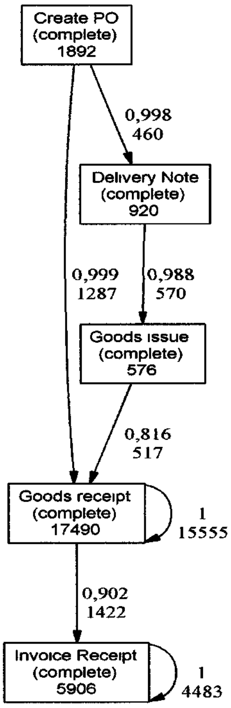
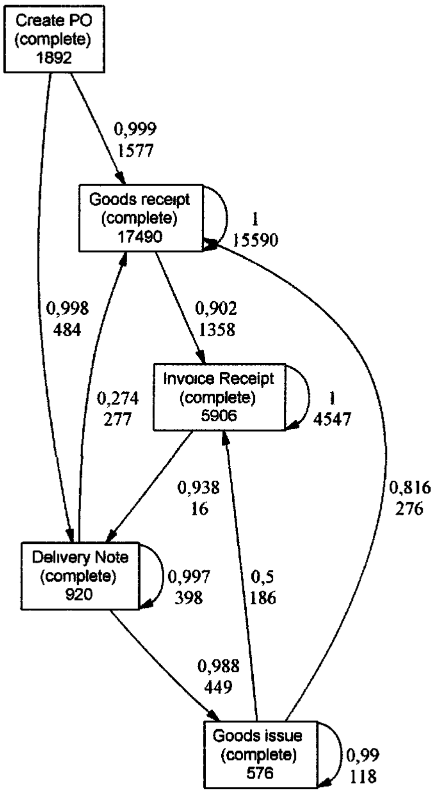


Figure 39: HeuristicsMiner process model based on event log 3, low treshold



Appendix XV: System Implementation Method

This appendix is a summary of the book "Systeem Implementatie Methode: methodische aanpak van de implementatie van informatiesystemen" by Kruithof and Poll (Kruithof & Poll, 1991).

Introduction

Seven aspects can be distinguished when setting up an implementation plan. These are:

- The project approach
- The project phasing
- The project organization
- The project crew
- The project facilities
- The project budget
- The project planning

The project approach

Based in two factors, the degree of structure and the speed of the project, there can be distinguished four types of project approaches. These four types are depicted below.

	Strong pre-structuring	**Any pre-structuring**
Speed primarily	Procedure approach	Rush approach
Speed secondarily	Step-by-step approach	Process approach

With degree of structure is meant the pre-defining of parts in the project. Speed is about the time horizon that is available and the effect of time pressure on planning. The **procedure approach** should be selected if there is a need for a string pre-structured project where also speed is needed when executing the project. Central in the procedure approach is a pre-design project plan. In such a plan the objectives per activity should be defined, the activities should be described and the milestones should be defined. The plan has a strict time plan. Also a complete procedure is developed for communication to the manager and involved employees. The way of organizing the change process and the division of roles is determined in advance. In the **rush approach**, no detailed project plan is formulated. This is a reason attend to structuring the project during the process. This can be done by working on three areas at the same time: the execution of a certain activity, the more detailed preparation of the next activity and the global preparation of the next activity. The rush approach should only be used in exceptional situations. Using the rush approach to bring a project to a successful end needs broad support in the organization. The **step-by-step approach** is selected if speed is of second importance, The time path of such a project is less strictly defined which is ideal for complex projects. After every phase a detailed execution plan with time planning is created for the next phase. The possibility of mistakes in planning and budgeting are minimized. In the **process approach** much more is left open. In advance several steps of the project are described but not who is involved in which activity. The emphasis lies on informal consultation. Advantage is the large manoeuvrability in the change process. Disadvantage is the uncertainty in time planning and the availability of resources.

The project phasing

An implementation project can be split up in several phases. When the System Implementation Method (SIM) is used, seven phases are distinguished:

- Preparation of the project
- Analysis
- Design
- Preparation implementation
- Implementation
- Readjustment
- Evaluation

These phases are used to split up the project in executable parts. All these phases have typical characteristics, a clear beginning and a defined end.

The project organization

Central in the project organization is the organizational structure and the control of the project.

The project crew

For the implementation of a project, staff capacity must be allocated. Having the right people available at the right time is one of the most important conditions of a successful project. This also applies to the users who have to work with the new system.

The project facilities

Under facilities, all the non-human resources are gathered. Examples are hardware, software, office space, material used for education and workshops.

The project budget

Cost estimating of a project is hard to do. As the project advances, more is known about:

- Amount of adjustments necessary in legacy systems
- Amount of adjustments necessary in the organization
- Amount of education
- Amount of time for data conversion
- Amount of tailor made solutions
- External advisors and system developer costs
- Internal project member costs
- Education costs
- Eventual disturbances in current operations
- Costs made for tailor made solutions

The project planning

Planning covers description of activities and the human resources reserved. Besides relevant activities, decision making moments should be planned.

Reference List

1. Amato,R.A. & Eysink,W.T. (2005) Young Deloitte. In.

2. Becht,M., Bolton,P. & Roëll,A. (2003) *CORPORATE GOVERNANCE AND CONTROL.*

3. Berre,A.J., Elvesaeter,B., Aegedal,J.O., Oldevik,J., Solberg,A. & Nordmoen,B. (2004) COMPONENT AND MODEL-BASED DEVELOPMENT METHODOLOGY: METHODOLOGY HANDBOOK. In.

4. Committee on the Financial Aspects of Corporate Governance (1992) THE CADBURY REPORT. In: London.

5. de Beer,H.T. (2004) THE LTL CHECKER PLUGINS: A REFERENCE MANUAL. In: Eindhoven University of Technology, Eindhoven.

6. de Medeiros,A.K., van der Aalst,W.M.P. & Weijters,A.J.M.M. (2005) USING GENETIC ALGORITHMS TO MINE PROCESS MODELS: REPRESENTATION, OPERATORS AND RESULTS. *BETA Working Paper Series.*

7. de Medeiros,A.K., van Dongen,B.F., van der Aalst,W.M.P. & Weijters,A.J.M.M. (2004) PROCESS MINING: EXTENDING THE A-ALGORITHM TO MINE SHORT LOOPS. *BETA Working Paper Series.*

8. Deckers,F.B.M. & van Kollenburg,J.C.E. (2002) *ELEMENTAIRE THEORIE ACCOUNTANTSCONTROLE.* Wolters-Noordhoff, Groningen.

9. Demneri,A. (2005) A NEW LOOK. In.

10. Eisenhardt,K.M. (1989) AGENCY THEORY: AN ASSESSMENT AND REVIEW. *Academy of Management Review,* 57-74.

11. Head,K.M. (2005) CONTINUOUS ASSURANCE: PROACTIVE MONITORING FOR ERRORS AND IRREGULARITIES. In.

12. Institute of Internal Auditors (2005) INFORMATION TECHNOLOGY CONTROLS (GLOBAL TECHNOLOGY AUDIT GUIDE (GTAG) NO.3, Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment. *Internal Auditing,* 20.

13. Kassem,G. & Rautenstrauch,C. (2006) IMPROVEMENT OF ENTERPRISE WORKFLOW IN ERP SYSTEMS BY MEANS OF USAGE MINING METHODS: SAP R/3 AS EXAMPLE OF THE PAPER. In: *Interactive Mobile and Computer Aided Learning Conference.*

14. Kassem,G. & Rautenstrauch,C. (2005) PROBLEM OF TRACING WORKFLOW INSTANCES IN ERP-SYSTEMS. In: *2005 International Business Information Management Conference,* pp. 123-131.

15. Kruithof,E.J.D. & Poll,H.K. (1991) *SYSTEEM IMPLEMENTATIE METHODE: METHODISCHE AANPAK VAN DE IMPLEMENTATIE VAN INFORMATIESYSTEMEN.* Academic Service.

16. Rasmussen,M. (2007) WILL THE REAL RISK AND COMPLIANCE VENDOR PLEASE STEP FORWARD? In: Forrester.

17. Sarva,S. (2006) CONTINUOUS AUDITING THROUGH LEVERAGING TECHNOLOGY. *Information Systems Control Journal,* 2.

18. van Brummelen,H., Coban,S., Dollieslager,D., Lakenman,E., Rogers,T., Tukker,M. & Verstegen,G. (2006) SOX AND COMPLIANCE TOOLS - KEY FINDINGS. In: Capgemini.

19. van der Aalst,W.M.P. (2005) BUSINESS ALIGNMENT: USING PROCESS MINING AS A TOOL FOR DELTA ANALYSIS AND CONFORMANCE TESTING. *Requirements Engineering Journal,* **10**, 198-211.

20. van der Aalst,W.M.P., Ter Hofstede,A.H.M. & Weske,M. (2003) BUSINESS PROCESS MANAGEMENT: A SURVEY. In: *International Conference on Business Process Management,* pp. 1-12. Springer-Verlag, Berlin.

21. van der Aalst,W.M.P. & Weijters,A.J.M.M. (2004) PROCESS MINING: A RESEARCH AGENDA. *Computers in Industry,* **53**, 231-244.

22. van Dongen,B.F., de Beer,H.T. & van der Aalst,W.M.P. (2004) PROCESS MINING AND VERIFICATION OF PROPERTIES: AN APPROACH BASED ON TEMPORAL LOGIC. In.

23. Van Giessel,M. (2004) PROCESS MINING IN SAP R/3. In: Master Thesis, Dept of TM, University of Technology, Eindhoven.

24. van Praat,J.C. & Suerink,J.M. (1992) *INLEIDING EDP-AUDITING,* 5th edn. Ten Hagen & Stam.

25. Weijters,A.J.M.M., van der Aalst,W.M.P. & de Medeiros,A.K. (2003) PROCESS MINING WITH THE HEURISTICS ALGORITHM. In.

26. Whitten,J.L., Bentley,L.D. & Dittman,K.C. (2004) *SYSTEMS ANALYSIS AND DESIGN METHODS,* 6th edn. McGrawHill.