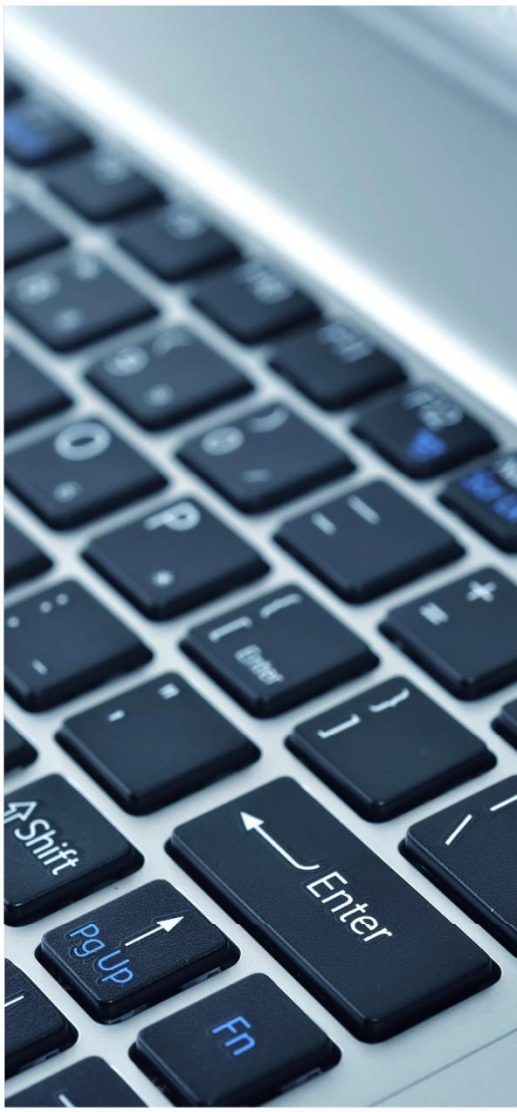
Auditing a Continuous Controls Monitoring System

Designing guidelines for assessing the adequacy of the design and operating effectiveness of a continuous controls monitoring system in the pharmaceutical industry







Master Thesis

Author	Tim Sweep
Student number	4015487
Date	12th of August 2015
Graduation Committee	Prof. dr. ir. M. F. W. H. A. Janssen – Chairman Dr. J. Hulstijn – First Supervisor Dr. M. L. C. de Bruijne – Second Supervisor M. S. van der Burg MSc. RE – External Supervisor
University	Delft University of Technology
Faculty	Faculty of Technology, Policy and Management
Program	Systems Engineering Policy Analysis and Management (SEPAM)
Track	Information Architecture (IA)
External Company	A Big4 audit firm

TU Delft Delft University of Technology

Preface

This report is the outcome of a research I conducted to obtain my Masters of Science degree in Systems Engineering, Policy Analysis and Management (SEPAM) at the Delft University of Technology. I started the research in February 2015 in collaboration with a Big4 audit firm in the Netherlands. In this section, I would like to take the opportunity to thank everybody that have contributed and supported me in the completion of this research.

First of all, I would like to thank the faculty of Technology Policy and Management which gave me the opportunity to enrich myself with valuable insights that are at the basis of this research. In particular, I would like to thank Joris Hulstijn as my first supervisor for his close involvement and guidance during the project. The many interesting discussions we had, and challenges he put me through made me rethink and improve fundamental aspects of this research. Next, I would like to thank Mark de Bruijne as my second supervisor for his adequate input for improving the conclusions and trigger me to critically reflect on the research. Also I would like to thank Marijn Janssen as the chairman of my graduation committee for the discussion we had on the establishment of the guidelines and for his fascinating lectures within the SEPAM program. Furthermore, I'm especially thankful to the Big4 audit firm which gave me access to the resources needed to complete this research. I'm very grateful to Martijn van der Burg for his ideas and inspiring me for IT auditing. Also I would like to thank Hamza Soekhai, Sander Faber, and Koen van Boggelen for their valuable insights, critical view and coaching during the project. Finally, I owe many thanks to my girlfriend, family and friends for supporting me throughout the entire graduation project.

Tim Sweep
The Hague, 12–07–2015

Research summary

Research problem

A common problem faced by external auditors is that assurance regarding an organisation's financial statements can only be provided in a retrospective fashion which is often referred to as the problem of audit timeliness. Although the problem of audit timeliness is not new (Rezaee et al., 2002; Sutton, 2000), it appears that the problem is still not addressed in a satisfactory manner and becomes even more urgent in the real-time economy (Chan & Vasarhelyi, 2011; Chiu et al., 2014; Vasarhelyi, 2011). The real-time economy refers to the business environment in which business processes are largely automated due to technological advances (Kogan et al., 1999; Rezaee et al., 2001; Sutton, 2000). In the real-time economy, modern organisations have automated and integrated their business processes to a great extent but due to the problem of audit timelines the reliability of the (financial) information generated by these automated processes cannot be properly assured. Consequently, It is argued that the audit profession "*has not kept pace with the real-time economy*" (Chan & Vasarhelyi, 2011, p. 152).

At this moment, researchers and practitioners are addressing this problem by exploring continuous auditing (CA) as the successor of traditional auditing (Vasarhelyi, 2011). CA encompasses three aspects: continuous data assurance (CDA), continuous controls monitoring (CCM), and continuous risk management and assessment (CRMA). To potentially address the problem of audit timeliness, this research is aimed at exploring how a CCM system could be used to provide continuous assurance in the real-time economy. In order to do so, the CCM system itself should be audited which is typically the expertise of an external IT auditor. However, it is currently unknown how a CCM system should be audited. Consequently, the main research question is formulated as follows: *How should the adequacy of the design and operating effectiveness of a continuous controls monitoring system be assessed from the perspective of the external IT auditor?* In Figure 1 a schematic overview of a CCM system is presented. In the old situation the IT auditor is required to focus on each individual control separately, whereas in the new situation the IT auditor could potentially rely on the CCM system to assess controls.

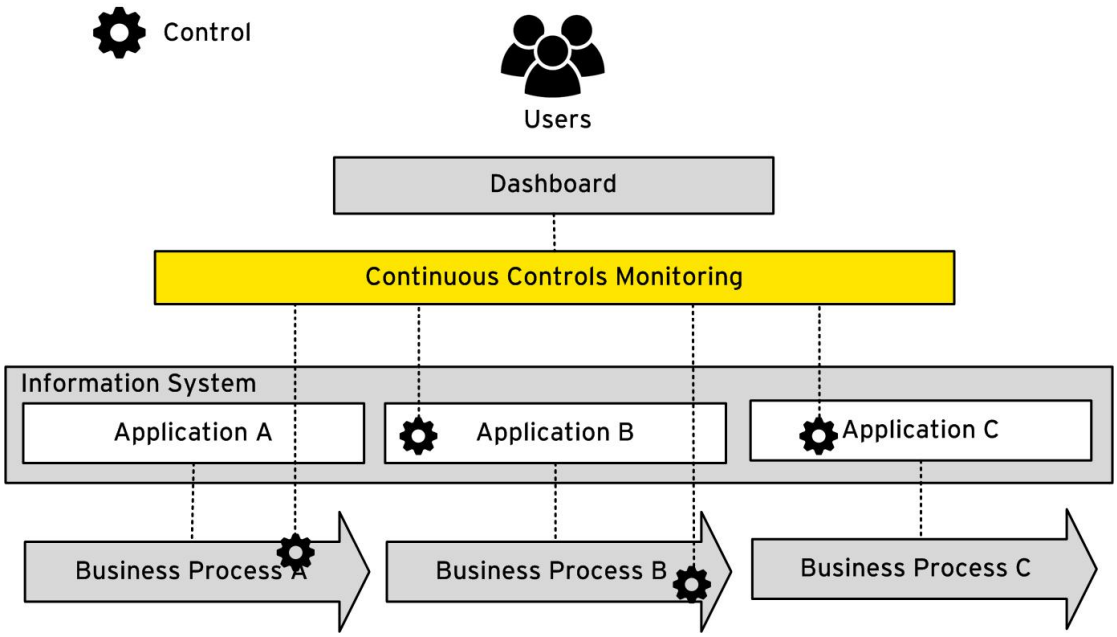


Figure 1 - A schematic overview of a CCM system

Research execution

Design science

To provide an answer to the main research question, an artifact is designed to guide the IT auditor in determining the adequacy of the design and operating effectiveness of a CCM system. To ensure the scientific and social relevance of the artifact, the framework for information system (IS) research as proposed by Hevner et al. (2004) was applied. Moreover, the research was structure according to the design science research methodology as described by Peffers et al. (2007). The designed artifact is a set of guidelines, which function as a frame of reference for assessing the adequacy of the design and operating effectiveness of a CCM system.

Research boundaries

To guide the design, research boundaries are set based on the topic and in accordance with the availability of time and accessibility of resources. First of all, the research was focused on the software package SAP GRC PC to establish the CCM functionality. SAP GRC PC was selected because of its extensive documentation and the fact that the IT auditors who participated in this research were relatively familiar with SAP GRC PC. Second, the research was scoped to the pharmaceutical industry. Because CCM is a relative novel technology, a limited amount of organisations have currently created a mature CCM environment. It turned out that organisations in the pharmaceutical industry are familiar with monitoring technology because of their high risk business processes. Third, the research adopts the perspective of the external IT auditor. External IT auditors are typically the independent party who could assure the reliability of the monitoring results of SAP GRC PC. Fourth, because the research adopts the perspective of the external IT auditor, it should be ensured that the final design is in line with the audit methodology of IT auditors. This research is scoped to the audit methodology maintained by a Big4 audit firm.

Methodologies

To construct the artifact, two research methodologies have been applied to gather the data needed to design the artifact: desk research and semi-structured interviews. The main motivation for making use of desk research is that a lot of the information needed, such as information concerning risk and controls is already described extensively in existing documents. Besides that a lot of the information is well documented, another motivation for using desk research is that the information is relatively easy to acquire. On the contrary, a disadvantage of performing desk research is that the information might not be specific enough for the purpose of this research; CCM is a relatively new concept for pharmaceutical organisations as well as external IT auditors. Desk research was performed by consulting various search engines such as Scopus, Google Scholar, and Sciencedirect to find academic contributions by searching for combinations of keywords including “continuous audit,” “continuous assurance, “ “risk,” “audit,” “continuous monitoring,” “continuous controls monitoring,” “internal control,” and “design science,”. The result was a comprehensive list of literature that is used for designing the artifact.

Interviews can be used for gathering various types of data such as opinions, perceptions and attitudes of the respondent on a certain topic such as CCM. In this research, it is chosen to make use of semi-structured interviews because on the one hand, a certain level of control over the interview is needed to derive information regarding the areas that should be addressed in the IT audit of SAP GRC PC while on the other hand, the respondent is expected to come up with new insights because auditing SAP GRC PC is a relatively unexplored research field. The semi-structured interviews are performed according to a protocol proposed by the non-profit research organization RAND (Harrell & Bradley, 2009). In total five appropriate IT auditors and representatives of two pharmaceutical organisations were found to be willing to participate in the semi-structured interviews.

Evaluation

After the initial design of the artifact, the artifact was evaluated by means of a plan evaluation and a process evaluation as discussed by Verschuren and Hartog (2005). After the execution of the plan- and process evaluation, the initial version of the artifact was improved according the evaluation results. A plan evaluation entails an evaluation of the design on paper. In this research the artifact was evaluated in terms of clearness, acceptance and interrelatedness by asking the IT auditors who have participated in the interviews to provide feedback regarding the structure of the artifact, the guidelines, and the relevance of the artifact. The feedback was received by means of an evaluation form. A process evaluation is aimed at evaluating the design process. It is believed that by ensuring the quality of the design process, this will increase the quality of the artifact to be designed as well. The quality of the process is ensured by following general process criteria which are referred to in the literature as design guidelines (Verschuren & Hartog, 2005). Because in this research the framework of Hevner et al. (2004) was applied, the design science research guidelines as proposed by Hevner et al. (2004) were taken into account for performing a plan evaluation. Also a product evaluation was considered. A product evaluation is aimed at applying the artifact in a real-world situation. It turned out that a product evaluation was not achievable in this research because no pharmaceutical organisations were found to have implemented a CCM system in such a mature way that a product evaluation was feasible. This does not take away the need for the performance of a product evaluation in the future.

Main findings

The main findings are embedded in the final artifact. The artifact consist of four areas in which a total of 41 guidelines were established to guide the external auditor in the assessment of SAP GRC PC in the pharmaceutical industry. The contours of the frame of reference were relatively easy to derive since the respondents were largely on the same page regarding the structure of the artifact which turned out to be in line with the audit methodology of a Big4 audit firm. As regards to the evaluation of the individual guidelines, there appeared to be many inconsistencies among the respondents which stresses the complexity of the topic. With respect to the discussions regarding the guidelines, the main research findings are:

(1) The IT auditor should verify the existence of a control in the source system and cannot blindly rely on the monitoring results as provided by the target system to ensure that the control actually exists. This finding is of particular relevance for the external IT auditor since in the old situation, there was no possibility to rely on a target system to verify the existence of a control.
(2) It was questioned to what extent the ITGCs of the source system should be tested. This question is of relevance because in a traditional audit no data in a source system was monitored. It turned out that testing logical access controls of the source system might be a redundant activity in the case application controls are monitored by targeting configuration data. No evidence was found that testing other ITGCs is a redundant activity.
(3) It turned out to be of relevance to test ITGCs of the target system. This finding is of relevance since in the old situation a target system was absent.
(4) It turned out to be of critical importance that the business rules are correct. In order to assess a business rule, the IT auditor could re-perform the rule, benchmark the rule, or inspect the rule. Conducting a client review with limited knowledge of SAP GRC PC is out of the question. This finding is considered of relevance since in the old situation, there was no monitoring functionality and hence no business rules to assess.
(5) It was concluded that a business rule change management process should be in place to ensure that the source system is still compatible with the target system after changes are made to the source system, and vice versa. This finding is considered a main finding since in the old situation only change related to the source system were taken into account since a target system was absent.

(6) Executing a business rule might negatively influence the performance of the source system. This turned out to be of relevance for the external IT auditor because in order to compensate for the decrease in performance, the organisation is likely to reduce the monitoring frequency.
(7) It turned out to be of relevance to consider the organisational embedding of SAP GRC PC within the organisation. This should allow the IT auditor to determine whether or not to rely on the monitoring results in the case deficiencies are reported. This finding is of particular relevance since in the old situation there were no monitoring results to rely on.

In Figure 2, the main findings are related to the schematic overview of a CCM system.

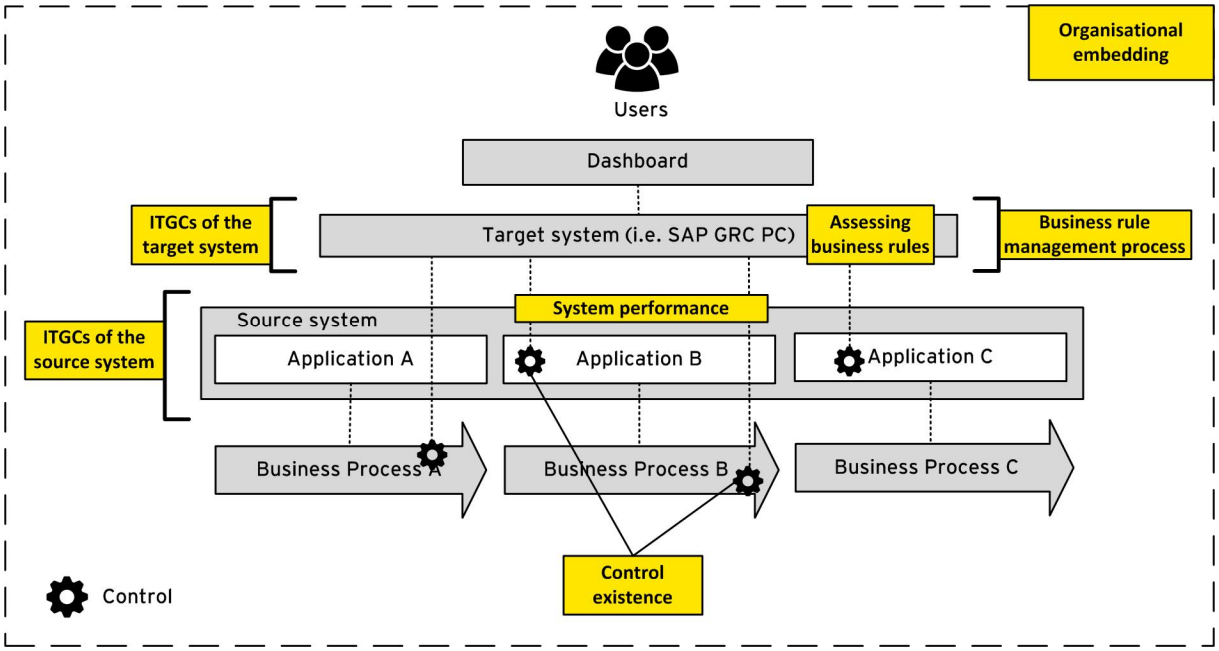


Figure 2 - Relating the main findings to the schematic overview of a CCM system

Theoretical contributions

This research contributes to the exploration of CA practices by conducting a research into CCM systems. Currently, there are only a limited amount of studies that explore the use of a CCM system into practice (Alles et al., 2006; Alles et al., 2008; Kuhn & Sutton, 2006), based on the MCL architecture as proposed by Vasarhelyi et al. (2004). This research is similar to those studies since it takes the implementation of a CCM system (i.e. SAP GRC PC) in a real environment (i.e. the pharmaceutical industry) as a starting point. Besides SAP GRC PC and the pharmaceutical industry have not yet been explored within CCM studies, this research distinguishes from the existing literature, by adopting the perspective of the external IT auditor. This is in line with Sutton (2000) who argues based on Glaser et al. (1968) that a given phenomenon (i.e. CCM) should be studied from numerous perspectives until a consistent pattern arises which eventually might lead to new theory. It could be questioned why it is of relevance to explore the use of a CCM system into practice. This could be explained as follows. It is believed that CA, and therewith CCM, as a phenomenon could potentially address the problem of audit timeliness (Chan & Vasarhelyi, 2011). Although the problem of audit timeliness is not new (Rezaee et al., 2002; Sutton, 2000), it appears that the problem is still not addressed in a satisfactory manner and becomes even more urgent in the real-time economy (Chan & Vasarhelyi, 2011; Chiu et al., 2014; Vasarhelyi, 2011). It is believed that in order to explore whether the claim that CCM could address the problem of audit timeliness is true, first a better understanding of the use of CCM into practice should be obtained.

Contributions to the IT audit community

This research contributes to the IT audit community by designing an artifact that could be used for the performance of an IT audit of a CCM system. The designed artifact supports the IT auditor in assessing the adequacy of the design and operating effectiveness of SAP GRC PC. It could be questioned why it is of relevance for IT auditors to audit a CCM system. This could be explained as follows. It is believed that auditing a CCM system could assure the reliability of the monitoring results which might increase the efficiency and effectiveness of the external IT audit. On the one hand the efficiency might increase because the IT auditor is no longer required to assess the operating effectiveness of each control individually. On the other hand, the effectiveness might increase since the IT auditor is no longer required to estimate the operating effectiveness of a control in a retrospective fashion. It should be noticed that it was not investigated whether the efficiency and effectiveness of the external IT audit will actually increase. The IT auditor himself should determine whether it is of relevance to make use of the monitoring results for the purpose of the external IT audit. What this research contributed, is an artifact that could be used to assess the operating effectiveness and adequacy of the design of a CCM system which is a prerequisite for relying on the monitoring results provided by that system.

Moreover, another contribution to the IT audit community could be explained by taking into account that the IT audit profession is currently subjected to change. In the real-time economy, the traditional audit paradigm seems to be outdated. This is claimed by Sutton (2000, p. 1) who stated that "*the audit profession is desperately trying to catch up with the changes in the business and financial world*", as well as by Chan and Vasarhelyi (2011, p. 152) who stated that the audit profession "*has not kept pace with the real-time economy*". Both claims implicitly call for new innovative approaches. This research contributes to this call by designing a unique artifact. Instead of approaching the audit object using the general audit methodology, this research approaches the audit object using an artifact tailored specifically for the object of interest. Because this research is the first to explore the use of guidelines in the audit profession, the real value of the artifact is unclear and should be explored in the future.

Societal relevance

An organisation's management is responsible for preparing financial statements on an annual basis. The reason for producing financial statements is to communicate the financial position and performance of that organisation towards stakeholders. Stakeholders might be shareholders or investors who rely on the statements to make economic decisions, or other members of society such as banks, suppliers and customers. Because stakeholders are not involved in managing the organisation, an independent external auditor is asked to assure the reliability of the financial statements. The problem faced by external auditors today is that they cannot assure the reliability of financial information continuously as demanded by the stakeholders in the real-time economy. The societal relevance of the artifact, provided that the underlying claim that assessing a CCM system addresses the problem of audit timeliness is true, is that the artifact might contribute to the provision of continuous assurance regarding financial information in the real-time economy.

Table of contents

INTRODUCTION 1

1 RESEARCH INTRODUCTION 2
1.1 Background 2
1.2 Knowledge gap 6
1.3 Scope 6
1.4 Main research question 8
1.5 Design artifact 8
1.6 Research framework 9
1.7 Methodologies 11
1.8 Research structure 12

DESIGN 14

2 THE CONTOURS OF THE FRAME OF REFERENCE 15
2.1 The relation between an IT audit and a financial audit 15
2.2 Designing a frame of reference 16
2.3 Conclusion 25
3 BUSINESS ENVIRONMENT 28
3.1 Understanding the business environment 28
3.2 Industry specific trends 29
3.3 Drivers to implement SAP GRC PC in the pharmaceutical industry 30
3.4 Barriers to implement SAP GRC PC in the pharmaceutical industry 31
3.5 Misperceptions between IT auditors and pharmaceutical organisations 33
3.6 Conclusion 34
4 THE INTERPLAY BETWEEN PROCESSES, RISKS AND CONTROLS 36
4.1 Process analysis 36
4.2 Risk identification 37
4.3 Control assessment 42
4.4 Conclusion 46
5 TECHNICAL ASPECTS OF SAP GRC PC 47
5.1 The technical architecture of SAP GRC PC 47
5.2 The CCM functionality of SAP GRC PC 51
5.3 Conclusion 56
6 COMMUNICATION 58
6.1 Organisational embedding 58
6.2 External reporting 62
6.3 Conclusion 64
7 A SET OF GUIDELINES 65
7.1 Artifact design 65
7.2 An answer to the main research question 65
7.3 Main findings 67

EVALUATION 71

8 EVALUATION 72
8.1 Plan evaluation 72
8.2 Process evaluation 77
8.3 Conclusion 79

CONCLUSIONS 82

9 CONCLUSIONS AND REFLECTION 83
9.1 Conclusion 83
9.2 Theoretical contributions 86

9.3 Contributions to the IT audit community *86*
9.4 Societal relevance *87*
9.5 Limitations *87*
9.6 Future research *88*
9.7 Reflection *89*
10 REFERENCES 91

APPENDICES 94

APPENDIX 1. SEMI-STRUCTURED INTERVIEW PROTOCOLS 95
APPENDIX 2. EXPLANATORY NOTES ON AUDIT RISK, IT RISK, AND QUALITY RISK 103
APPENDIX 3. EXPLANATORY NOTES ON THE INTERNAL CONTROL STRUCTURE 106
APPENDIX 4. EXPLANATORY NOTES ON THE THREE LINES OF DEFENSE MODEL 108
APPENDIX 5. EVALUATION FORM 110
APPENDIX 6. PLAN EVALUATION 116

Table of figures

FIGURE 1 - A SCHEMATIC OVERVIEW OF A CCM SYSTEM IV
FIGURE 2 - RELATING THE MAIN FINDINGS TO THE SCHEMATIC OVERVIEW OF A CCM SYSTEM VII
FIGURE 3 - A SCHEMATIC OVERVIEW OF A CCM SYSTEM 6
FIGURE 4 – CONSTRUCTING THE AUDIT PLAN 8
FIGURE 5 - IS RESEARCH FRAMEWORK 10
FIGURE 6 - GAM ROADMAP 15
FIGURE 7 – DERIVING THE CONTOURS OF A FRAME OF REFERENCE 17
FIGURE 8 - INTERNAL CONTROL STRUCTURE ADOPTED FROM THE GAM 20
FIGURE 9 - IT COMPONENTS REQUIRED FOR ESTABLISHING CCM BY MEANS OF SAP GRC PC 22
FIGURE 10 - QUERY-DRIVEN MONITORING VERSUS EVENT-DRIVEN MONITORING 23
FIGURE 11 - THREE LINES OF DEFENSE MODEL ADAPTED FROM IIA (2013, P. 2) 25
FIGURE 12 - CONTOURS OF THE FRAME OF REFERENCE 26
FIGURE 13 - RISK INTERRELATEDNESS 40
FIGURE 14 - REBALANCING THE AUTOMATED CONTROLS PORTFOLIO ADAPTED FROM NELSON AND AMBROSINI (2007, P. 30) 43
FIGURE 15 - DETERMINING THE MONITORING FREQUENCY 46
FIGURE 16 - OPERATING EFFECTIVENESS LOOP 59
FIGURE 17 - PROCESS IMPROVEMENT LOOP 60
FIGURE 18 - SYSTEM IMPROVEMENT LOOP 60
FIGURE 19 – A SET OF GUIDELINES 66
FIGURE 20 – A REDESIGN OF THE SET OF GUIDELINES 81
FIGURE 21 - RELATING THE MAIN FINDINGS TO THE SCHEMATIC OVERVIEW OF A CCM SYSTEM 84
FIGURE 22 - AUDIT RISK MODEL 103
FIGURE 23 – QUALITY RISK MANAGEMENT PROCESS ADOPTED FROM (ICH, 2005, P. 2) 105
FIGURE 24 - INTERNAL CONTROL STRUCTURE ADOPTED FROM THE GAM 106
FIGURE 25 - THREE LINES OF DEFENSE MODEL ADAPTED FROM IIA (2013, P. 2) 108

Table of tables

TABLE 1 – SAP GRC COMPONENTS DEFINITIONS DERIVED FROM EY (2014) 7
TABLE 2 - CCM TECHNOLOGIES, ADAPTED FROM CALDWELL AND PROCTOR (2009, P. 7) 7
TABLE 3 - BACKGROUND INFORMATION IT AUDITORS 11
TABLE 4 - BACKGROUND INFORMATION PHARMACEUTICAL ORGANISATIONS 12
TABLE 5 - RISK MITIGATION STRATEGIES ADOPTED FROM GTAG (2012, P. 12) 19
TABLE 6 - THREE ARCHITECTURES TO ESTABLISH CONTINUOUS MONITORING ADAPTED FROM KUHN AND SUTTON (2010) 21

TABLE 7 - SUB-QUESTIONS OVERVIEW 27
TABLE 8 - SUB-QUESTIONS CHAPTER 3 28
TABLE 9 - SUB-QUESTIONS CHAPTER 4 36
TABLE 10 - SUB-QUESTIONS CHAPTER 5 47
TABLE 11 - SUB-QUESTIONS CHAPTER 6 58
TABLE 12 - GUIDELINE CLASSIFICATION 67
TABLE 13 - THEORETICAL FOUNDATION OF THE MAIN FINDINGS 70
TABLE 14 - EVALUATION CRITERIA 73
TABLE 15 - EVALUATION RESULTS REGARDING THE FRAME OF REFERENCE 74
TABLE 16 - EVALUATION RESULTS REGARDING THE NORMATIVE GUIDELINE 75
TABLE 17 - EVALUATION RESULTS REGARDING THE RELEVANCE OF THE ARTIFACT 76
TABLE 18 - DESIGN-SCIENCE RESEARCH GUIDELINES ADAPTED FROM (HEVNER ET AL., 2004, P. 83) 77
TABLE 19 - POINTS OF IMPROVEMENT ACCORDING TO THE PLAN EVALUATION 80
TABLE 20 - RISK CONCEPTS 103
TABLE 21 - EVALUATION CRITERIA 116
TABLE 22 - EVALUATION RESULTS REGARDING THE FRAME OF REFERENCE 116
TABLE 23 - EVALUATION RESULTS REGARDING THE GUIDELINES RELATED TO THE BUSINESS ENVIRONMENT 117
TABLE 24 - EVALUATION RESULTS REGARDING THE GUIDELINES RELATED TO PROCESSES, RISKS AND CONTROLS 118
TABLE 25 - EVALUATION RESULTS REGARDING THE GUIDELINES RELATED TO THE TECHNOLOGICAL ASPECTS 119
TABLE 26 - EVALUATION RESULTS REGARDING THE GUIDELINES RELATED TO THE COMMUNICATION 122

Table of textboxes

TEXTBOX 1 - CCM TO MONITOR PHARMACEUTICAL PROCESSES, PROCESSES AND RECORDS 41
TEXTBOX 2 – CCM TO MONITOR THE ACCURACY OF CLINICAL DATA 42
TEXTBOX 3 - DATA INTEGRITY 51

INTRODUCTION

1

Research introduction

The purpose of this chapter is to introduce the research problem and explain the research approach. In order to do so, first the state of the art of the literature will be discussed (1.1). From the literature review a knowledge gap (1.2) will be derived. This knowledge gap will be scoped (1.3) to be manageable in a single project which result in the formulation of the main research question (1.4). In line with the research question, the final design will be described (1.5) where after a research framework (1.5) will be introduced and the research methodologies (1.6) will be explained. Finally the research will be structured (1.7) by identifying four research stages.

1.1 Background

1.1.1 The problem of audit timeliness

Management is responsible for preparing the financial statements of an organisation. The reason for producing financial statements is to communicate the financial position and performance of that organisation towards stakeholders. Stakeholders might be shareholders or investors who rely on the statements to make economic decisions, or other members of society such as banks, suppliers and customers. Because stakeholders are not involved in managing the organisation, an independent party is asked to assure the reliability of the financial statements. Typically, an external auditor acts as this independent party. The external auditor provides an opinion on the reliability of the statements by performing a financial audit. In general an audit is defined as "*a systematic, objective examination of one or more aspects of an organization that compares what the organization does to a defined set of criteria or requirements*" (Gantz, 2013, p. xxi). In the financial audit, the objectives are financial statements and the defined set of criteria are accounting standards like the General Accepted Accounting Principles (GAAP).

While performing a financial audit, the external auditor collects audit evidence to obtain reasonable assurance that the financial statements are free from any material errors or other misstatements. In the current international standard on auditing (ISA) 200, the International Federation of Accountants (IFAC) state that reasonable assurance "*is obtained when the auditor has obtained sufficient appropriate audit evidence to reduce audit risk (that is, the risk that the auditor expresses an inappropriate opinion when the financial statements are materially misstated) to an acceptably low level*" (IFAC, 2009a, p. 73). The problem with the collection of audit evidence, is that the evidence is always gathered after the publication of the financial statements. Consequently, the reliability of the statements can only be assured is a retrospective fashion. This is a major concern for the stakeholders of an organisation who have to rely on the financial statements to make economic decisions. These decisions must be taken in real-time.

Besides the stakeholders, organisations themselves are affected by the delay in the provision of assurance as well. The management of an organisation makes strategic decisions according to information originating from their internal processes. Just as in the external audit, the reliability of this information can only be assured afterwards. Within an organisation, the internal auditor is responsible for providing assurance. The function of an internal auditor is to perform assurance and consulting activities designed to evaluate and improve the effectiveness of an organisation's governance, risk management and internal control processes (IFAC, 2013). The activities of the internal auditor and external auditor are dependent on each other; the external auditor has to rely on the work of the internal auditor for assuring the reliability of the financial statements.

So the external auditor is an independent party who is responsible for assuring the reliability of an organisation's financial statements towards that organisation's stakeholders. Internal auditors are responsible for assuring the reliability of the information used by the management of that organisation for making strategic decisions. The problem faced by external auditors as well as internal auditors is that assurance can only be provided in a retrospective fashion. Academics and practitioners often refer to this as the "timeliness" of an audit (Chiu et al., 2014). Although the problem of audit timeliness is not new (Rezaee et al., 2002; Sutton, 2000), it appears that the problem is still not addressed in a satisfactory manner and becomes even more urgent in the real-time economy (Chan & Vasarhelyi, 2011; Chiu et al., 2014; Vasarhelyi, 2011).

1.1.2 The real-time economy

In the real-time economy, organisations are able to decrease the costs of processes through automation and increase process accuracy due to technological advances, such as the advent of enterprise resource planning (ERP) systems, specialised business-reporting languages, sensing devices to record economic events and methods to automatically integrate human-decision processes (Vasarhelyi, 2011). Process automation and technological advances allow for faster generation of information. Consequently, organisations and their stakeholders are forced to react to events based on this information more quickly. This increases the need for more timely assurance on the real-time generated information. However, by definition traditional audit procedures look back over a period in time, so they are not capable of providing proper assurance in the real-time economy. In short, the problem modern organisations face today is that although their processes are to a great extent automated and integrated, which can be of great value for their businesses, the reliability of these processes cannot be properly assured in real-time. At this moment, researchers and practitioners are addressing this problem by exploring continuous auditing (CA) as the successor of traditional auditing. The following paragraph will elaborate more on the CA methodology.

1.1.3 Continuous auditing

One of the first widely adopted definitions of CA is provided by CICA/AICPA (1999): "*A methodology that enables independent auditors to provide written assurance on a subject matter, for which an entity's management is responsible, using a series of auditors' reports issued virtually simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter*". Initially, these automatically generated reports used by auditors to provide written assurance contained audit evidence based on detected data irregularities on the transactional level. Nowadays the definition of the CA methodology has been widened and encompasses three main concepts (Vasarhelyi, 2011). Although together these concepts form the CA methodology, in academic literature they seem to be addressed as separated research streams.

The first concept is *continuous data assurance* (CDA). CDA allows for the continuous monitoring of transactions, comparing these transactions to predetermined benchmarks and identify anomalous situations. Traditionally CA was defined as what nowadays is called CDA. As a result, a lot of the initial work on CA is labelled as CDA. Examples are the works of Groomer and Murthy (1989) and Vasarhelyi and Halper (1991). The second concept is *continuous controls monitoring* (CCM). CCM is about monitoring a set of controls, for instance controls on system configurations or access controls. After regulatory changes such as the Sarbanes-Oxley Act, organisations are to a greater extent obliged to monitor their internal controls. Consequently, due to the increasing regulatory pressure, CCM gained a lot of attention in scientific research. The studies of Alles et al. (2006), (Alles et al., 2008) and Kuhn and Sutton (2006) are examples of some of the initial works on CCM. The third concept is *continuous risk management and assessment* (CRMA). CRMA is a discipline which is concerned with continuously monitoring the risk an organisations is exposed to, and to determine whether this risk is adequately assessed. The need for CRMA is increasing in the real-time economy where information to make strategic decisions is updated on a continuous basis. From the three concepts CRMA is the most novel one and should be extensively explored to determine its contribution to continuous auditing (Vasarhelyi, 2011).

In theory, the CA methodology can be used to provide assurance on the reliability of real-time generated information in modern organisations. After all, CA allows for continuously monitoring and

assuring the reliability of transactional data, controls and risk. In the following paragraph, the consequences of CA for external auditors will be discussed.

1.1.4 The external IT auditor

The large-scale automation of business processes is drastically altering the audit profession in which the continuous audit paradigm seems to get increasing attention (Chan & Vasarhelyi, 2011). Consequently, the procedures used by auditors have to be adapted to the new automated environment (Elliott, 2002). Rezaee et al. (2001) identified three aspects of the traditional audit process of external auditors that has to be adapted according to the new situation. First, the auditor's knowledge on the use of data and electronic documents in the organisation of interest and associated industry has to increase. Second, the auditor should gain a better understanding of the flow of transactions and control activities in the automated environment. Third, the auditor should use a control risk-oriented audit plan for assessing the internal controls implemented in the automated environment, and pay less attention on substantive audit tests. Rezaee et al. (2001) acknowledged the increasing importance of IT in the procedures of the external auditor already in 2001 when only 25% of the world's information was digital. Nowadays, in the real-time economy, where business processes are automated to a large extent, more than 98% of the world's information is digital (Cukier & Mayer-Schoenberger, 2013). Consequently, the IT-landscape of modern organisations had become more complex and the external auditor lacks the IT knowledge to properly assess the quality of audit evidence to provide reasonable assurance on an organisation's financial statements. This is where the external IT auditor comes into play.

From now on, the role of external auditor is differentiated in a financial auditor who is responsible for assessing an organisation's financial statements, and an IT auditor who is responsible for assessing the organisation's processes, IT assets and controls (Gantz, 2013). The IT auditor supports the financial auditor in his decision whether sufficient appropriate audit evidence is collected. There are some heuristics that financial auditors use for determining the amount of audit evidence that is needed in order to bring the audit risk to an acceptable, predefined level. One of these heuristics, which can be derived from the research on audit risk by Knechel (2001), is that less audit evidence is needed when the organisation of interest has a better internal control structure. In other words, when an organisation has insufficient internal control measurements, the external auditor is required to perform more substantive procedures (collect more audit evidence) to assure the reliability of the financial statements. Assessing the strength of the internal control structure is one of the tasks of the IT auditor.

The assessment of the internal control structure of an organisation starts with a risk assessment. This risk assessment is conducted by the financial auditor and is aimed at identifying the risk areas on an organisation's financial statements. According to the identified risk areas, the financial auditor composes a list of controls they expect within the organisation of interest. This might be automated controls, IT dependent controls as well as manual controls. The IT auditor takes the list with expected controls as a starting point to assess the internal control structure of the organisation. The assessment of the internal control structure is performed in close cooperation with the internal auditors. After all, the internal auditors are responsible for operating the internal control structure. For the assessment of a control, two aspects are investigated by the IT auditor. On the one hand, the IT auditor assesses the *design adequacy* of the control. The design adequacy is concerned with determining whether the controls sufficiently mitigate the risk they are supposed to cover. On the other hand, the IT auditor assesses the *operating effectiveness* of the control. The operating effectiveness is concerned with determining whether the control was in operation during a specified period in time, provided that the adequacy of the design is already established. During the investigation of the operating effectiveness of a control, the problem of audit timeliness becomes evident; the IT auditor is estimating the functioning of the control in a retrospective fashion. The IT auditor can only assure the operation of the control afterwards. When the IT auditor has obtained a realistic overview of the internal control structure of the organisation, the findings are communicated to the financial auditor who then determines the amount of appropriate audit evidence needed to provide reasonable assurance on the financial statements of the organisation. In the following paragraph it will be shown how the internal control structure of an organisation is changing in the light of CA. The focus will be on the influence of CCM on the auditing profession.

1.1.5 CCM to address the problem of audit timeliness

At the moment, a wide spread adoption of CA practices (Gonzalez et al., 2012; Vasarhelyi, Alles, et al., 2012), and CCM in particular (Vasarhelyi, Romero, et al., 2012), remains off. Although CCM implementations are rare, it is believed that organisations are increasingly interested in continuously monitoring their controls for two reasons. First of all, CCM systems could be used to demonstrate regulatory compliance. Corporate governance regulation forces organisations to give accountability for its pursued governance policy in their annual reports. In the United States, corporate governance regulation was introduced in 2002 in the form of the Sarbanes-Oxley (SOx) act after the corporate scandals with, among others, Enron and Worldcom. Similar to SOx, the European Union developed an action plan to enhance corporate governance in 2003. A second reason why organisations are believed to have a growing interest in CCM systems is because CCM systems could provide real-time insight into the internal control structure of the organisation. As a result, the internal auditor is no longer required to provide reasonable assurance on the operational effectiveness in a retrospective fashion. So a CCM system could enable internal auditors to address the problem of audit timeliness and assess the reliability of information with a higher level of assurance (Vasarhelyi, 2011). However, monitoring controls alone is not sufficient for assuring the reliability of information completely (Vasarhelyi, 2011). CCM only assures the operating effectiveness of the controls however, it does not assure that the risk mitigated by these controls has not occurred. To check whether the risk has occurred, CDA is needed to check for data irregularities on the transactional level. Vice versa, when no data irregularities are found on the transactional level, this does not ensure that an organisation has a proper internal control structure to mitigate risk. It could be luck that the risk has not occurred. Although, both CCM and CDA are important for providing continuous assurance, this research will focus on CCM in particular as will be motivated when describing the scope of the research.

Besides the potential advantages of CCM to show regulatory compliance and addresses the problem of audit timeliness for the internal auditor, CCM might also improve the effectiveness and efficiency of the external audit. Currently, a significant part of the time used for the external audit is spent on checking the operating effectiveness of individual controls. This is relatively elementary work for well-educated external IT auditors. Potentially, if the external IT auditor could rely on the CCM system operated by the internal audit department, this could limit the work of the IT auditor to the parts of an audit which require professional expertise. Moreover, if the expensive activities of the external IT auditors will become more efficient, this will relieve the financial burden for organisations which might be another motivation for organisations to implement a CCM system.

In Figure 3 a schematic representation of a CCM systems is presented to clarify the above described line of reasoning. An organisation have numerous business processes to perform their daily business activities. As can be derived from the figure, these business processes are supported by applications which are part of the organisation's information system. Currently, external auditors are providing assurance by assessing the design adequacy and operating effectiveness of controls. A CCM system monitors controls and provide information concerning their operating effectiveness via the dashboard. If the external auditor could rely on the CCM system operated by the internal auditor, this could increase the efficiency and effectiveness of the external IT audit and addresses the problem of audit timeliness.

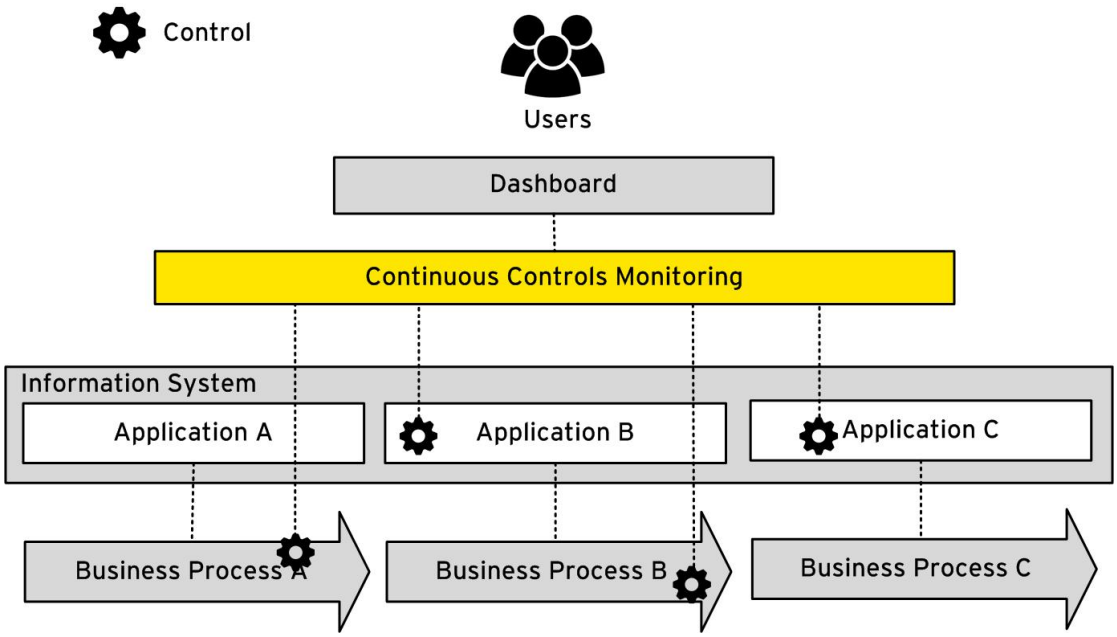


Figure 3 - A schematic overview of a CCM system

1.2 Knowledge gap

One of the problems faced by internal as well as external auditors is the problem of audit timeliness. In the real-time economy this problem is becoming more urgent because information is produced and processed faster as a result of process automation. Consequently, there is an increasing need among organisations and their stakeholders for continuous assurance on the reliability of this information. To provide continuous assurance, academics and practitioners are exploring CA as the successor of traditional auditing. CCM is considered part of the CA methodology and can potentially address the problem of audit timeliness. If auditors could rely on a CCM system this will ensure the operating effectiveness of controls in real-time and hence allow auditors to assure the reliability of information continuously, provided that adequacy of design is already established. However, for an auditor to rely on a CCM system, the CCM system itself should be audited which appears to be relatively unexplored territory. There appears to be a knowledge gap regarding the IT audit of CCM systems.

1.3 Scope

The main goal of scoping is to make explicit what is included in the research and what falls outside the research boundaries. The boundaries of the research are based on the topic, but are also defined according to the availability of time and accessibility of resources. In short, the research is scoped to the IT audit of SAP GRC PC for providing assurance on the reliability of financial statements of pharmaceutical organisations.

SAP GRC PC

CCM is a functionality which could be achieved by a variety of software applications such as governance, risk and compliance (GRC) applications. The term GRC has gained a lot of attention from software vendors and less from the academic community, which indicates that it is merely a marketing term rather than a scientific research field. According to Racz et al. (2010, p. 6) "*GRC is an integrated, holistic approach to organisation-wide governance, risk and compliance ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness*". The concept of GRC is rather broadly defined and covers more than just the concept of CCM. Currently there is a plethora of GRC applications on the market. For the purpose of this research SAP GRC is selected because of its extensive documentation. Moreover, the author is in contact with IT auditors who are familiar with this application. SAP GRC PC is composed of multiple components of which the most commonly used are described in Table 1 (EY,

2014). As can be derived from the descriptions in the table, the process control component corresponds with CCM. Therefore, only the PC component of SAP GRC will be taken into account for the purpose of this research.

Table 1 – SAP GRC components definitions derived from EY (2014)

SAP GRC component	Description
SAP GRC RM (Risk Management)	"offers a holistic risk visibility, key risk indicators and enterprise risk intelligence through dashboards and surveys".
SAP GRC PC (Process Control)	"provides a central controls repository, self-assessments, automated process and work flow management, as well as configurable controls testing and real-time exception based reporting"
SAP GRC AC (Access Control)	"enables sensitive access management and segregation of duties, critical and emergency access management, and compliant access provisioning"

In SAP GRC PC, CCM encompasses three monitoring targets: configurations, master data and backend transactions. Based on these targets, Caldwell and Proctor (2009) distinguish three types of CCM as described in Table 2. According to the definitions of CDA and CCM, monitoring transactions might be classified as CDA. However, if there are no irregularities found by monitoring transactional data, the likelihood that the internal control structure of the organisation is properly designed and operates as intended increases, which touches the objective of CCM. Although, by definition monitoring and analysing transactional data should be classified as CDA practices, there seems to be an indirect relation to CCM. Because of this indirect link, monitoring transactions will be taking into account as well when considering the CCM functionality of SAP GRC.

Table 2 - CCM technologies, adapted from Caldwell and Proctor (2009, p. 7)

CCM technology	Description
CCM-AC (Application Configuration)	Refers to continuously "monitor the presence, appropriate configuration and modification of built-in application controls". CCM-AC is used in conjunction with each of the other CCM technologies.
CCM-T (Transactions)	Refers to "continuously monitor ERP and financial application transaction information to improve governance and automate audit processes".
CCM-MD (Master Data)	Refers to continuously monitoring the quality and use of master data.

The pharmaceutical industry

The performance of an external IT audit depends on the sector of interest (Rezaee et al., 2001), therefore this research will focus on organisations from a particular industry. A precondition is that these organisations should be familiar with CCM. Because CCM is a relatively novel technology, there are very limited industries in which organisations have created a CCM environment by means of SAP GRC PC. The scope of this research will be limited to organisations in the pharmaceutical industry since they are likely to have an understanding of CCM because of their high risk production processes. Moreover, two pharmaceutical organisations were found to be willing to participate in this research which are familiar with SAP GRC PC.

The external IT audit for financial statements

This research will be focused on the usage of SAP GRC PC for the external audit. If it turned out that the external auditors can rely on the output of SAP GRC PC and use the results to ensure the operating effectiveness of a control real-time, this might address the problem of audit timeliness. Auditing software applications is typically the domain of the IT auditor. Consequently, this research adopts the perspective of the external IT auditor. Especially the external IT audit for providing assurance on an organisation's financial statement will be of interest. In fact, the scope is on the performance of an external IT audit to support the external financial audit.

1.4 Main research question

According to the knowledge gap and research scope the main research question could be formulated. The subdivision of the main research questions in to sub-questions will logically follow from the results of Chapter 2. Consequently, the sub-questions are presented in section 2.3. The main research question is formulated as follows:

How should the adequacy of the design and operating effectiveness of a continuous controls monitoring system in the pharmaceutical industry be assessed from the perspective of the external IT auditor?

It should be noticed that the purpose of this research is not to investigate whether the underlying claims that assessing a CCM system addresses the problem of audit timeliness and improves the quality of the external IT audit are true. The objective of this research is to explore how a CCM system should be audited from the perspective of the external IT auditor.

1.5 Design artifact

This research should classified as design science. According to Hevner et al. (2004, p. 75) "*the design-science paradigm seeks to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts*". To address the main research question, in this section an artifact will be proposed that supports the external IT auditor in the audit of a CCM system.

To define the artifact to be designed, first it will be described how an external auditor performs an IT audit regarding an audit object. In general, the IT auditor starts with defining an audit plan in which it is stated how the adequacy of the design and operating effectiveness of the audit object will be assessed. The construction of an audit plan is visualised in Figure 4. As can be derived from the figure, the audit plan is constructed with input from the audit object itself within its environment and with input from the audit methodology. Currently, the IT auditor uses his professional judgement to construct the audit plan. The IT auditor determines what aspects of the audit object should be addressed, and what aspects of the methodology should be applied to assure the adequacy of the design and operating effectiveness of the object.

Because CCM systems are relatively new to IT auditors, it is currently unknown how an audit plan for the assessment of the adequacy of the design and operating effectiveness of a CCM system should be constructed. Therefore, the artifact to be designed should guide the IT auditor in the IT audit of a CCM system. Currently, the concept of guidance is absent in the IT audit profession. Therefore, a solution is derived from another research field.

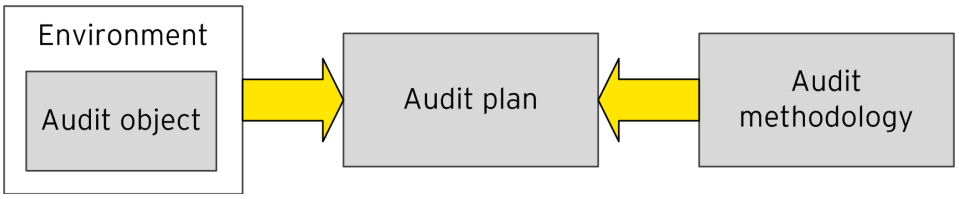


Figure 4 – Constructing the audit plan

An academic research field in which design guidance plays an important role is enterprise engineering in which enterprise architecture is considered a mean to govern enterprise transformations (Proper & Greefhorst, 2011). Dietz and Hoogervorst (2008, p. 574) define architecture as a "*normative restriction of design freedom*". According to Op't Land and Proper (2007), the architectural design of an enterprise is often normatively restricted by means of architectural principles (Op't Land & Proper, 2007). "*Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organization sets about fulfilling its mission*" (TOGAF, 2004). The concept that is of particular relevance for the purpose of this research is that design freedom is restricted by following principles. To translate this concept according to the purpose of this research, principles could be used as guidance for constructing the audit plan in which it is stated how the adequacy of the design and operating effectiveness of a CCM system might be assessed. It should be noticed that the IT auditor

should be guided and not restricted. Adopting the concept of guiding design by means of principles is dangerous since IT auditors use principles in a different manner. In general, IT auditors examine an audit object by comparing that object to a defined set of criteria which might be referred to as principles, norms, standards, or requirements. It should be noticed that the terms used to refer to audit criteria are used interchangeable and lack a clear and unambiguous definition. To be crystal clear, in this research a new term will be introduced that refers to the provision of guidance in the performance of an IT audit:

A *guideline* is a rule that provides guidance in a particular activity without imposing any strict obligations

According to this definition, guidelines might be followed, but do not have to be followed. Moreover it should be noticed that guidelines are not audit criteria used to assess an audit object, but guide the IT auditor in the performance of an IT audit. More specifically, for the purpose of this research, guidelines will be established that guide the IT auditor in the construction of an audit plan regarding the assessment of SAP GRC PC in the pharmaceutical industry. That being said, the artifact to be designed in this research is formulated as follows:

A set of guidelines, which function as a frame of reference for assessing the adequacy of the design and operating effectiveness of SAP GRC PC in the pharmaceutical industry.

1.6 Research framework

According to the knowledge gap and research deliverable, this section is aimed at describing a research framework to ensure the scientific and social relevance. For this purpose, the framework for information systems (IS) research as proposed by Hevner et al. (2004) will be used. In Figure 5. the framework was adjusted for the purpose of this research.

The main purpose for implementing information systems in organisations is to improve effectiveness and efficiency in that organisation. Researchers in the IS domain contribute to the improvement of effectiveness and efficiency by developing and communicating knowledge concerning the "*management of information technology and the use of information technology for managerial and organisational purposes*" (Zmud, 1997, p. iii). Acquiring this knowledge seems to originate mostly from two research paradigms: behavioural science and design science. The difference can be explained by looking to the objective of both paradigms in relation to IT artifacts. In IS behavioural science research the objective is to understand an IT artifact within its organisational context while in IS design science research the objective is to create and evaluate IT artifacts for solving organisational problems (Hevner et al., 2004). The IT artifact to be designed in this research is a set of guidelines which function as a frame of reference for the construction of an audit plan to perform an IT audit regarding SAP GRC PC in the pharmaceutical industry. So this research should be classified as design science.

As can be derived from the figure, on the one hand, the environment and knowledge base contribute to the research by providing guidelines, a frame of reference to structure the guidelines, and well established research methodologies. On the other hand, the research contributes to the environment since it could potentially provide a more consistent level of assurance on the organisation's financial statements in the real-time economy and could potentially improve the quality of the external IT audit. Moreover, the research contributes to the knowledge base by designing an artifact that could be used as a foundation for future research and documenting the lessons learned from applying the research methodologies. In the subsequent paragraphs, the problem relevance and research rigor will be discussed in more detail.

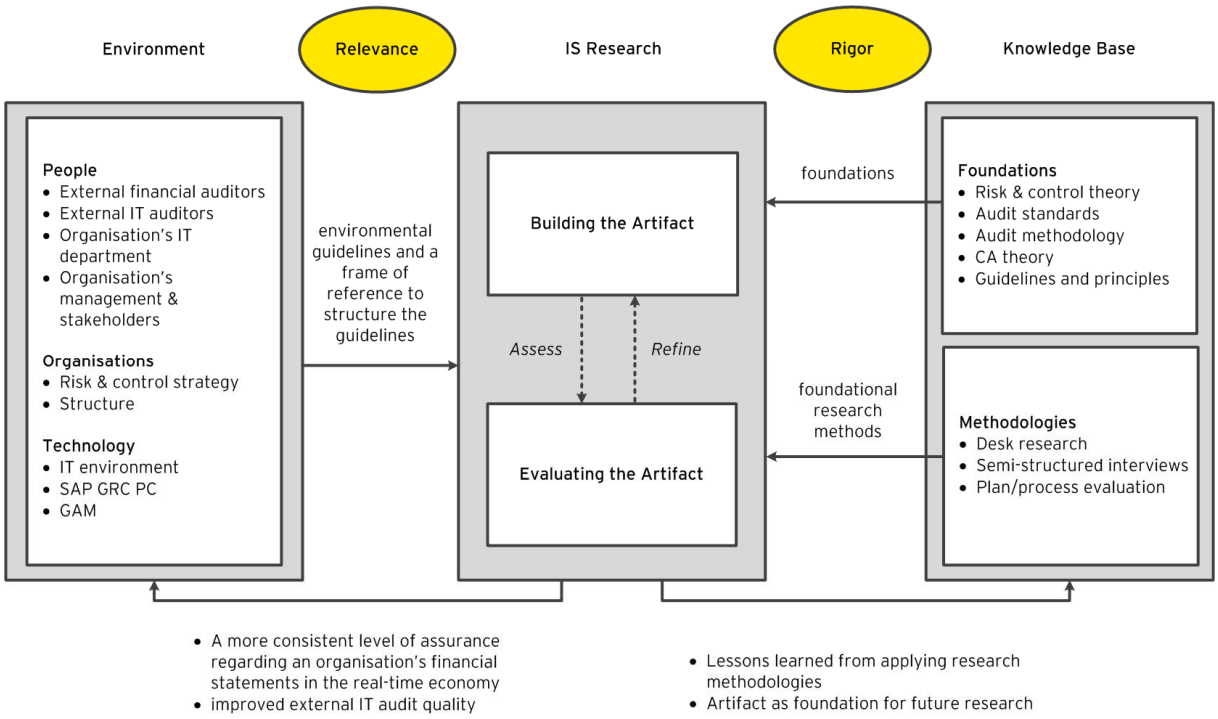


Figure 5 - IS research framework

Problem relevance

The environment is composed of people, organisations and technology. The problem that will be addressed in this research originates from the business needs resulting from the interplay between people, organisations and technology. The extent to which that problem will be solved is defined as the research relevance. In this research the identified business need is to provide continuous assurance in the real-time economy. To ensure research relevance, the final artifact should contribute to this business need. Designing a set of guidelines to enable IT auditors to assure the reliability of a CCM system and could potentially address the problem of audit timeliness and hence is believed to contribute to the provision of continuous assurance in the real-time economy. After all, by relying on the monitoring results provided by SAP GRC PC the operating effectiveness could be assured in a real-time fashion. Moreover, if the IT auditor is able to rely on the monitoring results as provided by SAP GRC PC, this might increase the quality of the IT audit since the IT auditor is no longer required to rely on samples for determining the operating effectiveness of a control. So the artifact to be designed is mainly of relevance since it is believed to address the problem of audit timeliness and hence contributes to the provision of continuous assurance in the real-time economy. Moreover, the artifact is might increase the quality of the external IT audit since the operating effectiveness is no longer estimated based on samples. Both assumptions will not be investigated as part of this research but are the underlying claims to ensure the research relevance.

Research rigor

The knowledge base is composed of foundations and methodologies. The foundations encompasses frameworks, instruments, constructs, models and methods developed in prior IS research. The foundations can be used for building the artifact. The methodologies in design science are used to safeguard the quality of the design process. To ensure research rigor, the research should be based on an extensive scientific foundation and make use of well-known IS research methodologies. Furthermore, the artifact to be designed might be used as a foundation in future IS research. Moreover, the way research methodologies are applied in this research could be taken into account in future IS research as well.

1.7 Methodologies

There are numerous types of data collection methods such as survey's, interviews, focus groups, guideline, data extraction (desk research) or secondary data sources (Harrell & Bradley, 2009). For the purpose of this research it is chosen to make use of desk research and semi-structured interviews.

Desk research

Desk research involves gathering data from existing data sources. The main motivation for making use of desk research is that a lot of the information needed, such as information concerning risk and controls is already described extensively in existing documents. Besides that a lot of the information is well documented, another motivation for using desk research is that the information is relatively easy to acquire. On the contrary, a disadvantage of performing desk research is that the information might not be specific enough for the purpose of this research; CCM is a relatively new concept for pharmaceutical organisations as well as external IT auditors. Desk research was performed by consulting various search engines such as Scopus, Google Scholar, and Sciencedirect to find academic contributions by searching for combinations of keywords including "continuous audit," "continuous assurance, " "risk," "audit," "continuous monitoring," "continuous controls monitoring," "internal control," and "design science,". The result was a comprehensive list of literature that is used for designing the artifact.

Semi-structured interviews

Interviews can be used for gathering various types of data such as opinions, perceptions and attitudes of the respondent on a certain topic such as CCM. Interviews can be placed on a continuum which ranges from unstructured, in which the interviewer has limited control over the interaction, to highly structured, in which the interviewer has significant control over the interaction. In this research, it is chosen to make use of semi-structured interviews because on the one hand, a certain level of control over the interview is needed to derive information regarding the areas that should be addressed in the IT audit of SAP GRC PC while on the other hand, the respondent is expected to come up with new insights because auditing SAP GRC PC is a relatively unexplored research field. The semi-structured interviews are performed according to a protocol proposed by the non-profit research organisation RAND (Harrell & Bradley, 2009). The protocol is adapted for the purpose of this research in appendix 1. It should be noticed that ideally a random sample of the community of respondents is taken. Because of the limited use CCM systems into practice, there is only a limited amount of IT auditors who have experience in this area and hence the pool of possible respondents is limited. In addition, it is desirable that the respondents are familiar with the pharmaceutical industry, which limit the amount of possible respondents even more. In total five appropriate IT auditors where found to be willing to participate in the semi-structured interviews which are presented in Table 3. Moreover, two pharmaceutical organisations were found willing to participate in the interviews which are presented in Table 4. Due to confidentiality the respondents were made anonymous and only a limited amount of background information is provided.

Table 3 - Background information IT auditors

IT auditor	Experience with CCM systems for audit purposes	Experience with SAP GRC	Experience with auditing in the pharmaceutical industry
Respondent A	No	Yes but not the PC component	Yes
Respondent B	Yes	Yes	No
Respondent C	No	Yes but not into practice	Yes
Respondent D	No	No	Yes
Respondent E	Yes but not SAP GRC PC	No	No

Table 4 - Background information pharmaceutical organisations

Pharmaceutical organisation	Top largest pharmaceutical organisations worldwide anno 2008	Familiar with SAP GRC	SAP GRC implementation
Organisation A	Top 10	Yes	Yes but not the PC component
Organisation B	Top 20	Yes	Currently in the implementation process

1.8 Research structure

As already argued for in section 1.5, this research should be classified as design science. The artifact to be designed in this research will be a set of guidelines that function as a frame of reference for assessing the adequacy if the design and operating effectiveness of a CCM system. Besides ensuring the relevance of the artifact by applying the framework for IS research as proposed by Hevner et al. (2004), the quality of the artifact will be ensured by adopting the design science research methodology (DSRM) as proposed by Peffers et al. (2007). More specifically, in this section the research structure will be elaborated on based on the DSRM.

Although this research adopts the DSRM of Peffers et al. (2007), it should be noticed that the research could be classified as a case study as well. Yin (1984, p. 23) defines a case study as "*an empirical inquiry that investigates a contemporary phenomenon within its real-life context*". The contemporary phenomenon in this research is a CCM system and the real-life context is the use of that CCM system for the purpose of the external IT audit in the pharmaceutical industry. Moreover, according to Eisenhardt (1989, p. 534), a case study research, "*typically combine data collection methods*". By making use of desk research as well as interviews, this research combines different data collection methods to form an understanding of how a CCM system should be audited.

Introduction

In the introduction phase (Chapter 1), a problem is identified which justifies the value of the artifact to be designed. According to Peffers et al. (2007) the resources required for the introduction phase include knowledge regarding the state of the art of the problem and the importance of a solution for the problem. To this end a literature review was conducted which formed the basis for the definition of the research problem. To ensure that the artifact addresses the problem and contributes to the business need, the IS research framework of Hevner et al. (2004) has been used.

Design

In the design phase, the research contribution will be laid down in the artifact to be designed. The resources needed for designing the artifact is knowledge with respect to the relevant research methodologies (Peffers et al., 2007). The research methodologies that will be used for the design of the artifact are desk research and semi-structured interviews. The design of the artifact consists of two parts. In the first part the contours of the frame of reference are designed which corresponds to the areas that are of relevance for the IT audit of SAP GRC PC (Chapter 2). The second part is concerned with the design of the guidelines which fall within the contours of the frame of reference (Chapter 3 – 6). The guidelines are designed according to a specific structure: first the guidelines itself is stated where after it is made clear how the guideline is derived with respect to the research methodologies by means of a symbol, to conclude with a discussion in which the interpretation of the author is presented. The symbols are visualised below. Finally, both parts of the design will be merged to arrive at a set of guidelines that function as a frame of reference for auditing SAP GRC PC in the pharmaceutical industry (Chapter 7).



Indicates that a guideline is derived according to interviews



Indicates that a guideline is derived according to desk research.

Evaluation

In the evaluation phase it will be evaluated whether the artifact meets its design purpose by evaluating whether the artifact addresses the problem of audit timeliness by auditing SAP GRC PC (Peffers et al., 2007). In order to do so, a plan evaluation as well as a process evaluation as described by Verschuren and Hartog (2005) will be conducted (Chapter 8). The evaluation phase will conclude by improving the artifact according to the evaluation results which will result in an improved version of the artifact.

Conclusion

Finally, the main findings of the research will be communicated in the conclusion phase which corresponds to the communication phase in the DSRM (Peffers et al., 2007). Besides the main findings, the theoretical contributions, societal relevance and contributions to the IT audit community will be stated. Furthermore, the limitations of the research will be revealed and areas for future research will be defined. Finally, a reflection on the research will be provided.

Design

2

The contours of the frame of reference

As explained in Chapter 1, the artifact that will be designed in this research is a set of guidelines that function as a frame of reference for auditing SAP GRC PC. Before the guidelines could be formulated, first it should be explored from what areas these guidelines should be derived. Because this research is focussed on the performance of an IT audit for assuring the reliability of financial statements, the areas should fall within the boundaries of performing a financial audit (2.1). Subsequently, all relevant areas will be identified and elaborated on in more detail (2.2). This chapter conclude by sketching the contours of a frame of reference and formulating sub-questions to ensure that the guidelines are formulated according the areas exposed in this chapter (2.3).

2.1 The relation between an IT audit and a financial audit

According to the scope, this research will focus on the IT audit performed in the context of assuring the reliability of an organisation's financial statements (i.e. the financial audit). In order explain the relation between IT audits and financial audits, the global audit methodology (GAM) of a Big4 audit firm will be considered. The GAM is a methodology used by external auditors for the performance of an financial audit of the assessment of an organisation's financial statements. Although the GAM itself is not established for the performance of an IT audit, as will turn out, an IT audit might be performed as part of an financial audit. The GAM encompasses four phases which are presented in Figure 6. Now each phase will be briefly explained.

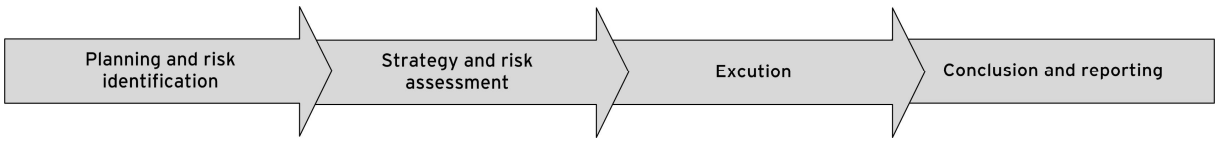


Figure 6 - GAM roadmap

Planning and risk identification

In the first phase of the assessment of the organisation's financial statements, the scope of the audit is established. The scope encompasses expectations and service requirements and is determined according to meetings with the internal stakeholders responsible for the organisation's management and governance. In this phase, the auditor is required to obtain a broad understanding of the organisation, including the nature of the business and its environment and the risks that the organisations faces. Furthermore, the risks of material misstatements due to fraud or error are identified and related to the organisation's financial statements as a whole and to relevant assertions for significant accounts and disclosures in particular.

Strategy and risk assessment

In the second phase, a combined risk assessment is made which forms the basis for determining the audit plan. Typically, in an audit plan it is made explicit which controls will be relied on by the auditor to ensure that the identified risks are sufficiently mitigated and hence assure that the organisation's financial statements are free from material misstatements. Moreover, in the audit plan the nature, timing and extent of the test of controls and substantive procedures are determined.

Execution

In the execution phase, the test of controls and substantive procedures are performed according to the audit plan. The combined risk is reassessed and it is determined whether the audit strategy should be adapted according to the change in the combined risk assessment.

Conclusion and reporting

After completion of the audit procedures, the result are communicated to those who are charged with the governance and/or management of the significant findings and issues. Moreover it will be assessed whether sufficient appropriate audit evidence is obtained to provide the auditor with reasonable assurance that the financial statements as a whole are free from material misstatements, whether due to fraud or error.

2.1.1 Positioning the IT audit within the GAM

According to the audit plan[1] as identified within the second phase of the GAM, relevant controls which are part of the internal control structure of an organisation are tested to assess whether the identified risks are sufficiently mitigated to assure that the organisation's financial statements are free from material misstatements. Due to process automation and technological advances the internal control structure has been drastically altered; numerous controls have been automated and new controls regarding information systems have be established. The role of the IT auditor is to assess the controls with respect to the organisation's IT environment that are of relevance for assuring the reliability of the organisation's financial statements. This is how the performance of an IT audit is positioned within the GAM. To illustrate this point consider, an segregation of duties (SOD) control. A SOD control should prevent fraud due to the misappropriation of assets by separating the duties of having access to the asset and being responsible for maintaining the accountability of the asset. Due to process automation, the controls used to ensure segregation of duties might be based on IT or even fully automated. Consequently, the financial auditor relies on the assessment of the SOD control made by the IT auditor. After all, assessing controls related to IT are the responsibility of the IT auditor (Gantz, 2013). It should be clear that the construction of an audit plan for auditing SAP GRC PC in the context of assuring an organisation's financial statements should fit within the boundaries of the GAM.

2.2 Designing a frame of reference

Now that it is made explicit that the design of a set of guidelines, which function as a frame of reference for the construction of an audit plan to perform an IT audit regarding SAP GRC PC should fit within the boundaries of the GAM, the contours of the frame of reference might be drawn. A first sketch of the outline of the framework was made according to information derived from the GAM and IT audit methodology literature (Gantz, 2013; Lindgreen et al., 2005; Van Praat & Suerink, 2013). The first sketch of the outline of the framework was used to structure the interviews with the IT auditors. Based on their responses, the draft outline was updated. Eventually it appears that guidelines are desirable in four areas: (1) pharmaceutical business environment, (2) processes, risks ad controls, (3) SAP GRC PC technology, and (4) organisational embedding. These areas are visualised in Figure 7. It should be noticed that the arrow from the audit methodology to the audit plan itself is not a separated area. However, what aspects of the audit methodology should be included in the audit plan is certainly of relevance and is implicitly determined according to the four areas. Moreover it should be noticed that Figure 7 is a more detailed representation of Figure 4. Now each area of the frame of reference will be further elaborated on.

[1] It should be noticed that this audit plan is established for the performance of a financial audit and not for an IT audit.

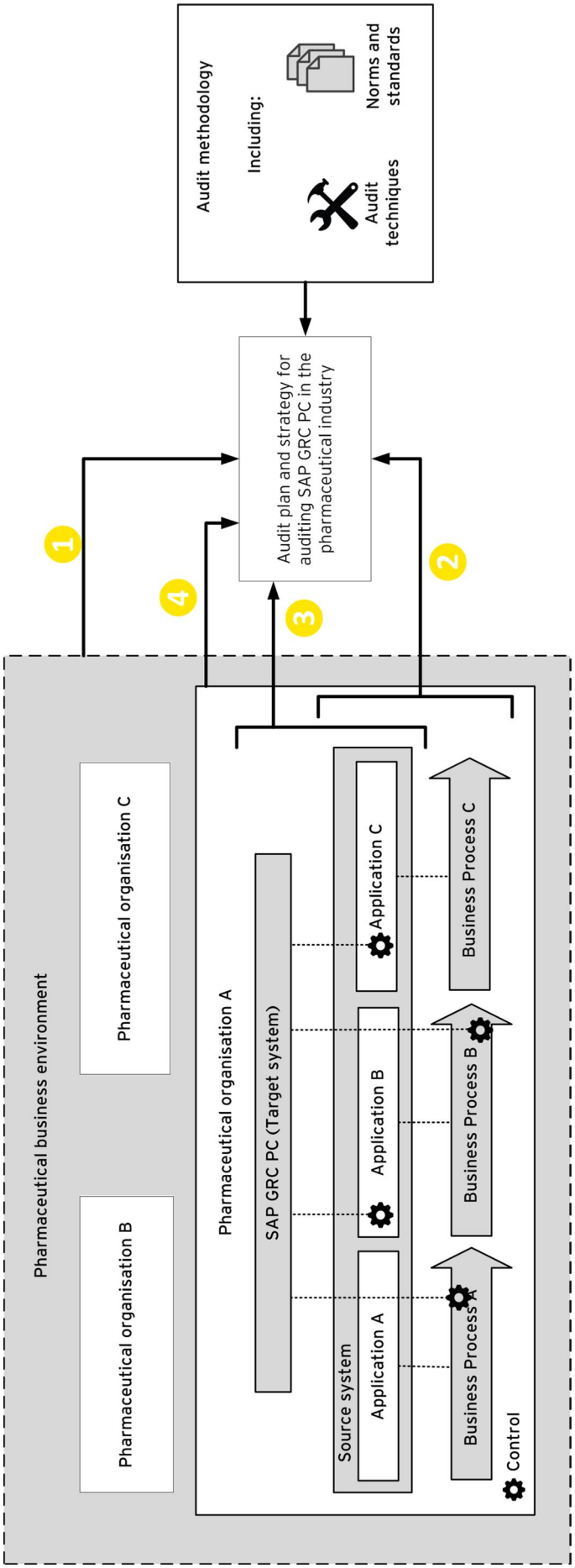


Figure 7 – Deriving the contours of a frame of reference

2.2.1 Understanding the businesses environment

Understanding the organisation's business environment is the first area which should be addressed by the IT auditor for auditing SAP GRC PC and corresponds to arrow one in Figure 7. The IT auditor should understand the core business of the organisation in order to determine what processes, risks and controls are relevant, with respect to SAP GRC PC, to be included in the audit plan and which not. Therefore, it is of importance to understand the business environment in which the organisation is operating. Beforehand it is not expected that gaining an understanding of the business environment will significantly differ for the audit of SAP GRC PC compared to other audit objects. Consequently, the way IT auditors form an understanding of the business will only be slightly addressed in this research.

It appears to be more interesting for the IT auditor to understand how organisations intend to use SAP GRC PC within the pharmaceutical industry. Therefore, industry specific trends will be revealed and drivers and barriers of pharmaceutical organisations to implement SAP GRC PC will be identified. The trends, drivers and barriers will be derived according to the interviews with the pharmaceutical organisations. Because SAP GRC PC is implemented to a very limited extent, IT auditors are relatively unfamiliar with the motivations of pharmaceutical organisations to adopt SAP GRC PC. This unfamiliarity might result in misperceptions between pharmaceutical organisations and IT auditors with respect to the use of SAP GRC PC. Therefore, an attempt will be made to reveal these misperceptions. To this end, the interviews with IT auditors will be taken into account as well.

It should be noticed that exploring industry specific trends, drivers, barriers, and misperceptions are not an area for the frame of reference for which guidelines should be derived. However, they might influence the activity of understanding the business environment. Consequently, they have to be interpreted as context for the understanding the business.

2.2.2 Processes, risks and controls

After the IT auditor has gained an understanding of the business, all relevant processes, associated risks and mitigating controls should be identified which corresponds to arrow two in Figure 7. The auditor determines which processes result in a significant account on the organisation's financial statements. Subsequently, the risks within these processes are identified where after it will be assessed whether these risks are sufficiently mitigated by controls in order to provide reasonable assurance that the financial statements are free from material misstatements. This audit activity is extensively discussed in the GAM and especially process analysis and risk identification are not likely to significantly differ for performing an IT audit regarding SAP GRC PC. As will be argued, the assessment of controls might be different since the operating effectiveness of the controls will be assessed by means of SAP GRC PC. Now all three components will be discussed in more detail.

Process analysis

A process is defined as "*a specific ordering of work activities across time and space, with a beginning and an end, and clearly defined inputs and outputs*" (Davenport, 1993). By analysing the processes, the IT auditor determines which processes should be included in the audit plan and which not. Because the research is focused on the performance of an IT audit in the context of the organisation's financial statements, the processes that result in a significant account on the organisation's financial statements will be included in audit plan. Beforehand it is expected that there will not be a lot of differences in analysing the organisation's processes in comparison with other audit objects since SAP GRC PC does not directly affect the functioning of a process itself; CCM only allows monitoring data that is created or altered by means of process activities. Moreover, the identification of processes in relation to financial statements is extensively elaborated on in the GAM. Therefore, it is expected that only a limited amount of guidelines will be derived.

Risk identification

After the analysis of relevant processes, the risks within these processes will be identified. IT auditors should assure themselves whether the organisation has properly acknowledged all the risks, and whether the risks are correctly classified in accordance with their impact. Risks are identified by performing so called walkthroughs of the processes. Since the IT audit is performed in the context of the organisation's financial statements, the walkthrough should be performed in conjunction with financial auditors. The role of the IT auditor is here to explore the risks originating from the use of IT

that might affect audit risk which is "*the risk that the auditor expresses an inappropriate audit opinion whether the financial statements are materially misstated*" (IFAC, 2009a, p. 73). Explanatory notes on audit risk are provided in appendix 2. In a walkthrough, the auditors go step by step through the processes in order to identify all relevant risks. Often the risks identified by the auditors are compared with the risks that are recognized by the organisation. Any deviations between both risk assessments will be discussed. The result of the risk identification is that the organisation and the auditors agree on the relevance an significance of all risks.

Risks are inextricably connected to business processes. Eliminating all risks is utopia. Therefore, the auditors assesses whether the risks correspond to the organisation's risk appetite. Risk appetite can be defined as "*the degree of risk, on a broad-based level, that a company or other organisation is willing to accept in pursuit of its goals. Management considers the organisation's risk appetite first in evaluating strategic alternatives, then in the setting of objectives aligned with the selected strategy, and in developing mechanisms to manage related risks*" (COSO, 2004, p. 2). The auditors determine whether the organisation's exposure to risks is consistent with the organisation's risk appetite.

The identification of risks should be executed regardless of the audit object. Therefore, it could be expected that risk identification does not significantly differ in the audit of SAP GRC PC relative to other audit objects. However, because this research is focused on a specific industry, this creates opportunities to consider risks that are of particular relevance within the pharmaceutical industry in terms of the organisation's financial statements.

Control assessment

Although eliminating all risks is not possible, there are risk mitigation strategies which could be used to align the overall risk of an organisation with its risk appetite. Roughly, there are four risk mitigation strategies: accept the risk, eliminate the risk, share the risk or control the risk (GTAG, 2012). The strategies are elaborated on in Table 5. Considering the purpose of this research, only the "control the risk' strategy will be taking into account.

Table 5 - Risk mitigation strategies adopted from GTAG (2012, p. 12)

Mitigation strategy	Description
Accept the risk	"Some risks are minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate as well as periodically reviewing the risk to ensure its impact remains low."
Eliminate the risk	"It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors."
Share the risk	"Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the risk to an insurance provider."
Control the risk	"Instead of – or in combination with – other options, controls may be devised and implemented to prevent the risk from manifesting itself to limit the likelihood of this manifestation or to minimize its effects."

The main purpose of having controls is to mitigate risks. It is the responsibility of the auditor to assess the internal control structure of the organisation to determine whether the risks are properly mitigated and hence the reliability of an organisation's financial statements could be assured. Internal control can be defined 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 (1) effectiveness and efficiency of operations (2) reliability of financial reporting, and (3) compliance with applicable laws and regulation*" (COSO, 1992, p. 3). It is not likely that all controls are of relevance for assuring the reliability of the financial statements. Consequently, the auditors should determine which controls are of interest and should be included in the audit plan. After the relevant controls are identified, the controls will be assessed by testing their design adequacy and operating effectiveness. If the adequacy of the design and operating effectiveness is sufficient, this reduces the control risk and hence the audit risk as can be derived

from the ARM as explained in appendix 2. It should be noticed that SAP GRC PC provides continuous insight in the operating effectiveness of a control during a specified period of time. However, SAP GRC PC does not provide insight in the adequacy of the design. The direct advantage of using SAP GRC PC for the external audit is the increased insight into the operating effectiveness of all monitored controls. Consequently the operating effectiveness of the controls could be assessed with a more consistent level of assurance and hence might increase the quality of an audit. Controls can be classified in various ways (GTAG, 2012). From the perspective of the IT auditor, the internal control structure is most often approached by the model as presented in Figure 8. The components of the model are well-known to practitioners and academics in the field of auditing. Therefore, the explanatory notes on the model are transferred to appendix 3.

As opposed to analysing the processes and identifying risks, SAP GRC PC directly affects the assessment of controls because the operating effectiveness of the controls is monitored automatically on a real-time basis. Assessing the operating effectiveness is extensively prescribed in the GAM. However, at this moment it is unclear how the assessment of the operating effectiveness of a control by means of SAP GRC PC influences the audit procedures as described in the GAM. Because of the serious impact of SAP GRC PC on the internal control structure of an organisation, it is believed that various guidelines are needed for assessing the controls.

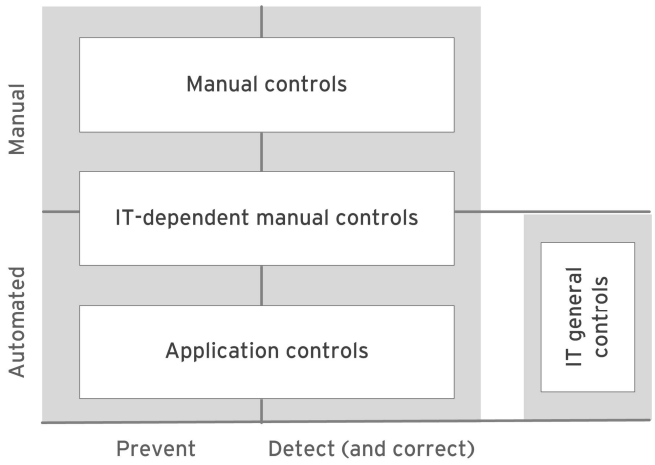


Figure 8 - internal control structure adopted from the GAM

2.2.3 Technical aspects

After the IT auditor has analysed the relevant processes, identified the associated risks and assessed whether these risks were properly mitigated by controls, the IT auditor should assess the technical aspects of SAP GRC PC which corresponds to arrow three in Figure 7. It should be noticed that this area is new for IT auditors since CCM systems are quite novel, especially for the purpose of the external IT audit. The lack of experience of IT auditors with SAP GRC PC increases the need for guidelines. Consequently, it is expected to derive numerous guidelines regarding the relevant technical aspects that should be included in the audit plan and be part of the audit strategy. Because this area is at this moment largely unexplored, the guidelines that will be derived are considered an important contribution of this research. As regards to the technological aspects, two areas will be explored. First the contours of the frame of reference regarding the technical architecture will be sketched where after the contours of regarding the establishment of the CCM functionality will be drawn.

Technical architecture

Kuhn and Sutton (2010) provide a clear overview of the three different technical architectures that could be distinguished to establish a continuous monitoring functionality. An overview is presented in Table 6.

Table 6 - Three architectures to establish continuous monitoring adapted from Kuhn and Sutton (2010)

Architecture	Definition
Embedded Audit Module (EAM)	EAMs prescribe "coding of audit procedures directly into the auditee's host system to facilitate real-time monitoring and reporting of transactions and system settings" (Kuhn & Sutton, 2010, p. 94)
EAM Ghosting	"Ghosting entails operating a "copy" of an entire system on separate hardware, including data and system settings, in a real-time fashion similar to an instantaneous fail-over common to disaster recovery and business continuity planning procedures and redundant firewall systems" (Kuhn & Sutton, 2010, p. 95)
Monitoring Control Layer (MCL)	"The MCL approach take the continuous auditing system and "hooks" it into the client's existing enterprise system, generally using a middleware layer to integrate loosely coupled applications such as ERP systems, legacy systems, and web-based applications" (Kuhn & Sutton, 2010, p. 95)

The technological architecture of SAP GRC PC corresponds to the MCL architecture. The MCL architecture was proposed by Vasarhelyi et al. (2004). The first two efforts on exploring the viability of MCL into practice were aimed at the German manufacturing conglomerate Siemens AG (Alles et al., 2006; Alles et al., 2008) and the former American telecom operator WorldCom (Kuhn & Sutton, 2006). Alles et al. (2006) implemented a continuous auditing system for continuous monitoring of business process controls (CMBPC) in a live environment at Siemens AG, whereas Kuhn and Sutton (2006) designed a continuous auditing system for testing financial transactions in the aftermath of the bankruptcy of WorldCom. Before identifying the architectural aspects that are of relevance for the assessment of SAP GRC PC, two notions should be made. First of all, technically speaking, MCL cannot provide continuous monitoring and hence continuous reporting since the monitoring systems is hooked into the system being monitored (Kuhn & Sutton, 2010). However, the delay in monitoring is considered negligible and hence in this research it is assumed that SAP GRC PC could monitor continuously as well. Second, the researches described above adopting the perspective of the internal auditor whereas this research takes the perspective of the external auditor. Consequently, this research is aimed at exploring whether the external IT auditor could rely on the output of SAP GRC PC which is already implemented by the internal auditor.

Based on the above discussed literature and SAP GRC PC documentation, a high level description of the technical architecture needed to perform CCM by means of SAP GRC PC is provided. The business processes of an organisation are supported by information technologies which are used for processing information electronically. The environment in which these technologies are deployed is referred to as the organisation's IT environment. In Figure 9, the components of the IT environment which are required for establishing CCM by means of SAP GRC PC are presented. It should be noticed that this figure is a more detailed representation of Figure 3 as presented in section 1.1.5. Furthermore, the figure is not a complete overview of the organisation's IT environment since only the components relevant for CCM are taken into account. When implementing SAP GRC PC, it is assumed that the information technologies used to support the organisation's business processes are already established. Moreover, it is assumed that the organisation already has an internal control structure in place. Based on the Figure 9, three architectural aspects appears to be of relevance for the performance of an IT audit OF SAP GRC PC: the source system, the interface, the target system. Now all three aspects will be elaborated on in more detail.

The source system

The monitored systems are referred to as *source systems*. The data which is the objective of the monitoring activity resides in databases within the source system. SAP GRC PC, can be connected to various kind of source systems simultaneously (e.g. ERP, CRM) provided by different software vendors (e.g. SAP, Oracle, Microsoft). A source system might be used to manage and process master data (CCM-MD) and transactional data (CCM-T) for certain business processes. Furthermore, a source system could be used for the configuration of automated controls and hence contains database tables with configuration data (CCM-AC) . SAP GRC PC, which is referred to as the target system, is connected to the source system via a connector.

The interface

The connector is also denoted as the interface between the target system and the source system. It should be noticed that no data is transferred from the source system to the target system. The interface only enables the target system to perform monitoring functionality on the data which resides in the source system. The type of interface is dependent on the source system. In order to establish the interface, either a turnkey connection (e.g. RFC, ODBC) or a homemade connection could be used.

The target system

The target system (i.e. SAP GRC) consists of a backend and a frontend. Besides the interfaces, the backend consists of the GRC suite which is connected to the SAP GRC database. Within the SAP GRC suite, various components could be deployed (e.g. PC, AC, RM). For establishing the CCM functionality, at least the PC component should be implemented. The SAP GRC suite is used to access the data within the source systems and to perform analysis on this data. The data that should be analysed and the different kind of analysis that should be performed are determined and formulated by users and stored in the SAP GRC database via the dashboard in the frontend. In this way the SAP GRC suite, which is connected to the SAP GRC database as well, is instructed on how to execute the monitoring activities. The results of the analysis are stored in the SAP GRC database. In the frontend, the user arranges the monitoring activity by designing the analysis. These analysis will be made accessible for the SAP GRC suite by storing them in the SAP GRC database. Moreover, via the dashboard in the frontend the user determines how the monitoring results should be presented and communicated through the organisation.

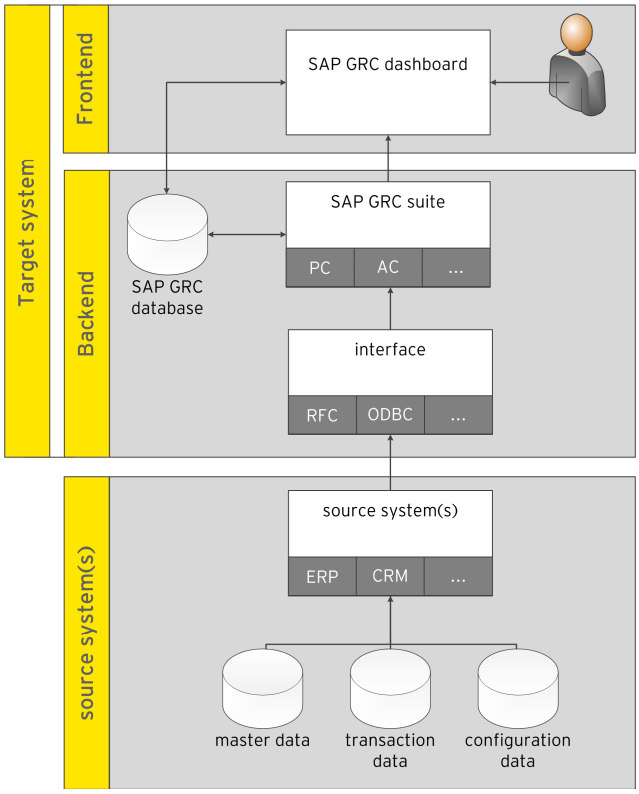


Figure 9 - IT components required for establishing CCM by means of SAP GRC PC

Technical aspect of CCM functionality

Now that a high level description of the technical architecture of SAP GRC PC is provided, in this section it will elaborated how the technical components could be used to continuously monitor controls. In order to establish the CCM functionality, five steps should be taken consecutively (Sudhalkar, 2011). The first step is for a user to define a data source and business rule. A *data source* could be considered a description of source data. In such a description, metadata such as

data type, name, and the source path to locate the data in a source system is provided. Data sources tell SAP GRC PC where the source system is located, how to authenticate itself to the source system, and how the data which resides in the source system should be accessed. A data source provides its metadata to a business rule. A *business rule* is specified by a user and encompasses the actual monitoring logic. In a business rule the user defines problem situations which are referred to as deficiencies. The design of a business rule is dependent on the kind of source data and hence on the data source. It should be noticed that a business rule can be applied to only one data source, but one data source could be used for multiple business rules. Designing business rules is a highly complex activity for which a lot of knowledge concerning SAP GRC PC as well as knowledge about the source systems is required. The second step is to map a business rule to a control. It is a prerequisite that the controls and accompanied risks and business processes are clearly described in SAP GRC PC. Depending on the type of CCM functionality (CCM-T, CCM-MD, or CCM-AC), the business rule is mapped to a different type of control (transactional-, master data-, or configuration-control). After the business rule is mapped to the corresponding control, the third step is to actually monitor the controls. In SAP GRC PC, there are two main monitoring methods: query-driven and event-driven monitoring. The methods are visualised in Figure 10. In query-driven monitoring the monitoring activity is initiated by SAP GRC PC itself. The frequency of monitoring could be scheduled by the user. In event-driven monitoring, an external system which is referred to as the event engine, initiates the monitoring activity. The event engine recognizes predetermined events and when they occur, the engine communicates to SAP GRC PC. The fourth step is to analyse the results, which is done in the SAP GRC suite, and remediate any deficiencies. After a deficiency is identified, it is communicated to the responsible instance according to a predefined protocol. SAP GRC PC keeps track whether a deficiency is resolved or not. The protocols are considered an important part of the monitoring activity and will be further elaborated on in Chapter 5. The last step is to actually report the findings of the analysis performed in previous step.

According to the description of the CCM functionality of SAP GRC PC, the monitoring aspects that should be taken into account for the performance of an IT audit are data integrity, business rules, and management of SAP GRC PC. Now all three aspects will be elaborated on in more detail.

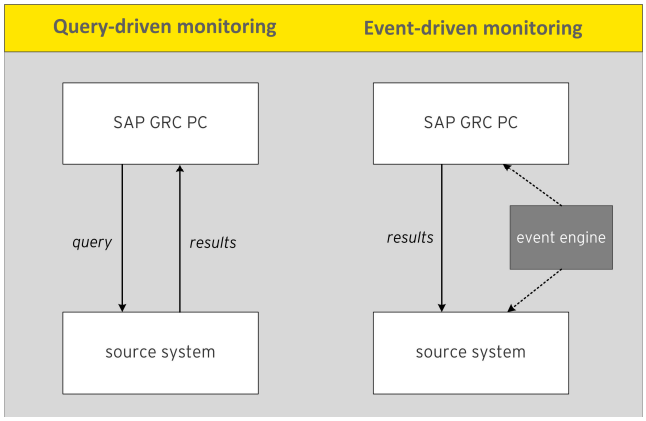


Figure 10 - query-driven monitoring versus event-driven monitoring

Data integrity

A first aspect that should be taken into account is data integrity. Data integrity seems to be of importance since CCM is monitoring a control based on data. Obviously, when the data being monitored has no integrity, the output of CCM is useless and could be even misleading.

Business rules

A second aspect that appears to be of importance are the business rules. Especially the business rules which monitor controls that mitigate risks that are significant in terms of an organisation's

financial statements will be of interest. An organisation is likely to have business rules to monitor other controls as well. The IT auditor should determine which controls and accompanied business rules are useful in terms of the audit. Therefore the IT auditor cannot claim to build on an organisation's CCM functionality in general. The IT auditor should always apply nuances to a certain claim by motivating which business rules will be used for the IT audit in the context of assuring the reliability of an organisation's financial statements and why. After exclusion of the irrelevant business rules the IT auditor should audit the residual ruleset.

Management of SAP GRC PC

Besides ensuring data integrity in the case of CCM-T and assessing the business ruleset, the IT auditor should also gain insight into the reliability of the target system itself. It could be that a business rule is properly functioning today, but the IT auditor want the assurance that the rule was properly functioning during a specific period of time. In order to ensure the reliability of the target system, the ITGCs of SAP GRC PC itself should be assessed. The ITGCs which are currently included in the GAM of a Big4 audit firm are believed to be applicable for the IT audit of SAP GRC PC because they are not considered strict norms. The ITGCs in the GAM are referred to as Primary Control Procedures (PCPs) which are flexible and leave room for professional judgement of the IT auditor. Because of this flexibility, it is believed that they are appropriate for the audit of SAP GRC PC although not all of them are of equal relevance.

2.2.4 Communication of monitoring results and audit findings

After the IT auditor has assessed the technological aspects of SAP GRC PC, it should be assessed whether the monitoring results are properly communicated to the responsible instances which corresponds to arrow four in Figure 7. There are two types of communication, the first is referred to as organisational embedding and is about the communication of monitoring results to all relevant entities within the organisation and external entities such as the IT auditor. Second, there is the communication of the result regarding the IT audit from the external IT auditor to the relevant entities within the organisation. The organisational embedding is an unexplored territory since currently SAP GRC PC is only to a limited extent implemented within organisations. Therefore it is expected to derive various guidelines to guide the auditor what aspects should be included in the audit plan for performing an IT audit regarding SAP GRC PC. Besides the communication of the monitoring results, although not directly of relevance with respect to the financial audit, the IT auditor might also assess whether the deficiencies are properly dealt with within the organisation. With respect to the reporting of the findings of the IT audit to the organisation, it is not expected to derive numerous guidelines. Although the content of the results might be different, the communication of the results is likely to remain the same. Because the assessment of the organisational embedding is an unexplored area, it will be elaborated on in the following paragraph.

Organisational embedding

Organisational embedding refers to the use of SAP GRC PC inside an organisation. By assessing the organisational embedding, the IT auditor ensures himself that all deficiencies are properly followed up by the right entity within the organisation. Especially the follow up regarding the communication of the monitoring results to the right entities (i.e. external IT auditor) are of relevance. Inside the organisation, various stakeholders (e.g. compliance team, internal control specialists, internal auditors, quality inspectors) are involved in managing risks and operating controls. These stakeholders are positioned in different departments across the organisation and have different perspectives on risk and controls. Consequently, just having a proper risk and control framework being monitored by means of SAP GRC PC is not sufficient, the challenge is to coordinate the collaboration between all stakeholders to use SAP GRC PC to its full potential. Therefore, it is of importance that clear boundaries and responsibilities are defined to adequately mitigate risks and operating controls. This is where the Three Lines of Defense model comes into play. The model "*provides a simple and effective way to enhance communications on risk management and control by clarifying essential roles and duties*" (IIA, 2013, p. 2). The motivation for using the Three Lines of Defense model is because the model is acknowledged by Big4 audit firms (EY, 2013; PwC, 2015b) as well as diverse audit institutions (IIA, 2013; ISACA, 2011) as a best practice model. Because the

model is used as best practice, it should be noticed that the model describes an ideal situation whereas in practice, organisations might not have defined responsibilities and strict boundaries between the stakeholders in such an accurate manner. Nevertheless, the Three Lines of Defense model will be used in this research to derive guidelines concerning the assessment of the organisational embedding of SAP GRC PC by the external IT auditor. An overview of the Three Lines of Defense model[2] is presented in Figure 11. Because the specifics of the model are well-known to practitioners and academics in the field of auditing, explanatory notes are transferred to appendix 4.

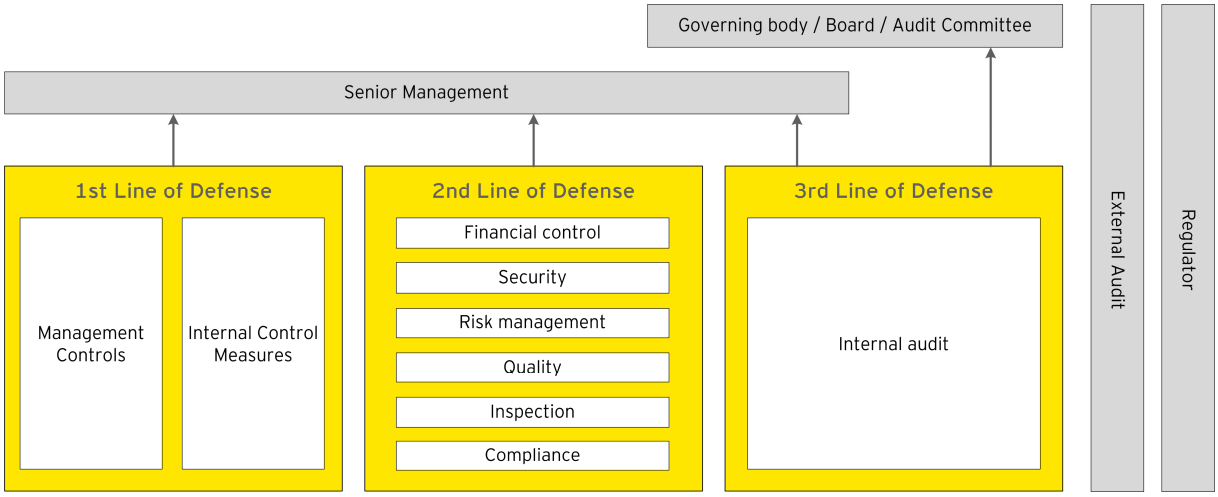


Figure 11 - Three Lines of Defense model adapted from IIA (2013, p. 2)

With the CCM functionality of SAP GRC PC, the operating effectiveness of a control could be monitored continuously, which relates to the activities of the operational management. Consequently, SAP GRC PC will be operated and maintained by the first line of defense. However, the output of the monitoring activity is relevant for all other entities in the model. For instance, the second line of defense might use the results of the monitoring activity for compliance purposes whereas the internal audit team as well as the external audit team rely on the monitoring results to independently assess the functioning of the risk and control structure of the organisation. The governing body and senior management will use the insights derived from the monitoring activity for strategic purposes. Moreover, the monitoring results have to be communicated to the external IT audit which is of particular relevance with respect to the purpose of this research. The Three Lines of Defense model will be used to substantiate guidelines derived from to the semi-structured interviews and desk research.

2.3 Conclusion

According to the findings from previous section the contours of the frame of reference are visualised in Figure 12. The frame of reference identifies the areas that should be addressed while constructing the audit plan in order to assess the adequacy of the design and operating effectiveness of SAP GRC PC. The guidelines that will be derived in the upcoming chapters should be established with respect to the identified areas as presented in Figure 12. There appear to be four relevant areas: the business environment; processes, risks and controls; technical aspects; and communication. The following four chapters each cover an identified area. It should be noticed that the use of SAP GRC PC within the pharmaceutical industry itself is not an area of interest but provide context to understanding the business environment. Consequently the industry specific trends, drivers and barriers for implementing SAP GRC PC, and misperceptions between IT auditors and pharmaceutical

[2] The name of the Three Lines of Defense model is based on a military metaphor in which a fortress has established various lines of defense to arm against the enemy. In this metaphor, the fortress represents the organisation and the enemy is the occurrence of a risk. The means to arm against the enemy are the controls which are operated by different stakeholders in the organisation which corresponds to the lines of defense.

organisations will be discussed in the business environment chapter. Furthermore, it should be noticed that the arrows between the areas imply a certain order in which the IT audit should be performed. This order follows logically from the performance of an audit in general as suggested within the GAM. Although all areas are relevant for the performance of an audit regarding SAP GRC PC, the aspects marked in yellow are of special interest since they are either new or should be approach in an alternative way compared to the audit of other audit objects. In order to derive relevant guidelines, numerous sub-questions are composed according to the identified frame of reference. The sub-questions are presented in Table 7.

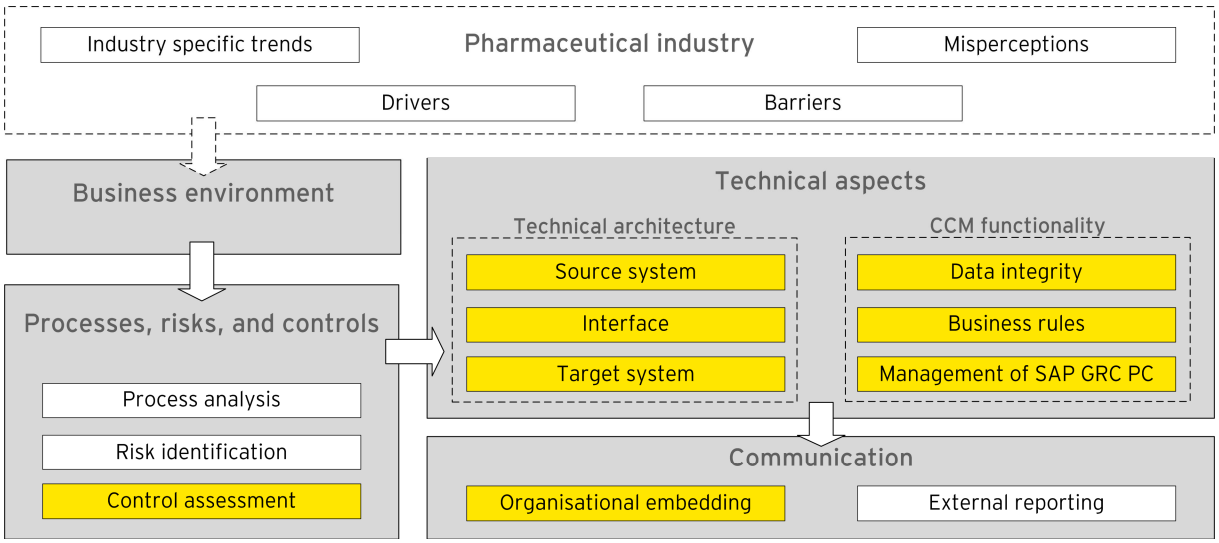


Figure 12 - Contours of the frame of reference

Table 7 - Sub-questions overview

Chapter	Sub-question	Output
3. Business environment	What are the relevant guidelines regarding business environment understanding in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
	What are the industry specific trends underlying the implementation of SAP GRC PC according to pharmaceutical organisations?	Trends
	What are the drivers for implementing SAP GRC PC according to pharmaceutical organisations?	Drivers
	What are the barriers for implementing SAP GRC PC according to pharmaceutical organisations?	Barriers
	What are the misperceptions regarding the drivers and barriers between IT auditors and pharmaceutical organisations?	Misperceptions
4. The interplay between processes, risks and controls	What are the relevant guidelines regarding process analysis in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
	What are the relevant guidelines regarding risk identification in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
	What are the relevant guidelines regarding control assessment in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
5. Technical aspects	What are the relevant guidelines regarding the technical architecture in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
	What are the relevant guidelines regarding the CCM functionality in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
6. Communication	What are the relevant guidelines regarding the organisational embedding in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
	What are the relevant guidelines regarding external reporting in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines

3

Business environment

According to the outline of the frame of reference as identified in Chapter 2, first the guidelines with respect to understanding the business environment will be identified (3.1). The guidelines will be derived according to the sub-questions as presented in Table 8. Beforehand it is not expected to derive a lot of guidelines in this area since understanding the business environment is not believed to be significantly different relative to other audit objects. The guidelines are derived according to the interviews with IT auditors of which their background is presented in Table 3 in section 1.7. Furthermore, industry specific trends (3.2) along with the main drivers (3.3) and barriers (3.4) for the implementation of SAP GRC PC will be derived to explore how pharmaceutical organisations intend to use SAP GRC PC. Moreover, the misperceptions between IT auditors and pharmaceutical organisations will be revealed (3.5). The trends, drivers, barriers and misperceptions are identified according to the interviews with pharmaceutical organisations of which background information is provided in Table 4 in section 1.7. All insights are presented according the structure as elaborated on in section 1.8.

Table 8 - Sub-questions Chapter 3

Section	Sub-question	Output
3.1 Understanding the business environment	Are there relevant guidelines regarding business environment understanding in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
3.2 Industry specific trends	What are the industry specific trends underlying the implementation of SAP GRC PC according to pharmaceutical organisations?	Trends
3.3 drivers to implement SAP GRC PC in the pharmaceutical industry	What are the drivers for implementing SAP GRC PC according to pharmaceutical organisations?	Drivers
3.4 barriers to implement SAP GRC PC in the pharmaceutical industry	What are the barriers for implementing SAP GRC PC according to pharmaceutical organisations?	Barriers
3.5 Misperceptions between IT auditors and pharmaceutical organisations	Are there any misperceptions regarding the drivers and barriers between IT auditors and pharmaceutical organisations?	Misperceptions

3.1 Understanding the business environment

Guideline 1: Understanding the business environment does not significantly differ in the case of auditing SAP GRC PC

All five respondents acknowledged that understanding the business environment does not significantly differ for auditing SAP GRC PC relative to other audit objects because an understanding of the business should be formed regardless of the audit object (Respondents A – E).

According to the interviews with IT auditors, it could be concluded that there are no significant differences in the audit of SAP GRC PC when it comes to gaining an understanding the organisation's business environment.

Guideline 2: The organisation's strategy should be considered in terms of IT changes which might affect the monitoring functionality of SAP GRC PC

The IT environment is subjected to change. These changes could have various causes. For instance, as noted by respondent B, it could be that the organisation is planning to automate certain processes which might result in changes to the operating model and processes which will affect the activities of the IT auditor in the future. Furthermore, the organisation might change or abolish certain automated processes which should be taken into account by the IT auditor for considering whether the IT audit activities provide sustainable results (Respondents A, C and E). Another example is the situation in which an organisation acquires another business. Consequently, the acquired processes will become part of the IT environment of the organisation which will be of influence on the activities of the IT auditor (Respondents A and B)

On first sight, the organisation's strategy seems not to be of influence on the audit activities because the audit activities take place in a retrospective fashion and the strategy of an organisation is by definition focussed on the future. However, annual IT audit activities often are part of a multiannual audit plan. Therefore, it could be argued for considering the strategy of the organisation of interest anyway. Considering the organisations strategy is of relevance because it could contain evidence that the IT environment is going to change in the future. These changes might be the result of process automation (Respondent B), process changes or abolishment (Respondents A, C and E), or process integration (Respondents A and B). If these changes are stated, implicitly or explicitly, in the strategy of the organisation, the IT auditor should be aware of this. This is of relevance since IT changes might affect the monitoring functionality of SAP GRC PC. For instance, it could be that the database tables are renamed due to changes made to the source system. Consequently, the business rules might monitor a non-existent database table. To make the IT auditor aware of such pitfalls in the performance of an IT audit regarding SAP GRC PC it is of relevance to consider the organisation's strategy in terms of IT changes that might cause the monitoring functionality to fail.

3.2 Industry specific trends

Trend 1: Pharmaceutical organisations have recently acquired various smaller companies to strengthen their business

Organisation A has acquired numerous other companies in the past which resulted in the proliferation of local affiliates.

Organisation B has not directly acquired other companies but does recognize the acquisition trend. Instead organisation B makes intensive use of partnerships. Furthermore organisation B noted that currently the market seems to consolidate.

According to the interviews, there seems to be an acquisition trend among big pharmaceutical organisations. At this moment the market seems to consolidate, however the organisations still have to deal with the aftermath of the acquisitions. This is of relevance for the external IT audit of SAP GRC PC since acquisitions result in a diversified IT landscape in which various legacy systems reside. Consequently, it is more complex to establish the monitoring functionality if controls in different source systems should be targeted.

Trend 2: Pharmaceutical organisations seems to make increasingly use of IT outsourcing

As stated by organisation A, they possess a large amount of legacy systems due to the acquisition trend. The global office of the organisation is currently integrating all the legacy

systems into a single ERP instance which is outsourced to an external party. This party is responsible for the application management support as well as managing the infrastructure of the global system. Outsourcing implies that all the processes and procedures supported by the legacy systems of the affiliates has to be adapted to become suitable for outsourcing. Internally, organisation A will create internal control teams which are familiar with all the ins and outs of the local business processes and communicate directly with the outsourcing party. This includes educating the outsourcing party how the business processes should be supported by IT. Consequently, a change of minds of the employees of the pharmaceutical organisation is needed because their proceedings will change.

Organisation B is currently in the process of changing service provider globally. This service provider is responsible for the establishment of the IT infrastructure and operation of various applications. Organisation B stated that the changing process was significantly delayed.

According to a report on the outsourcing trend among pharmaceutical organisations as provided by PwC (2015a, p. 1) it was stated that "Pharmaceutical companies have moved up the value chain for outsourcing from non-core functions, such as IT and Human Resources, to secondary core functions, such as R&D and manufacturing"

So a second trend, which is encountered by both the organisations being interviewed, is the intensive use of IT outsourcing. Whereas organisation A explicitly stated that they are planning to increase their IT outsource activities, organisation B already has outsourced a great part of their IT. However, the outsourcing process of organisation B seems not to be finished yet since they are currently changing service providers. This indicates that organisation B as well has not finished the outsourcing process. Moreover, the outsourcing trend in general, including IT outsourcing, is recognized by a Big4 audit firm. Consequently, it is concluded that there is a trend among pharmaceutical organisations to make increasingly use of IT outsourcing. This is of relevance for the external IT auditor since it could be that SAP GRC PC is operated by a third party instead of internal stakeholders. This will require the IT auditor to rely on the monitoring results provided by that third party which will affect the way the IT audit is performed. For instance outsourcing might increase the risk that deficiencies are not communicated on a timely basis.

3.3 Drivers to implement SAP GRC PC in the pharmaceutical industry

Driver 1: SAP GRC PC is seen as an opportunity to reduce the amount of manual controls

As stated by organisation B, the update of their internal control framework which they associated with the implementation of SAP GRC PC is their main driver for implementing SAP GRC PC. The term update is referring to reducing their reliance on manual controls.

The first driver, which was stressed by organisation B, is to reduce the amount of manual work regarding the operation of the internal control framework[3]. Currently, organisation B has a relatively large amount of manual controls and sees the implementation of SAP GRC PC as an opportunity to automate the greater proportion of them. Although SAP GRC PC could be used for monitoring manual controls as well, the real added value is that automated controls could be monitored on a real-time basis which reduces the amount of man hours needed to operate the internal control structure. It should be noticed that the driver to reduce the amount of manual controls does not seems to originate from the need to reduce cost but merely from the need to work more efficiently and effectively.

[3] For a more elaborated discussion of the organisation's internal control framework the reader is referred to section 2.2.2.

Driver 2: SAP GRC PC could contribute to the integration of legacy systems into the organisation's existing IT environment

Because of the various acquisitions, organisation A possesses a large amount of legacy systems. According to organisation A, implementing SAP GRC PC will support the integration of legacy systems into their new IT environment and hence contributes to the consolidation of their IT landscape.

A second driver, as stated by organisation A, is that SAP GRC PC could contribute to the integration of the legacy systems into the organisation's existing IT environment. This driver is a direct consequence of the acquisition trend. By enforcing the affiliates to adapt their legacy systems in a way the underlying data structures will be suitable to be monitored by SAP GRC PC, the affiliates are implicitly enforced to align their systems in a way they could be easily integrated in the organisation's existing IT environment.

Driver 3: SAP GRC PC could be used to facilitate communication to management

According to organisation A, SAP GRC PC was globally initiated by the CIO because it facilitates communication to management.

A third driver which was recognized by organisation A is that SAP GRC PC could be used to facilitate communication to management. Because the pharmaceutical organisation is active around the globe, it might be difficult for the organisation's global management to get an overview of all the details at local sites. The reporting functionality of SAP GRC PC could be used to inform the organisation's global management about risk management and the operation of the control structures at local sites. Furthermore, the reports could be used to substantiate strategic decision making on a global level.

3.4 Barriers to implement SAP GRC PC in the pharmaceutical industry

Barrier 1: Different interests among the various quality assurance and compliance teams complicates the implementation of SAP GRC PC

As stated by organisation B, a barrier might be to get all quality assurance and compliance teams "onto the same system, happy to be there, and using it productively". According to organisation B, in fact this barrier is more a challenge since it could be expected that the parties involved understand the benefits of SAP GRC PC in terms of automation and visibility.

The interests of the quality assurance and compliance teams might differ and so might their intention on how to use the system. It could be a barrier to align all the different interests. The fact that it could be expected from the internal teams that they recognize the benefits of having SAP GRC PC does not take away the contradictory interests itself but it might ensure that the various teams are prepared to make some concessions in aligning their interests. Although the different interests might form a barrier, it is believed that all parties involved are willing to put some effort in taking this barrier which makes is merely a challenge.

Barrier 2: The profitability of the pharmaceutical industry takes away the direct urge for implementing SAP GRC PC

According to organisation B, "Costs are not an issues since the pharmaceutical industry is very profitable. In other industries, where there is continuous cost pressure, they have to strip the manual activities out of the business and hence strip people out of the business to save money. We don't have that pressure."

First of all, this notion should be placed in context. As argued in previous section, reducing the amount of manual controls is considered a driver for organisation B for the implementation of SAP GRC PC to increase the efficiency and effectiveness of operating the internal control structure. As argued by organisation B, other industries encounter higher cost pressure which forces them to increase the cost-effectiveness of their internal control structure and hence decreases the amount of manual controls which could be accomplished by the implementation of SAP GRC PC. Because there is no direct urge to reduce the amount of manual controls in the pharmaceutical industry because of its profitability, the implementation of SAP GRC PC seems to get a relatively low priority. That does not nullify the wish of pharmaceutical organisations to work more efficiently and effectively but limited cost pressure seems to be a barrier make that wish come true. It should be noticed that this line of reasoning is only valid provided that SAP GRC PC actually reduces the amount of manual controls[4]. Another notion should be made regarding the cost pressure in the pharmaceutical industry. It is not stated that cost pressure itself is absent only that it is less relevant compared to other industries. Fact is that pharmaceutical organisations want to make a profit and hence should decrease costs as well in order to ensure their existence.

Barrier 3: The possibility of detecting misstatements might make managers reluctant to implement SAP GRC PC



Organisation B pointed out the "see no evil hear no evil" barrier. SAP GRC PC provides an increased insight in the functioning of the internal control structure of the organisation. A result could be that it turns out that some risks are not mitigated properly. In the pharmaceutical industry there is strict vigilance regulation which requires the organisations to report back any misstatements. So on the one hand the organisation wants SAP GRC PC in order to improve the internal control structure but on the other hand the organisation doesn't want to implement SAP GRC PC because they might hear something bad.

So there seems to be a see no evil hear no evil barrier which implies that an organisation is reluctant to implement SAP GRC PC due to the increased insight in the internal control structure, which might reveal misstatements. An example might be that a manager is not comfortable with having to deal with the reality of fraud risk. Than this manager might not want to hear more information regarding fraud and hence will be reluctant in supporting the implementation of SAP GRC PC. This barrier might be inappropriate because being not aware of misstatements might seriously harm the business in the future. However, according to organisation B it is a barrier that should be taken into account.

Barrier 4: The presence of legacy systems delays the implementation of SAP GRC PC



Organisation A stated that they possess numerous legacy systems which is a barrier for the implementation of SAP GRC PC. According to organisation A, the legacy systems should first be integrated into the organisation's existing IT environment. Because of this integration the legacy systems itself will disappear in the future. Monitoring a system that will disappear is a waste of effort and resources.

So the presence of legacy systems, which arises according to the acquisition trend among pharmaceutical organisations is considered a barrier. Implementing SAP GRC PC in an IT environment which is currently subjected to change because of the integration of legacy systems seems pointless. After all, when the integration process is finished, SAP GRC PC should be adapted to the changed IT environment. It should be noticed that this barrier is of temporary nature; once the IT environment is harmonised and no significant changes are planned, SAP GRC PC could be implemented. Another notion should be made that the presence of legacy systems is a barrier and a driver at the same time. As stated in section 2.2, the presence of legacy systems is a driver since it forces local affiliates to reorganize their data structures in a way the legacy systems could easily be integrated in the organisations existing IT environment. The driver is used to overcome the barrier

[4] For a more elaborated discussion of manual control the reader is referred to guideline 8 in section 4.3.

since the driver to facilitate legacy system integration reduces the barrier of having various legacy systems.

Barrier 5: Having a third party operate SAP GRC PC hinders communication and suppress the advantages of SAP GRC PC

Organisation A is increasingly making use of IT outsourcing. The barrier stated by organisation A is that in the scenario that SAP GRC PC will be outsourced, it will be a challenge to ensure that the monitoring results are communicated timely from the third party to the right entities within the organisation.

So there seems to be an additional challenge for the implementation of SAP GRC PC with respect to the IT outsourcing trend. The challenge identified by organisation A, which arises because SAP GRC PC is likely to be monitored by an external party, is that the monitoring results are not communicated timely to the right entities within the organisation. It could be questioned whether it makes sense to implement SAP GRC PC if the results of the monitoring activity are not properly communicated to the pharmaceutical organisation. The communication delay could nullify the advantage of having continuous insight into the functioning of the organisation's internal control structure. This makes the challenge a barrier. Although this barrier results from an industry specific trend, it is of structural rather than temporary nature.

Barrier 6: The low priority assigned to the implementation delays the implementation of SAP GRC PC

Organisation B encountered a prioritisation barrier. This prioritisation barrier is a direct result of the change in outsource partner. This change was significantly delayed which resulted in a backlog of IT projects. Since management prioritized other IT projects higher, the implementation of SAP GRC PC was put on hold.

The prioritisation barrier is a direct result from the outsourcing trend. Organisation B is currently in the process of changing from one outsourcings partner to another. This project was delayed and consequently numerous IT projects were put on hold. Currently the organisation is dealing with the backlog of IT projects but due to resource constraints not all projects could be executed simultaneously. The higher prioritization assigned to other IT projects is in this case a barrier for the implementation of SAP GRC PC. It should be noticed that this barrier is of temporary nature because once the backlog of project activity is eliminated, SAP GRC PC could be implemented anyway.

3.5 Misperceptions between IT auditors and pharmaceutical organisations

Misperception 1: The alignment of different views on risk and controls by various compliance teams should be interpreted as a driver instead of a barrier.

According to respondent B, SAP GRC PC should be a driver for organisations since it stimulates alignment between various compliance teams because the controls are managed within a single control repository.

A first misperception that stands out has to do with the alignment of different views on risk and controls by various quality assurance and compliance teams within the pharmaceutical organisation. As stated by respondent B, implementing SAP GRC PC should be a driver because it stimulates alignment between internal compliance teams. On the contrary, the pharmaceutical organisations themselves seems to look at the different interest across the teams as a barrier since the alignment of the interest complicate the implementation of SAP GRC PC. According to organisation B, aligning the interests between various teams might be problematic since risk assessment methodologies are conceptually as well as qualitatively different across teams. Both lines of reasoning seems to be valid and should be taken into account in the performance of the external IT audit. However, as already

stated in section 2.3, the internal compliance teams are aware of the benefits implementing SAP GRC PC. Consequently, it could be expected from these compliance teams that they are willing to put effort in aligning their different perspectives on risk and controls for the sake of implementing SAP GRC PC. This might decide the discussion in favour of the external IT auditor which wavers the relevance of barrier 1. Nonetheless, for the purpose understanding the business environment of pharmaceutical organisations, the IT auditor should be aware of both lines of reasoning.

Misperception 2: Cost savings is at least not a main driver for pharmaceutical organisations to implement SAP GRC PC

As stated by respondent B, organisations are aware of the fact that with the implementation of the SAP GRC PC, the activities of the external auditors could be reduced which will result in a reduction of audit fees. This is a driver for implementing SAP GRC PC.

As noticed by respondent E, organisations should see a possibility to earn back their investment otherwise they are not likely to procure SAP GRC PC

A second misperception that stands out has to do with financial drivers. IT auditors seem to have the idea that cost savings plays an important role in the pharmaceutical industry while in fact, according to the pharmaceutical organisations themselves, cost savings is rarely considered a key driver because the industry is very profitable. For instance, respondent B stated that organisations see the reduction of audit fees as a driver to implement SAP GRC PC. Despite the discussion whether or not a reduction in audit fees will occur, this seems of less relevance for pharmaceutical organisations. Respondent E noticed that it might be a barrier for organisations to implement SAP GRC PC when they do not recognize a genuine possibility to earn back their financial investment. According to the pharmaceutical organisations this is at least not a key barrier. It should be noticed that both respondents who explicitly mentioned the financial barriers did not have pharmaceutical organisations in their client portfolio, while the other three respondents who did not mentioned financial barriers do have audited pharmaceutical organisations. Therefore it might be concluded that cost savings is at least not a main driver for pharmaceutical organisations.

3.6 Conclusion

What are the relevant guidelines regarding business environment understanding in the IT audit of SAP GRC PC in the pharmaceutical industry?

Conform the expectation, the audit activity of gaining an understanding of the business environment seems not to significantly differ for the audit of SAP GRC PC except for one guideline. This guideline state that the organisation's strategy should be considered in terms of IT changes which might affect the monitoring functionality of SAP GRC PC.

What are the industry specific trends underlying the implementation of SAP GRC PC according to pharmaceutical organisations?

According to the interviews with the pharmaceutical organisations, two industry specific trends are distinguished. On the one hand, there seems to an acquisition trend. On the other hand there seems to be an IT outsourcing trend.

What are the drivers for implementing SAP GRC PC according to pharmaceutical organisations?

According to the interviews with pharmaceutical organisations, three drivers are distinguished. The drivers for implementing SAP GRC PC are (1) reducing the amount of manual controls, (2) enhance the integration of legacy systems, and (3) facilitate communication to management.

What are the barriers for implementing SAP GRC PC according to pharmaceutical organisations?

According to the interviews with pharmaceutical organisations, six barriers were identified which can be classified as structural barriers or temporary barriers. The structural barriers for implementing SAP GRC PC are (1) the aligning different interest between compliance and quality assurance teams, (2) lack of cost pressure, (3) the fear to discover misstatements, and (4) IT outsourcing. The barriers which are of temporary nature are (1) the presence of legacy systems, and (2) a relatively low priority to the implementation of SAP GRC PC.

What are the misperceptions regarding the drivers and barriers between IT auditors and pharmaceutical organisations?

Two misperceptions were identified when comparing the interview results of the pharmaceutical organisations with the interview results of the IT auditors. The first misperception is concerned with the alignment of different views on risk and controls by various compliance teams. Pharmaceutical organisations look at this as a barrier while IT auditors as a driver. Because the different compliance teams are believed to be willing for the implementation of SAP GRC PC to succeed, it is assumed that the alignment of interest is merely a driver. This wavers the relevance of the first barrier. The second misperception is that IT auditors might consider cost savings an important driver for pharmaceutical organisations while in fact it is at least not a main driver according to the pharmaceutical organisations themselves.

4

The interplay between processes, risks and controls

In this chapter, the guidelines regarding process analyses (4.1), risk identification (4.2), and control assessment (4.3) will be composed. The guidelines will be derived according to the sub-questions as presented in Table 9. In this chapter only the guidelines themselves will be presented, for an explanation of the audit activities the reader is referred to section 2.2.2. Beforehand it is not expected to derive a lot of relevant guidelines regarding the process analyses and risk identification since those activities are not believed to be significantly different relative to other audit objects. On the other hand, SAP GRC PC directly influences the control assessment by providing insight in the operating effectiveness and hence it is expected to acquire various guidelines regarding this audit activity. The guidelines will be derived according to desk research and interviews with IT auditors. The background of the IT auditors who participated in the interviews is presented in Table 3 in section 1.7. All insights are presented according the structure as elaborated on in section 1.8.

Table 9 - Sub-questions Chapter 4

Section	Sub-question	Output
4.1 Process analysis	What are the relevant guidelines regarding process analysis in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
4.2 Risk Identification	What are the relevant guidelines regarding risk identification in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
4.3 Control assessment	What are the relevant guidelines regarding control assessment in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines

4.1 Process analysis

Guideline 3: The identification of relevant processes does not differ in the case of auditing SAP GRC PC

All five respondents acknowledged that identifying relevant processes do not differ for auditing the SAP GRC PC relative to other audit objects (Respondents A – E).

The respondents are unanimous that the identification of relevant processes that should fall within the audit scope does not differ for auditing SAP GRC PC. The underlying line of reasoning is that SAP GRC PC itself does not affect the processes, it only monitors the controls which resides in the processes or supporting IT applications. Indeed it seems that the identification of processes stands apart from the identification of controls so there seems no evidence to doubt their statements since CCM does not affect the processes themselves.

Guideline 4: It is of relevance to understand how processes are reflected in data structures

Respondent E explicitly noticed the importance of understanding the relation between the processes and data structures within the IT environment of the organisation for auditing SAP GRC PC. The main reason to address the relation between processes and data structures is that controls used to mitigate risks within processes are often established within data structures. So to assess whether the controls are properly monitored by SAP GRC PC the IT auditor should understand how the process of interest is translated into data structures.

It might be needed that the connection between the data structures and processes should receive special attention. This could be explained as follows. Processes are supported by the organisation's IT environment. The IT environment includes "*hardware, software communications, applications, protocols, and data, as well as their implementation within the physical space, within the organisation structure and between the organisation and its external environment*" (GTAG, 2012, p. 10). Processes use or create data which is processed and stored within the IT environment. This data is actually the audit object in the IT audit of SAP GRC PC since the controls itself are represented in the data[5] or the data could be used to analyse the controls[6]. If the IT auditor determines whether controls adequately mitigate the risks associated with a process, the IT auditor should understand how these controls are represented in data structures underlying the processes. Therefore it is of relevance for the IT auditor to understand how processes are reflected in data structures.

4.2 Risk identification

Guideline 5: A broader perspective on audit risk is desirable in the performance of an IT audit

Audit risk and the associated audit risk model (ARM) is strongly embedded in the accounting profession. "Audit risk is the risk that the auditor expresses an inappropriate audit opinion whether financial statements are materially misstated" (IFAC, 2009a, p. 73). explanatory notes on audit risk and the ARM are provided in appendix 2. Despite its intensive use, the ARM has much been criticised by practitioners as well as academics. The main point of criticism is that the ARM entails a too narrow focus on risk. According to Lemon et al. (2000), the ARM is only focussed on limiting the risk that financial statements are materially misstated rather than a more comprehensive approach towards organisational risk. This narrow focus of auditors was breached with the introduction of COSO's internal control framework (COSO, 1992) which was updated with the enterprise risk management (ERM) framework (COSO, 2004). Both frameworks challenged auditors to perceive risk in a wider context than just considering accounting errors. Auditors were now considering risk at the organisational level. Another twist in the risk perception of auditors originated from the introduction of the business risk model as proposed by Knechel (2001) along with the idea that audit risk is driven by business risk (Eilifsen et al., 2001). Business risks "result from significant conditions, events, circumstances, actions, or inactions that could adversely affect the entity's ability to achieve its objectives and execute its strategies, or through the setting of inappropriate objectives and strategies" (AICPA, 2006, p. 1674). The observation that audit risk is driven by business risk might not be ground-breaking; making the connection between the risk of declining sales and the state of the general economy seems evident. However, it is argued that "in many instances, the link between business risk and audit risk were sufficiently vague and subtle, that it is unlikely that any auditor would have made the connection" (Knechel, 2007, p. 393). Although it is complex to get an understanding of the relation between business risk and audit risk, it seems key to have this understanding in order to define and implement adequate controls.

So the perspective on audit risk was two times changed over time, first with the introduction of the enterprise risk management framework and second with the notion that audit risk is driven by business risk. Whereas the enterprise risk management framework

[5] Corresponds to CCM-AC as elaborated on in Table 2 section 1.3.

[6] Corresponds to CCM-T and CCM-MD as elaborated on in Table 2 section 1.3

proposes that auditors should focus on risk at the organisational level rather than just considering audit risks as suggested by the ARM, the business audit risk model suggests that auditors should take into account business risks and focus on emanating residual risks. In the aftermath of the financial crisis, the audit profession was placed in disrepute and the adequacy of the risk models used by auditors was questioned (Power, 2009). As a result, the audit community started to increase their attention to business risk as evidenced by the issuing of ISA 315 (IFAC, 2009b). Up to the present day, audit risk plays an important role in the performance of an audit and there seems consensus that a broader view on risk, rather than just considering audit risk in isolation, is desirable.

The observation that the perspective on audit risk should be updated is supported by the findings of a panel assembled by the American Public Oversight Board (POB) who conducted a research into the applicability of the ARM into practice and concluded that the ARM was still applicable but needed "enhancing and updating" (POB, 2000). Furthermore, according to the studies of (Elder & Allen, 2003; Johnstone & Bedard, 2001; Mock & Wright, 1999), Eimers (2006) concluded that financial auditors fail to effectively respond to changing risks which implies that the auditors are not able to properly apply the ARM into practice. This does not mean that the ARM itself is inappropriate, but it raises the question whether the ARM is used well in the performance of an audit. The bottom line is that IT auditors nowadays should be aware that in some situations the usability of the ARM is limited, and that audit risk should not be dealt with in isolation but rather in combination with other risk approaches such as the ERM framework or the business risk model.

For the purpose of this research it is of particular relevance to understand how IT auditors could adopt a broader perspective on risk in the pharmaceutical industry. In the performance of an IT audit, typically three stakeholders seems to be of interest: the IT auditor, the financial auditor and the pharmaceutical organisation being audited[7]. The IT auditor assess the IT risks within the business processes of the pharmaceutical organisation on behalf of the financial auditor who is especially interested in reducing the audit risk. All three stakeholders are focussed to deal with a particular type of risk. The financial auditor deals with audit risk which was just defined in the desk research paragraph. The IT auditor assesses IT risk which is the technical risk that an organisation faces through the use of IT (GTAG, 2012). Pharmaceutical organisations deal mainly with quality risk which is the risk that a set of inherent properties of a product, system, or process does not fulfils predefined requirements (ICH, 2005). Because the activities of the three stakeholders are organised around different risks, it is important to have an understanding of the interrelations between the risks and how the risk approaches of the individual stakeholders could be aligned to avoid that these risks are managed in silos. In appendix 2, explanatory notes on audit risk, IT risk and quality risk are provided.

In the light of this research, it is of particular relevance to explore how audit risk is influenced in the pharmaceutical industry from an IT perspective. After all, it is the responsibility of the IT auditor to assess an organisation's internal control structure and supporting the financial auditor with the assessment of audit risk. Considering this notion, an overview including examples of the relations between audit risk, IT risk and quality risk is presented in Figure 13. The observations that IT risk and quality risk directly influence audit risk might be obvious, though it is not directly the responsibility of the IT auditor to assess the relation between quality risk and audit risk. It becomes more interesting when considering how IT risk influences audit risk via quality risk. Although this might not be a ground-breaking observation, an IT auditor should be aware of this subtle indirect relation. As can be seen in Figure 13, two examples of the relation from IT risk via quality risk to audit risk are provided. In the first example, an IT auditor is assessing authorization which belongs to the more basic operations when conducting an IT audit. In this case, the IT auditor is likely to *unintentionally* relate IT risk via quality risk to audit risk; it could very well be that the IT auditor was

[7] It should be noticed that the pharmaceutical organisation itself can be subdivided in different stakeholders with different interest as well. For instance it might be that the control operators have the need to implement CCM functionality but that management does not recognize the relevance of this need. However, for the purpose of discussing quality risk, the pharmaceutical organisation is treated as a single stakeholder.

not aware of the existence of the quality risk that a wrong batch of ingredients is received when auditing the authorisation around an IT application. In the second example, it is likely that the auditor *fails* to make the relation; it is not likely that the IT auditor considers the execution of mathematical formulas within an application to determine the proportion of ingredients relevant in terms of audit risk if the IT auditor is not aware of the quality risk of having an unusable batch of medicines. Especially in the second example where the relation is overlooked, but also in the first example where the relation is made unintentionally it should be clear that the IT auditor should have an understanding of quality risks as well when performing an IT audit in the pharmaceutical industry.

It could be discussed whether this relatively general observation should be a guideline since adopting a broader view on audit risks seems not directly of interest for the IT audit of SAP GRC PC in the pharmaceutical industry. However, because "a broader view" could be made explicit for the pharmaceutical industry (i.e. risk influences audit risk via quality risk) it is decided to contain this observation into a guideline.

A final notion has to be placed at the relations between the different types of risk. According to Kloosterman (2004), different types of risk such as IT risk and quality risk can only be used to provide information to the ARM to determine the audit risk. The ARM cannot be used to describe other types of risk such as IT risk or quality risk. When considering the ARM as a Bayesian model, IT risk and quality risk can be interpreted as Bayesian variants of the ARM (Kloosterman, 2004).

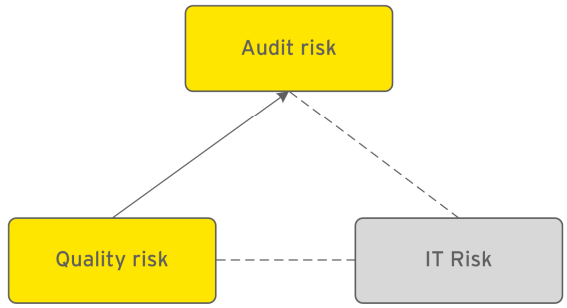
Guideline 6: The implementation of SAP GRC PC might result in additional risks

There is the risk of insufficient knowledge meaning that the organisation does not possess the necessary knowledge to exploit SAP GRC PC to its full potential (Respondent A). The impact of this risk is believed to be limited since the organisations who have the resources to implement SAP GRC PC are likely to have the resources for acquiring the required knowledge as well, and hence the impact of the risk of insufficient knowledge is limited (Respondent A).

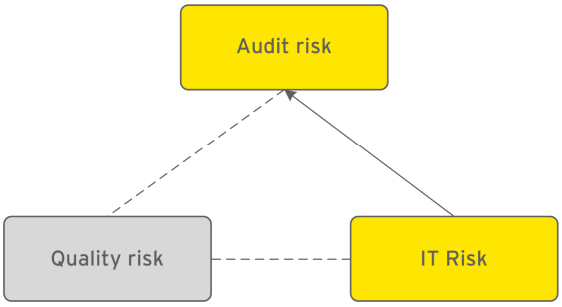
There is the risk of incorrect knowledge meaning that the employees lack the knowledge to properly interpret the results of the monitoring functionality (Respondent E).

Both notions derived from the interviews imply that the implementation of the SAP GRC PC comes with additional risks. As regards to the first notion, it could be that the organisation has never had the necessary knowledge or that the knowledge has disappeared as employees leave the organisation. It could be argued that considering additional risk is of relevance for other audit objects as well and hence should not be made explicit as a special concern for the audit of SAP RC PC. This motivates why some of the respondents did not mention additional risk. On the contrary, two of the respondents did explicitly mention additional risk which evidenced that additional risk is not necessarily taken into account when performing an IT audit. Although the impact of the this risk is believed to be limited, there seems evidence that additional risk is not by definition taken into account if the performance of an IT audit. Therefore, the IT auditor should be made aware of the additional risks when it comes to the IT audit of SAP GRC PC.

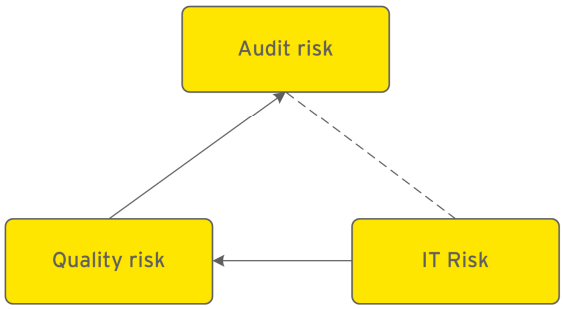
As regards to the second notion it could be that the users of SAP GRC PC blindly trust the output of the monitoring activity and are not sufficiently aware that the output is as good as the logic inside the system, which is developed by humans. This could result in a situation in which the users unjustly conclude that no risks have occurred. Here SAP GRC PC contributes to a false sense of security and hence it is of importance that the IT auditor is aware of the risk of incorrect knowledge. It should be noticed that unlike the risk of insufficient knowledge, the risk of incorrect knowledge is of relevance for a particular range of audit objects, namely CCM systems such as SAP GRC PC. This substantiate why this guideline is relevant to be included with respect to the audit of SAP GRC PC.



Consider for instance the storage or distribution of ingredients for the production of medicines. These might be simple raw materials or complex processed ingredients which are extremely sensitive for humidity or temperature changes. The quality risk that a large proportion of the ingredients becomes useless during storage or distribution might Have a material effect on the financial statements of a pharmaceutical organisation since it might result in significant financial losses and hence affects the audit risk.



Consider for instance a human resource application that is used for documenting personal information of employees not including payroll records. This application will not be of interest to the external IT audit since it will not influence the financial statements directly. However, if the application is also used for keeping track of the timesheets of employees it will become relevant for the financial statement audit; personnel costs might be a material account on the organisation's financial statements. There is the IT risk that the application inaccurately processes the data which affects the audit risk.



Example 1:
Consider the IT risk that unauthorized changes are made to master data such as adjusting the approved vendor list. If this IT risk occurs this might lead to a situation in which a wrong batch of ingredients is received by a pharmaceutical production plant. Receiving a wrong batch of ingredients is considered a quality risk. A wrong batch of ingredients can Have a material effect on the organisation's financial statements and therefore could affect the audit risk.

Example 2:
Consider for instance the IT risk that mathematical formulas used to determine the proportion of ingredients for the production of a medicine are inaccurately executed within an application. On first sight, an IT auditor and financial auditor might conclude that the execution of these formulas is not interesting in terms of the organisation's financial statements. However, producing medicines with wrong proportions of ingredients might result in an unusable batch of medicines which is considered a quality risk. An unusable batch of medicines can Have a material effect on the financial statements since ingredients can be extremely costly in the pharmaceutical industry. In a worst case scenario, the organisation has already launched the product to the market and is required to retrieve the medicine with all its financial consequences (e.g. reputational damage, compensation claims, loss of the batch of medicines). Here the IT risk that an application inaccurately execute mathematical formulas to determine the proportion of ingredients for a medicine affects the quality risk of an unusable batch of medicines which affect the audit risk because losing a batch of medicines can be significant in terms of the organisation's financial statements.

Figure 13 - Risk interrelatedness

Examples are created by the author and verified by an auditor with a RA/RE background. It should be noticed that in the examples it is only stated that the a quality risk or IT risk affects audit risk without making explicit whether the audit risk in increased or decreased. This is done on purpose since quality risk and IT risk directly increase the risk of material misstatements which could be offset by decreasing the detection risk. In other words, the quality risk and IT risk only increases the audit risk provided that the detection risk remains the same and is not decreased by the performance of substantive procedures.

Guideline 7: SAP GRC PC might be used to monitor quality risk

Recently the FDA published a guide on risk-based monitoring in the pharmaceutical industry (FDA, 2013). There are two main drivers which result in the issuing of this guide. The first driver is the increase in the number and complexity of clinical trials during the past two decades. The second driver is the increased usage of automated systems and electronic records by pharmaceutical organisations. Both developments caused the FDA to rethink the traditional monitoring techniques and publish recommendations on alternative monitoring.

Monitoring can be seen as a "quality control tool" which implies that monitoring can be used to control quality risk (FDA, 2013, p. 2). In the pharmaceutical industry, typically the sponsor is responsible for conducing monitoring activities. A sponsor "takes responsibility for and initiates a clinical investigation" and may be "an individual or pharmaceutical company, governmental agency, academic institution, private organization, or other organization" (FDA, 2014). The FDA recommend each sponsors to develop a monitoring plan in order to manage quality risks critical to human safety and clinical trials. Traditionally, sponsors make extensive use of on-site monitoring. On-site monitoring is an in-person evaluation at the site where the clinical trial is being executed. Nowadays, sponsors make increasingly use of centralized monitoring which is a remote evaluation executed at a location different than the site where the clinical trials are taking place. In the guide concerning risk-based monitoring in the pharmaceutical industry, the FDA explicitly state that they encourage "greater use of centralized monitoring practices, where appropriate, than has been the case historically, with correspondingly less emphasis on on-site monitoring" (FDA, 2013, p. 1).

The increased usage of automated systems and electronic records by pharmaceutical organisations together with the encouragement of the FDA to embrace centralised monitoring techniques are two developments which enable the usage of SAP GRC PC for monitoring quality risk. In Textboxes 1 and 2, examples of how CCM could be used for clinical trials are provided.

The work of the IT auditor is currently limited to assessing the internal control structure of an organisation in terms of financial statements. If pharmaceutical organisations indeed start using CCM to monitor quality risks, this will result in the need for assessing the IT system which is used for establishing the CCM functionality. Assessing CCM supporting systems is typically the domain of the IT auditor. There seems evidence that the role of the IT auditor in the pharmaceutical industry might be extended to audit the CCM functionality used for controlling quality risks. As visualised in Figure 13, IT risk might influence audit risk via quality risk. Assessing a CCM system used for controlling quality risk enables IT auditors to improve the assessment of audit risk, under the condition that the IT auditor is able to properly identify the relation of IT risk via quality risk to audit risk. This guideline could be seen as an opportunity to improve the effectiveness and of the external IT audit

One of the monitoring activities of a sponsor is to monitor the study site's processes, procedures and records (FDA, 2013). In an automated environment the clinical procedures are supported by automated systems which could be monitored remotely at a central point in the organisation. A sponsor could check whether a procedure is executed properly or whether there are deviations from the protocol by monitoring the progress in the automated system. However, this could be a time-consuming activity and there remains the risk that errors in the procedures are overlooked. In an automated environment it is also a possibility that a proper execution of the procedures is enforced in the systems by means of automated controls. These automated controls could be monitored with CCM. In this scenario, the sponsor could use monitoring reports generated by the CCM system to monitor the clinical procedure remotely.

Textbox 1 - CCM to monitor pharmaceutical processes, processes and records

Another monitoring activity of the sponsor is the monitoring of the accuracy of the clinical data submitted to the sponsor (FDA, 2013). This is a critical monitoring activity in the pharmaceutical industry because it affects people's health. Therefore the sponsor should ensure the quality of the data which are used to draw conclusions. In an automated environment, the sponsor could perform data reviews remotely and identify missing data and data outliers and define follow-up procedures. However, in an automated environment the accuracy of the data could be ensured by means of automated controls as well. Just like in the example of monitoring a clinical procedure, monitoring reports generated by the CCM system could be used to monitor data inconsistencies.

Textbox 2 – CCM to monitor the accuracy of clinical data

4.3 Control assessment

Guideline 8: It is desirable to remove any redundant controls prior to implementing SAP GRC PC

CCM is established according to the risk and control framework. It was stated that an organisation should first have a proper internal control structure prior to the implementation of SAP GRC PC (Respondents B). Proper in this context means discard any redundant controls. The reason why it is of relevance to remove redundant controls prior to the establishment of the monitoring functionality of SAP GRC PC is that monitoring redundant controls brings along the following disadvantages (Respondent B):

(1) the implementation of redundant controls requires an unnecessary investment,
(2) redundant controls unnecessary overload the system which could negatively affect the performance,
(3) redundant controls blurring the findings provided by adequate controls.

The conclusion that could be drawn with respect to the above notion is clear, the organisation should first update their internal controls structure and remove any redundant controls. Respondent B provided three arguments of which the first one could be questioned because costs seems not to drive pharmaceutical organisations in particular. Obviously, this line of reasoning only holds to a certain extent; pharmaceutical organisations have a cost ceiling as well, although the ceiling might be higher compared to other industries.

Guideline 9: Automated, IT dependent and manual controls could all be targeted by SAP GRC PC

Most IT auditors recognize that SAP GRC PC could be used to monitor automated controls, but are not aware that SAP GRC PC could be used to monitor manual controls and IT-dependent controls as well (Respondents B and C).

SAP GRC PC could be used to monitor automated as well as IT dependent controls however, manual controls could not be monitored by SAP GRC PC (Respondent A).

As regards to manual and IT-dependent controls, SAP GRC PC provide a checklist in which the controls could be checked off manually, and functions basically as a self-assessment tool. By means of CCM, this checklist could be monitored and hence information concerning manual controls and IT-dependent controls could be included in the monitoring reports. As regards to automated controls, business rules could be formulated which directly monitor the automated controls. So all three types of controls seems to be suitable to be targeted by SAP GRC PC. Considering the two notions, it seems that there is disagreement about what type of controls could be monitored. It should be noticed that this disagreement might be the result of the vague boundary between the term "IT dependent" and "manual" after all, it could be argued that an digital checklist makes the control IT dependent. Nevertheless, for the purpose of this research the checklist will be considered manual since it is assumed that the checklist is developed by a human and not generated by an IT system. So, SAP GRC PC could be used to monitor automated, IT dependent, as well as manual controls. However, it should be noticed that monitoring manual controls could never be continuous since manual activities are by definition executed with a predefined frequency.

Guideline 10: Automated controls should be preferred above manual controls

Automated controls are more reliable compared to manual controls provided that the ITGCs are effective (Respondents A, B and D). According to the respondents, humans are more likely to make mistakes while operating a control compared to computers. This claim is substantiated by GTAG (2009, p. 3) which state that "application controls are more reliable than manual controls when evaluating the potential for control errors due to human interventions".

There seems to be a cost dimension to this discussion as well. A first aspect to this discussion seems to be whether to automate manual controls or not. As stated by Respondent D, it is good to have a great amount of automated controls because of their reliability however, it requires a significant investment to automate all of them. Especially for some less frequent controls, it might be more cost-effective not to automate them. But if the hurdle is taken and manual controls are automated to a large extent, Respondent B noted that costs will decrease because less man-hours are required to operate automated controls. Manual controls are by definition tied to a certain frequency (e.g. annual, semi-annual, quarterly, daily), whereas automated controls are operating effective or not provided that the ITGCs are effective (GTAG, 2009). As a result, operating and monitoring manual controls is more time intensive and hence requires a higher financial investment. A second aspect to this discussion comes to light when taking CCM into account. With CCM a large part of the process of operating and monitoring a control will be automated and hence reduces the amount of time needed by humans. According to Nelson and Ambrosini (2007), this will reduce the overall compliance costs as visualised in Figure 14. Although initially the automation of controls requires a certain financial investment, in the long term operating and monitoring automated controls seems to be more cost-effective compared to manual controls.

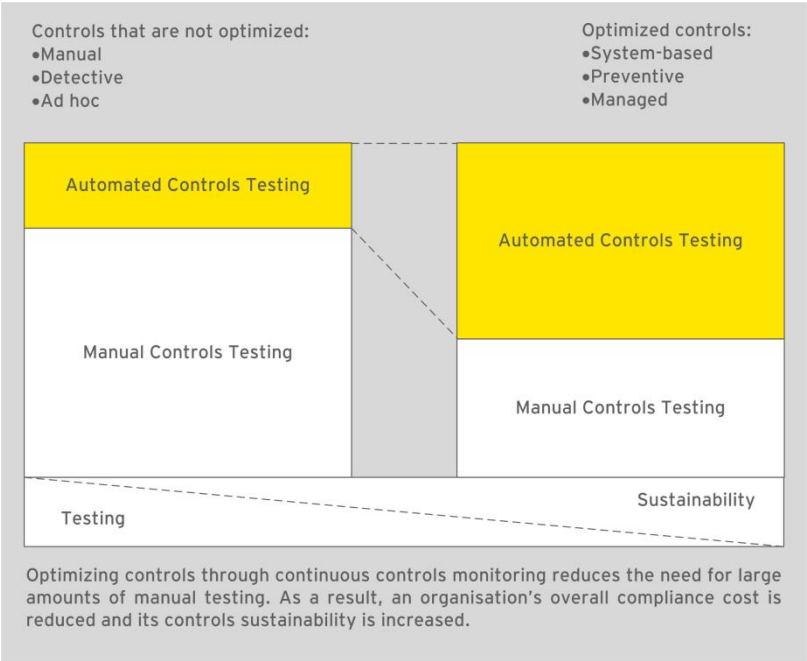


Figure 14 - Rebalancing the automated controls portfolio adapted from Nelson and Ambrosini (2007, p. 30)

Respondent E added some nuances to the claim that automated controls should be preferred above manual controls and argued that a preference for automated or manual controls is dependent on the situation of the client. If the organisation of interest has a high degree of automated processing information, than the IT auditor should not expect more than a few manual controls. A lot of manual controls in a fully automated environment makes the IT auditor suspicious concerning the adequacy of the risk and control framework. Besides the degree of automation, the amount of transactions plays an important role as well. For instance, if an organisation only sends 20 invoices in a year, it might be irrelevant to make use of automated controls. The amount of transactions also depends on the type of process. So the degree of automation, the nature of the process and volume of transactions determine whether or not the IT auditor should expect automated controls or not.

Nowadays a significant amount of business processes is automated. Consequently, organisations have to deal increasingly with computerized data processed by IT systems. These IT systems could be used to establish automated controls. It could be argued that continuously monitoring automated controls is preferred above continuously monitoring manual controls. The main motivation for this assertion is that automated controls seems to be more reliable compared to manual controls. It should be noticed that this argument seems not to apply solely to the audit of SAP GRC PC but that automated controls are preferred in general. The reason this argument is being provided in this research is because updating the internal control framework by reducing the amount of manual controls is a driver for pharmaceutical organisations to implement SAP GRC PC, which was stated in Chapter 3. The increased reliability of automated controls contributes to the improvement of the effectiveness of the control structure and hence is of particular relevance in the audit of SAP GRC PC in the pharmaceutical industry. Another motivation for this claim is that although CCM requires an initial financial investment, in the long-term the overall compliance costs will reduce and hence CCM will be more cost-effective when targeting automated controls instead of manual controls. This argument is less applicable in the pharmaceutical industry where costs are not believed to be a main driver. So, it seems to be that automated controls in general are favoured above manual controls because of their reliability and cost-effectiveness. However, there are some situations in which this claim does not apply and hence the IT auditor should take into account the context of the audit as well. Moreover, it should be noticed that monitoring manual controls could never be continuous since manual activities are by definition executed with a predefined frequency. Consequently, it makes more sense to monitor automated controls by means of SAP GRC PC.

Guideline 11: SAP GRC PC could be used in a detective as well as preventive manner

According to respondent A, SAP GRC PC could have a preventive as well as a detective nature. The detective nature is obvious since monitoring allows directly for detecting deficiencies. The preventive nature arises when process improvements are executed based on the identified deficiencies. Improving processes might prevent deficiencies from happening in the future again.

Besides the value of detecting more deficiencies, there is also the risk of information overload which might mask the causes underlying the deficiencies (Kuhn & Sutton, 2010). Information overload might mask the real cause underlying the deficiencies which might jeopardise the preventive nature of SAP GRC PC as noted by Respondent A.

According to Respondent E, from the perspective of an IT auditor, detective controls are preferred because the IT auditor wants assurance that all misstatements within the organisation's business processes are detected and corrected. From the perspective of the organisation, preventive controls are preferred. After all, the organisation wants to prevent a risk from occurring. To illustrate this point, an example of an online web shop was provided by Respondent E. In a web shop the customer directly interacts with the system of the organisation in a public environment. The web shop owner wants to ensure the correctness of an order and is likely to have preventive controls in place to ensure customers can only place

valid orders. These preventive controls are not relevant for the activities performed by the IT auditors. The IT auditor should be aware of the different perspective on controls between the IT auditor and the organisation.

SAP GRC PC seems to meet the need of IT auditors as well as organisations since it has a detective and a preventive nature. The detective nature is obvious, by monitoring controls continuously, any misstatements are detected and communicated through the organisation. The preventive nature could be explained as follows. As elaborated on in section 1.3, SAP GRC PC could be used to monitor transactions in order to gain insight in the functioning of the internal control structure as a whole. By continuously monitoring these transactions, deficiencies come to light. By analysing these deficiencies, the root cause could be revealed where after the underlying process could be improved. An improved business process prevent future deficiencies from occurring which explains the preventive nature of SAP GRC PC. A notion should be made that an increased amount of deficiencies could also result in information overload which could mask the root cause of the deficiencies.

In a traditional audit, there seems to be friction between IT auditors and organisations. The IT auditors are interested in detecting a misstatement which is best found by data analyses whereas organisations want to be protected against the occurrence of a risk which is best achieved by testing the operating effectiveness and adequacy of the design of the internal control structure. SAP GRC PC seems to address this friction because of its detective as well as preventive nature.

Guideline 12: The frequency of monitoring is dependent on the amount of events associated with the control as well as the significance of the risk mitigated by the control

The frequency of monitoring a control should be determined according to the amount of events that are related to the monitored control as well as the significance of the risk that is mitigated by the monitored control (Respondents A, C and D).

When discussing the frequency, it should be noticed that not the frequency of executing a control is referred to, but it is the frequency of monitoring whether the control functions properly which is of interest when discussing SAP GRC PC. The main question that should be addressed is whether a control should be monitored continuously, or that another frequency is more appropriate.

It turned out that the frequency of monitoring is dependent on the amount of events that are targeted by the control and the significance of the risk that is mitigated by the control. This is visualised in Figure 15. To illustrate this point, consider the example of a two-way-match control which obliged that an invoice is approved by another entity than the entity who approves the order. If an organisation processes a great amount of purchase orders which requires a two-way-match control, and the risk of paying an incorrect or fraudulent invoice is classified as high for that particular organisation, the frequency of monitoring the two-way-match control should be high or even continuous. So the higher the amount of events that are targeted by a control and the more significant the risk that is mitigated by the control, the more relevant it is to monitor the control continuously. It should be noticed that the frequency of monitoring is hard to determine beforehand since the amount of events and significance of a risk are complex to predict and are subjected to change.

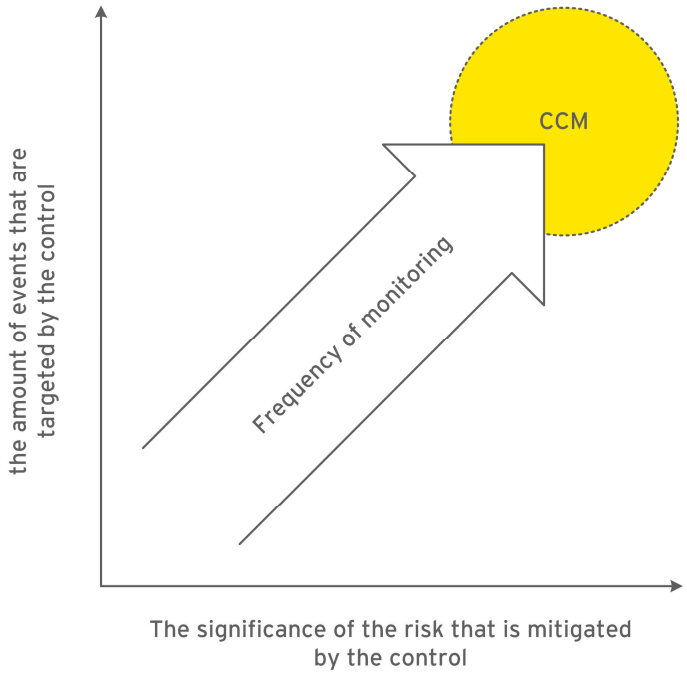


Figure 15 - determining the monitoring frequency

4.4 Conclusion

What are the relevant guidelines regarding process analysis in the IT audit of SAP GRC PC in the pharmaceutical industry?

Conform the expectations, there is a limited amount of differences regarding the analyses of processes. In fact only a single guideline was derived next to the guideline which stresses that there are no relevant differences in the process analyses activity. This guideline state that the IT auditor should gain insight into how the processes are translated to the data structures in the underlying IT environment.

3.2 Are there relevant guidelines regarding risk identification in the IT audit of SAP GRC PC in the pharmaceutical industry?

The identification of risks should be executed regardless of the audit object. Therefore, it was expected that risk identification does not significantly differ in the audit of SAP GRC PC. Nevertheless, three relevant guidelines are made. The first guideline is that IT auditors should adopt a broader perspective on audit risk. Furthermore, the IT auditor should be aware of the fact that implementing SAP GRC PC brings additional risks along. The last guideline is merely an opportunity which stresses that CCM could be used to monitor quality risks in pharmaceutical organisations.

3.3 Are there relevant guidelines regarding control assessment in the IT audit of SAP GRC PC in the pharmaceutical industry?

Beforehand it was expected to derive various guidelines regarding the assessment of the internal control structure with respect to SAP GRC PC. The guideline made include (1) it is desirable to remove redundant controls prior to the implementation of SAP GRC PC, (2) all three types of controls could be targeted with SAP GRC PC, (3) automated controls should be preferred above manual controls, (4) SAP GRC PC could be used in a detective as well as preventive manner, and (5) The frequency of monitoring is dependent on the amount of events associated with the control as well as the significance of the risk mitigated by the control.

5

Technical aspects of SAP GRC PC

In this chapter, the guidelines regarding the technical aspects of SAP GRC PC will be composed. According to the contours of the frame of reference as visualised in Figure 12 in section 2.3, the guidelines should be derived by discussing the technical architecture of SAP GRC PC (5.1) as well as the CCM functionality of SAP GRC PC itself (5.2). The guidelines will be derived according to the sub-questions as presented in Table 10. As regards to the technical architecture three areas will be addresses which are: (1) the source system, (2) the interfaces, and (3) the target system (i.e. SAP GRC PC). As regards to the CCM functionality, three areas will be addressed as well which are (1) data integrity, (2) business rules, and (3) management of SAP GRC PC. For a clarification regarding these aspects, the reader is referred to section 2.2.3. Beforehand it is expected to derive various relevant guidelines since IT auditors are currently unfamiliar with the technical details of SAP GRC PC for the purpose of the external IT audit. The guidelines will be derived according to desk research and interviews with IT auditors. The background of the IT auditors who participated in the interviews is presented in Table 3 in section 1.7. All insights are presented according the structure as elaborated on in section 1.8.

Table 10 - Sub-questions Chapter 5

Section	Sub-question	Output
5.1 The technical architecture of SAP GRC PC	What are the relevant guidelines regarding the technical architecture in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
5.2 The CCM functionality of SAP GRC PC	What are the relevant guidelines regarding the CCM functionality in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines

5.1 The technical architecture of SAP GRC PC

5.1.1 Guidelines regarding the assessment of the source system

Guideline 13: The verification of the existence of a control should be performed manually in the source system

As stressed by two of the respondents, the only way for the IT auditor to ensure that a control actually exists is to manually verify the existence of that control in the source system (Respondents C and D). This is of relevance since SAP GRC PC might suggest that a control is working properly while in reality it is not.

This point could be illustrated by considering an empty deficiency report. An empty deficiency report could either mean that there are no deficiencies or that there is no control implemented in the source system. This raises the question how to ensure that the control which is monitored by SAP GRC PC actually exists in the source system? This might be done by means of the evaluating functionality within SAP GRC PC. However, if the evaluation is performed automatically instead of manually, the question remains whether the outcome of the evaluation activity is reliable. After all, if during the evaluation no deficiencies are detected this could mean that there is no control. So it appears that the verification of the existence of a control in the source system should performed manually, which is also explicitly stated by respondents C and D.

Guideline 14: Assessing logical access controls of the source system for CCM-AC and CCM-MD appears to be a redundant activity

According to respondents C and D, there is no evidence that the IT auditor might skip certain ITGCs regarding the source system.

Respondents A, B, and E, asking themselves whether it is relevant to assess (all) the ITGCs of the source system without providing an unambiguous answer.

As stresses by respondent B, it is the question to what extent the logical access controls should be monitored however, change management controls cannot be ignored since there has to be a process which translates the impact of changes made to the source system in terms of impact on the target system.

Another question that was raised during the interviews was to what extent the IT auditor should assess the ITGCs of a source system, provided that the control exists? The respondents were equivocal regarding this question. The respondents with the least IT audit experience stated that in order to ensure the integrity of the data being monitored, the IT auditor should assess the ITGCs of the source system. On the contrary, the more experienced respondents were more reluctant to state that all the ITGCs of the source system should be assessed, especially in the case of logical access controls. For instance, consider the situation in which CCM-AC is applied and a table with configuration data is being monitored which resides in the source system. In this case, it might be a redundant activity to test logical access controls since any modifications to the configuration settings will be registered and reported by SAP GRC PC, provided that the configuration data has integrity in the first place according to guideline 21. The same holds for applying CCM-MD, provided that the master data is correct in the first place and adequately applied within transactions and thus has integrity according to guideline 21. In these scenarios, the discussion whether to test all ITGCs of the source system in any case seems to get decided in favour of the more experienced IT auditors. However, if CCM-T is applied and a control is monitored based on transactional data, the integrity of this data should be ensured which is done by testing the ITGCs including logical access controls of the source system. So in the situation in which CCM-AC or CCM-MD is applied, the IT auditor might ignore the logical access controls of the source system since they are covered by the monitoring functionality. This claim should be interpreted with care and has to be substantiated with evidence from researches considering real-world cases. Although logical access controls might be ignored in certain situations, other ITGCs such as system development controls and program change management controls cannot be ignored; there has to be a process which translates the impact of changes made to the source system in terms of impact on the target system.

Guideline 15: If changes are made to the source system, special attention should be paid to the impact of these changes on the compatibility with SAP GRC PC and vice versa

According to respondent B, it is of relevance to understand how changes made to the source system affects the compatibility with the target system and vice versa. This is of relevance for the audit of SAP GRC PC because if these changes are not taken into account, the monitoring functionality might fail. Because the changes which affect the compatibility of the source system with the target system is new for IT auditors, this point should get special attention (Respondent B).

Currently, the IT auditor is likely to focus on assessing whether changes made to the source system are tested before they are carried out. However, for the audit of SAP GRC PC, the IT auditor should not only assess whether the changes are properly tested before implementation, it should also be known what the impact is of the proposed changes in terms of the compatibility with SAP GRC PC and vice versa. Consequently, the IT auditor should widen its perspective on change management controls.

5.1.2 Guidelines regarding the assessment of the interfaces

Guideline 16: SAP GRC PC negatively affects the performance of the source system

As argued by Kuhn and Sutton (2010) based on the work of Debreceny et al. (2005), continuously monitoring might significantly impact the performance of the source system. The impact is dependent on the type of interface being used. According to Kuhn and Sutton (2010), especially EAMs but MCLs as well, will negatively impact the performance of the source system. This problem is also recognized by respondent B.

An IT auditor should understand how the implementation affects the performance of the source system and hence the IT audit activities. It should be assessed whether the source system could cope with the monitoring functionality of SAP GRC PC. A solution for this problem offered by SAP is SAP HANA. SAP HANA is a relational database management system to ensure the performance of a system while processing a high amount of data and executing complex business rules simultaneously on the same platform. Especially for CCM-T it is desirable for an organisation to make use of an performance improver such as SAP HANA because the amount of transactions could become significantly high.

Guideline 17: The reliability of the interface should be determined by assessing the correctness, completeness and timeliness of the interface

The respondents stated that an interface should be assessed in terms of correctness, completeness, and timeliness of the data being transferred by the interface (Respondents A – E). According to the respondents this is basic audit methodology.

According to respondent E, it appears that completeness of an interface is more often an issue than the correctness of an interface. Respondent E observed this notion in the performance of various audits in which an interface had to be assessed.

When assessing the interfaces, the respondents stated that they were interested in the correctness, completeness and timeliness of the data transferred by the interface. In general, the correctness of the data is rarely a concern while the completeness of the data is more often an issue. This notion is not specific for the audit of SAP GRC PC and applies to the audit of other interfaces as well. The timeliness of the interface is of particular relevance in the audit of the CCM functionality of SAP GRC PC. After all, a delay in the monitoring activity directly override the advantages of having continuously insight in the functioning of the internal control structure. The interface could be assessed in various ways. For instance, the IT auditor could perform the same query as formulated in SAP GRC PC and execute this query directly on the source system. By comparing the retrieved transactions it could be concluded whether the interface works properly. Another possibility is for the auditor to make use of a hash function. It should be noticed that this guideline applies to interfaces in general. However, because the interface plays an important part in the technical architecture of SAP GRC PC this guideline was made anyway.

Guideline 18: It is of less relevance to assess the technological details regarding standard interfaces

In the assessment of an interface, the IT auditor should not perform intensive audit activities if the interface is provided by a trustworthy vendor (Respondent B and D). The respondents argue that if the interface is provided by a trustworthy vendor, for IT audit purposes this decreases the probability that the interface is erroneous.

Besides the trustworthiness of the vendor, the IT auditor should take into account his own experience with the interface and the extent to which the interface is used by other organisations. If the IT auditor has experience with the interface and the interface is commonly

implemented by other organisations, it is of less relevance to extensively assess the technical details of the IT audit (Respondent D).

An interface is considered standard if (1) it is provided by a trustworthy vendor, (2) the IT auditor is familiar with the interface, and (3) the interface is widely adopted among organisations. An example of a standard interface is a RFC connection. According to the interviews, it seems of less relevance to assess the technical details of a standard interface. Although from an assurance perspective the interface should always be assessed extensively, in reality this might be unfeasible due to financial and time constraints. Moreover, the IT auditor strives for reasonable assurance instead of full assurance in the performance of an IT audit. It becomes another story when the interfaces are custom-made or can be configured according to the preferences of the organisation. In this case, the IT auditor should perform audit procedures to test the interface for completeness, timeliness and correctness. It should be noticed that this guideline applies to interfaces in general but is stated anyway for the same reason as guideline 17. A final notion regarding the line of reasoning of respondents B and D should be made. The respondents argue that an interface is less erroneous if that interface is provided by a trustworthy vendor. This argumentation might be sufficient for IT auditors who provide reasonable assurance whereas in reality also a trustworthy vendor could develop erroneous interfaces.

5.1.3 Guidelines regarding the assessment of the target system

Guideline 19: The extent to which the programmed logic of SAP GRC PC should be tested should be determined according to the professional judgement of the IT auditor

The fact that SAP GRC PC is delivered by a trustworthy vendor such as SAP should provide reasonable assurance that the program logic is designed and programmed well provided that the organisation did not customize SAP GRC PC themselves by adapting ABAP code[8] (Respondent A and D).

If SAP GRC PC is implemented by various organisations and there are no bug reports, this is an indicator for the IT auditor that the application functions as intended (Respondent A and D).

Here the same line of reasoning as is used in guideline 18 applies. If the target system (1) is provided by a trustworthy vendor, (2) the IT auditor is familiar with the system, and (3) the system is widely adopted among organisations the importance to assess the technological details underlying the system are of less relevance although undesirable from an assurance perspective. It should be noticed that if the organisation has customized ABAP code, the IT auditor is required to thoroughly consider test reports and perform code reviews in order to provide assurance, regardless of resource constraints. Because SAP GRC PC is currently in the initial stage of adoption and IT auditors appear to have limited experience using SAP GRC PC for the performance of an IT audit, it is likely that the IT auditor should delve into the technological details. However, SAP GRC PC is provided by a trustworthy vendor. As long as SAP GRC PC is not widely adopted the IT auditor should appeal his professional judgement in determining the intensity of delving into the technological

Guideline 20: A monitoring rationale that states how the organisation intends to use SAP GRC PC could be used to assess whether the technical implementation of SAP GRC PC meets its purpose

A point made by respondent D is that the organisation should have a description of how they intent to use SAP GRC PC within their business. This document could be used to assess whether SAP GRC PC meets its monitoring purpose.

[8] Advanced Business Application Programming (ABAP) code is a high level programming language developed by SAP and is used for building SAP GRC PC.

If the organisation being audited actually has a monitoring rationale in which they have made explicit how they intend to use SAP GRC PC, the IT auditor should assess whether the actual technical implementation of SAP GRC PC corresponds to this rationale. Every deviation from the document could be interpreted as an implementation error. Although it is desirable for an organisation to have a monitoring rationale, it should be noticed that in reality this document might be absent. Moreover this rationale could be used to guide the implementation process as well which is described in guideline 25.

5.2 The CCM functionality of SAP GRC PC

5.2.1 Guidelines regarding data integrity

Guideline 21: The integrity of the data being targeted by the monitoring functionality should be safeguarded

According to respondent E, it is of importance to safeguard the integrity of the data being monitored.

According to the definitions of CDA and CCM, it could be suggested that only CDA encompasses data analysis. However, CCM encompasses data analysis as well since a business rule is executed on data and performs analysis according to user-specified logic. Anyway, even without that discussion, the integrity of the data is of relevance in the audit of SAP GRC PC. Obviously, if the data being monitored has no integrity, the monitoring functionality will provide false monitoring output. Data integrity is especially of relevance for CCM-T since transactional data is often created automatically. On the contrary, configuration settings and master data is often composed carefully and hence data integrity is of less relevance for CCM-AC and CCM-MD, provided that the data was correct in the first place. This notion should be interpreted with care. For instance, if master data has integrity but is inaccurately applied within a business process the integrity might be called into question.

Information integrity is dependent on data integrity. Information integrity is a broader concept than data integrity since “data are considered to be raw material used to create a finished product ready for use, i.e. information” (Flowerday & Von Solms, 2005, p. 606). Information has integrity if, the timeliness, completeness, accuracy, validity and processing method is safeguarded. Consequently, data integrity is ensured if the data is: timely, complete, accurate, valid and properly processed. Moreover, according to Boritz (2004), data integrity means that the data is in an unimpaired or unmarred condition.

Textbox 3 - Data integrity

5.2.2 Guidelines regarding the assessment of the business ruleset

Guideline 22: It should be known whether the business rule is correct

The correctness of a business rule refers to the design of the rule itself. It should be assessed whether the functionality envisioned by the rule designer corresponds to the actual functioning of the rule when applied into practice (Respondent E).

As noted by Debreceny et al. (2005), the external IT auditor should have extensive knowledge of ERP systems when implementing EAMs. This line of reasoning also applies to assessing a business rule. After all, in order to determine whether the rule is applied to the right tables in the source system, the IT auditor should be aware of the data structures target by the monitoring functionality and hence should have knowledge about the source system (respondent B). As stressed by respondent E, beside knowledge regarding the source system, the IT auditor should have extensive knowledge of the target system. Obviously, if the IT auditor lacks the knowledge to understand how a business rule is formulated, it is not possible to properly assess the correctness of the rule. According to respondent E, the complexity of assessing the correctness of the business rule is often underestimated by IT auditors.

As noted by respondent A, the method to assess the correctness of a business rule should be that the IT auditor first forms an expectation of how the rule should look like according to its conceptual description. Subsequently, the IT auditor compares the actual rule with its expectations and considers any deviations in detail.

As regards to the correctness, the IT auditor has to determine whether a business rule performs the analyses it is intended to do. If a business rule is not correct, the output of the monitoring functionality is likely to be incorrect as well, which could result in a false sense of security among the organisation. Therefore, the IT auditor cannot build blindly on the output of the monitoring activity, even if the organisation claims that the CCM functionality is properly implemented. The IT auditor should always delve into the technical specifics of a business rule before relying on the monitoring output. For the assessment of the correctness of a business rule, it should be determined whether the technical specifics are in line with the expectation of the IT auditor. It should be noticed that the IT auditor is required to have thorough knowledge about SAP GRC PC in order to formulate an expectation. Furthermore it should be determined whether the business rule monitors the right control in the right process which includes assessing whether all relevant configuration tables or transactions are taken into account and that data filters are absent. Therefore the IT auditor should have thorough knowledge about the technical details of the source systems. After all, the IT auditor should understand how transactions, master data and configuration tables are managed in the source systems. It should be noticed that assessing the correctness of the business rule is often underestimated and more complex than most IT auditors are aware of. There are various audit techniques (re-performance, inspection, client reviews, and benchmarking) to assess the correctness of a business rule. These techniques will be discussed in more detail in guidelines 26 – 29.

Guideline 23: There should be a business rule management process to ensure the ruleset is adapted according to changes made in the source system

According to the respondents, there has to be a business rule management process in order to ensure the business rules are adapted according to changes made to the source system (Respondent B – E). If the business rules are not adapted according to the changes made to the source system, this might result in an erroneous monitoring functionality which is of relevance for the IT audit of SAP GRC PC.

Besides the correctness of the business rule, four of the respondents explicitly mentioned the importance of a *business rule management process*. Organisations, business processes and source systems change. Consequently, the business rules should be adapted according to the changed environment to ensure the adequacy of the monitoring analyses. A management process should be in place to ensure that the business rules are up to date. To illustrate this guideline, respondent D provided the example in which a source system was updated. After the update, the data structure of the source system was changed and configuration settings were stored in different database tables. Consequently, the business rule monitors a non-existent or unused configuration table. Here the problem of false security becomes visible as well. The IT auditor should determine whether the organisation has a management process in place to translate changes made to a source system to the target system. This process is not the same as testing system development controls and program change management controls of the source system as described by guideline 15 because these ITGCs are predominantly focused on testing the compatibility of the target system and the source system. Here it is argued that a business rule management process should be in place to ensure that a business rule is adapted according to changes made to the source system. In such a process the business rule should be reassessed after changed made to the IT landscape in which the source systems resides.

Guideline 24: An adequate risk and control framework is a prerequisite before designing business rules

It should be a prerequisite that an adequate risk and control framework is in place before an organisation could start with the implementation of SAP GRC PC (Respondent B). Changing the control framework after the implementation of SAP GRC PC will most likely cause the need for updating the business ruleset which could be a time-consuming, costly, and complex activity.

It seems to be more cost-effective for an organisation to first update their risk and control framework before implementing SAP GRC PC. According to guidelines 8 and 10, the risk and control framework should be free from redundant controls and encompass merely automated controls. Updating the risk and control structure is likely to result in changes made to the source systems. Consequently, the business rules should be adapted accordingly as stressed in guideline 23. Adapting business rules is a complex and timely activity which decreases the cost-effectiveness of the implementation of SAP GRC PC. Therefore having an adequate risk and control framework which is free from redundant controls and includes as many as possible automated controls is a prerequisite for designing the business ruleset.

Guideline 25: For the assessment of the iterative process of implementing a business ruleset the organisation's monitoring rationale should be used

Respondent E stated that designing business rules is an iterative process. After the design on paper is implemented, the organisation is not finished as opposed to what numerous IT auditors and organisations think. By implementing SAP GRC PC, controls are monitored more frequent compared to traditional audit procedures in which the operating effectiveness of a control is largely estimated. Consequently, more exceptions will be detected in the case where controls are monitored continuously. By analysing these exceptions the underlying causes of the deficiencies might be revealed which will enable the organisation to improve their business processes. After process improvement it is likely that the business ruleset should be updated which might result in new exceptions and hence in the need for new process improvements. It is believed that an organisations should go through various rounds of updating the business ruleset and business process improvement until no new exceptions come to light. To guide this design and implementation process, it is of importance for the organisation to explicitly state the purpose of using SAP GRC PC in a monitoring rationale. This document could then be used as guidance in the implementation process of SAP GRC PC. An IT auditor should be aware of the hurdles which has to be taken in the process of implementing the business ruleset.

During the establishment regarding the assessment of a business rule, up until now it was assumed that SAP GRC PC was already implemented. However, at this moment, there is only a limited amount of organisations who have actually implemented SAP GRC PC in a mature way. Therefore, IT auditors should form an opinion of the implementation process as well. Organisations should have a monitoring rationale to guide the iterative process of designing and implementing a business rule. The IT auditor might use this rationale to form his opinion on the implementation process by determining whether the monitoring in practice corresponds to the monitoring rationale. It should be noticed that in the dirty reality such a monitoring rationale might be absent. This could be an indicator for the IT auditor to assess the implementation process with care.

Guideline 26: Assessing a business rule by means of re-performance is believed to be relatively reliable but time consuming which might negatively affect the cost-effectiveness of an audit

An audit technique commonly used by IT auditors to test a control is re-performance. According to GTAG (2009) re-performance could either mean re-performing the control activity using system data or re-performing the control activity in a test environment with robust testing scripts.

Re-performance is an audit technique that could be applied to assess the correctness of a business rule. Re-performance of a business rule includes replicating the monitoring functionality in a different environment and verifies whether the business rule functions as intended. In order to do so, the same input will be provided to the actual target system and to the re-performed monitoring functionality where after the results are compared. If the results are equal it could be concluded that the business rule is correct while any deviations should be scrutinized. It is believed that re-performance provides a relatively high amount of assurance compared to other audit techniques. A disadvantage of re-performance is that it might be a time consuming activity to rebuilt the monitoring functionality in an external IT environment. Moreover, re-performance only provides results concerning a relatively small part of the IT audit. Therefore, the IT auditor should consider whether re-performance is the most cost-effective technique in a certain situation.

Guideline 27: In order to assess a business rule by means of inspection, the IT auditor should have extensive knowledge regarding the technology of SAP GRC PC as well as the source systems and the code should be constructed in a review friendly manner

Inspection is an audit technique commonly used by IT auditors to assess a control. According to GTAG (2009), inspection could apply either to the inspection of (1) system configurations, (2) user acceptance testing, (3) reconciliations with supporting details, or user access listening. As explicitly stated by respondent B, inspection could be used for assessing a business rule as well.

A requirement for inspection of a business rule is that the IT auditor has extensive knowledge with respect to SAP GRC PC itself as well as the source system (respondent B and C).

According to respondent C, in order for the IT auditor to perform inspection, a prerequisite is that the code is constructed in a review friendly manner.

Inspection is an audit technique that could be applied to assess the correctness of a business rule. Inspection is concerned with interpreting the business rule by reviewing the code. This could include the code of the business rule itself in which the logic of the rule is established as well as the ABAP code which is constructed by SAP itself in order to execute the business rule. As already argued for in guideline 19, it is not likely that the ABAP code itself contains any errors. And if there is evidence that the ABAP code contains any errors it is more likely that the IT auditor will make use of re-performance since ABAP code could be very lengthy and extremely complex. A requirement for inspection of the logic of a business rule is that the IT auditor should have specific knowledge of SAP GRC PC as well as IT environment and source systems of the organisation. Furthermore, the code should be composed in a review friendly manner which is in practice often not the case.

Guideline 28: Assessing a business rule by means of client review is less reliable than other audit techniques however, it might offer a solution when the IT auditor lacks extensive knowledge regarding SAP GRC PC

According to respondent E, client review is an audit technique that could be used to assess a business rule which is especially applicable if the IT auditor lacks extensive knowledge regarding the technology of SAP GRC PC.

Client review is an audit technique that could be applied to assess the correctness of a business rule. Client review seems to be an audit technique that could be applied when the IT auditor has decided to inspect the logic of a business rule but only has limited knowledge of SAP GRC PC. In the case, the IT auditor would inspect the business ruleset together with the rule designers of the organisation. The rule designer will explain step by step to the IT auditor how the business rules are established. This will allow the external auditor to assess the business rule with only limited knowledge of the target system. Obviously, because of the limited knowledge of the IT auditor, it could be that errors are overlooked and hence a false conclusion is provided by the IT auditor. Moreover, in the dirty reality, it could be that there is not a single rule designer and that numerous people have contributed

to the construction of the business ruleset from different point of views. In this scenario, performing a client review seems an impossible task.

Guideline 29: Benchmarking is a reliable audit technique for assessing a business rule provided that a proper best practice set is available

Respondent A, who has audited the AC component of SAP GRC, stated that they compared the ruleset of the client with a best practice set which was established in a cooperation of the Big4 audit firms. After the comparison, the deviations from the best practice ruleset were discussed with the client where after it was decided whether or not to use the AC component for the external audit. According to the knowledge of the author, there is not such a benchmark rule set available for the PC component.

Benchmarking is an audit technique that could be applied to assess the correctness of a business rule. Because the benchmarking technique was used in the past for the audit of SAP GRC AC by external IT auditor it is believed that this is a reliable audit technique for assessing the correctness of a business rule. However, at the moment benchmarking seems not usable for SAP GRC PC because a best practice ruleset is lacking. There are some standard rulesets available provided by SAP but these are not assessed by IT auditors and hence could not be used of the shelf as a best practice ruleset.

5.2.3 Guidelines regarding the management of SAP GRC PC

Guideline 30: It is of relevance to consider logical access controls as well as change management controls with respect to SAP GRC PC

The respondents noticed the importance of logical access controls of SAP GRC PC (Respondent A – E). It should be known which persons in the organisation have access to SAP GRC PC and could make adjustments to the monitoring functionality such as modifying business rules or changing the monitoring frequency

In general, it could be claimed that if the amount of people with access to the target system increases the reliability of the target system decreases which negatively influence the usefulness of SAP GRC PC for the external IT audit (Respondent E).

The respondents noticed the importance of the change management controls of SAP GRC PC (Respondent A – E). In the decision whether or not to rely on SAP GRC PC for the external audit, it is of importance that the target system is up to date. If SAP GRC PC is not up to date, the organisation should have a sound motivation based on the release notes for not updating the target system. Moreover, the IT auditor should know whether the update was properly tested before it was implemented.

Although assessing the logical access controls of the source systems might be redundant in certain situations with respect to guideline 14, the logical access controls of the target system cannot be ignored. The IT auditor should expect only a limited amount of people who can make adjustments to SAP GRC PC. Moreover, the change management controls regarding SAP GRC PC appears to be of relevance as well; the IT auditor should know whether SAP GRC PC was updated. It should be noticed that these change management controls are not the same as referred to in guideline 15. Guideline 15 relates to the change management controls of the source systems. Iit turned out that the ITGCs of the target system are of relevance as well. This is an important notion since in a traditional audit a target system was absent and hence testing ITGCs with respect to a target system was not part of the IT audit practices.

Guideline 31: It should be known how downtime of SAP GRC PC influences the monitoring functionality

Respondent C noticed that the IT auditor should understand what happens during downtime of the target system. The IT auditor should know whether the monitoring functionality was inactive in order to determine whether or not to use SAP GRC PC for the purpose of the IT audit.

It appears to be of relevance to understand how any downtime of SAP GRC PC influences the monitoring functionality. If the IT auditor wants to rely on SAP GRC PC to assess the operating effectiveness of the monitoring functionality it should be understand how downtime of SAP GRC PC influences the monitoring functionality. Currently the influence of downtime seems to be unknown. Moreover, the IT auditor should know whether SAP GRC PC was down during the time period of interest. This touches the importance of having a trustworthy logging functionality which will be elaborated on in guideline 32

Guideline 32: Downtime and changes made in SAP GRC PC should be properly logged

Respondent A and C explicitly noticed that all the changes made to business ruleset as well as any downtime of the target system should be properly logged in a log file. Such a log file can be used by the IT auditor to determine whether the monitoring functionality was enabled during the time period of interest. The IT auditor should ensure that the log file has integrity and therefore assess whether the log file can be manipulated or changed. For instance it could be possible to turn off logging. Ideally the log file would log whenever the logging functionality is disabled. Furthermore, the IT auditor should ensure that the log file is constructed properly by the target system.

The IT auditor should have access to the log file in which changes made to the CCM functionality of SAP GRC PC as well as any downtime are logged. In the decision whether or not to use SAP GRC PC for determining the operating effectiveness of a control it is of relevance that any downtime is properly logged. After all, if the system is down, the monitoring functionality is down as well which directly influence the operating effectiveness of the control and hence the IT audit. For the purpose of the IT audit of SAP GRC PC the integrity of the log file should be safeguarded. Furthermore, IT auditors should be aware of the possibility to turn off logging when auditing SAP GRC PC.

5.3 Conclusion

What are the relevant guidelines regarding the technical architecture in the IT audit of SAP GRC PC in the pharmaceutical industry?

The IT auditor should assess three aspects regarding the technical architecture in the audit of SAP GRC PC which are: (1) the source system, (2) the interfaces, and (3) the target system. The guidelines that turned out to be of relevance for the assessment of the source systems are: (1) that the existence of a control should be verified manually in the source system itself, (2) the logical access controls regarding the source system in the case of CCM-AC or CCM-MD might be ignored, (3) changes made to the source system might affect the compatibility with SAP GRC PC and vice versa, and (4) SAP GRC PC negatively affects the performance of the source system. Two guidelines were made with respect to the interfaces: (1) the interface should be assessed in terms of correctness, completeness and timeliness, and (2) it is of less relevance to assess the technological details of standard interfaces. Considering the target system two guidelines were found of relevance which are: (1) the extent to which the programmed logic of SAP GRC PC should be assessed depends on the professional judgment of the IT auditor, and (2) a monitoring rationale could be used to assess whether the target system meets its purpose.

What are the relevant guidelines regarding the CCM functionality in the IT audit of SAP GRC PC in the pharmaceutical industry?

The aspects that are of relevance in the assessment of the CCM functionality of SAP GRC PC are (1) data integrity, (2) business rules, and (3) the management of SAP GRC PC. With respect to the data integrity a single guidelines appears to be of relevance which is that the integrity of the data being targeted by the monitoring functionality has to be safeguarded. Considering the business rules, eight guidelines were found to be of importance of which four were related to the audit technique of assessing a business rule. The four guidelines regarding the business rules are (1) it should be known whether the business rule is correct, (2) a business rule management processes is required to translate changes to the source system in terms of the business ruleset, (3) an adequate risk and control framework is a prerequisite before designing business rules, and (4) for the assessment of the iterative process of implementing a business ruleset the organisation's monitoring rationale should be used. The four guidelines related to the audit technique for assessing a business rule are (1) re-performing a business rule is reliable but time consuming and cost-ineffective, (2) inspection requires the IT auditor to have the extensive knowledge of SAP GRC PC and requires that the business rules are formulated in a review friendly manner, (3) client review might be less reliable compared to other audit techniques but could be applied whenever the IT auditor lacks extensive knowledge regarding SAP GRC PC, and (4) benchmarking is a reliable audit technique for assessing a business rule provided that a proper best practice set is available. As regards to the management of SAP GRC PC, three guidelines were made (1) it is of relevance to consider logical access controls as well as change management controls with respect to SAP GRC PC, (2) it should be known how downtime of SAP GRC PC influences the monitoring functionality, and (3) downtime and changes made in SAP GRC PC should be properly logged.

6

Communication

After the IT auditor has assessed the technological aspects of SAP GRC PC, the next phase is to assess the communication which includes the organisational embedding (6.1) and external reporting (6.2) as elaborated on in section 2.2.4. In this chapter, guidelines with respect to the communication will be derived according to the sub-questions as presented in Table 11. Because the organisational embedding is new in the audit of SAP GRC PC compared to other audit objects, it is believed to derive various relevant guidelines in this area. The guidelines will be derived according to desk research and interviews with IT auditors. The background of the IT auditors who participated in the interviews is presented in Table 3 in section 1.7. All insights are presented according the structure as elaborated on in section 1.8.

Table 11 - Sub-questions Chapter 6

Section	Sub-question	Output
6.1 Organisational embedding	What are the relevant guidelines regarding the organisational embedding in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines
6.2 External communication	What are the relevant guidelines regarding external reporting in the IT audit of SAP GRC PC in the pharmaceutical industry?	Guidelines

6.1 Organisational embedding

Guideline 33: To rely on the monitoring results regarding the operating effectiveness of a control the communication between operational management and internal auditors, together with the communication between the internal auditors and external auditors should be assessed

In the thesis of van Niekerk (2013), various information flows within the Three Lines of Defense model are revealed. Based on these information flows, different reporting and change cycles are composed which are classified as "production loops". One of the production loops is formulated as follows: "a big loop (yearly) that audits the design, implementation and operating effectiveness of the entire framework. This is done by the third line, based on reliance on the file prepared by the first line" (van Niekerk, 2013, p. 27).

The loop as described by van Niekerk (2013) is taken as a starting point to establish the operating effectiveness loop as visualised in Figure 16. The operating effectiveness loop is about sharing the information resulting from the monitoring activity in order to increase the assurance that risks are properly mitigated by the internal control structure of the organisation. Internally, assessing whether the organisation mitigates risks properly is the responsibility of the third line. So the first line, which is responsible for operating the CCM functionality, should provide the results obtained from the monitoring activity to the third line. Moreover, the third line should discuss the results with external auditors. In order to rely on the insights concerning the operating effectiveness of a control as provided by SAP GRC PC, the IT auditor should assess the communication between the first line and third line, as well as the communication between the third line and the external auditor himself. If the communication is not proceeding well, for instance when certain deficiencies are not reported,

this nullifies the envisioned advantages of having SAP GRC PC. It should be noticed that the communication between the external auditors is of special relevance for the purpose of this research and is absent in the reporting loop of van Niekerk (2013). This is due the different perspectives of both researches; where the work of van Niekerk (2013) takes the perspective of the organisation as a starting point, this research reasons from the perspective of the external IT auditor.

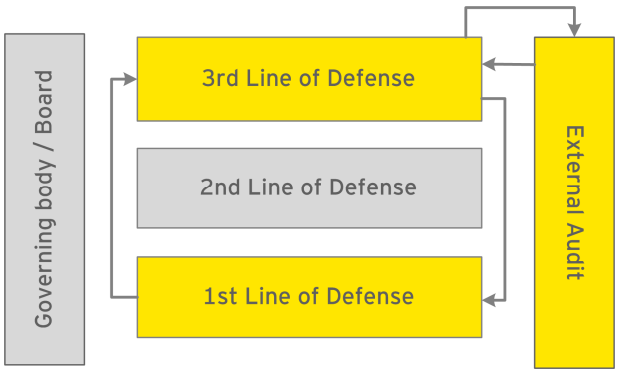


Figure 16 - Operating effectiveness loop

Guideline 34: The process improvement loop might provide relevant information regarding the IT audit of SAP GRC PC

Another loop identified by van Niekerk (2013, p. 27) is formulated as follows: "There is a change loop as a result of internal influences, like change and implementation of business processes"

The loop as identified by van Niekerk (2013) is taken as a starting point to establish the process improvement loop as visualised in Figure 17. It should be noticed that this loop describes the preventive nature of CCM as described in guideline 11. By continuously monitoring the operating effectiveness of the control, more accurate information regarding the functioning of the control will be available. This information might be used to reveal and address the root cause of the dis-functioning of the control in the underlying process which might create the opportunity for process improvements. Process improvements are typically initiated and carried out by the first and second lines. A discussion between both lines should result in improvements which (1) are feasible from an operational perspective, (2) are in accordance with regulation from a compliance perspective, and (3) are mitigating risks more adequately from a risk mitigation perspective. Although process improvement is mainly the area of the first and second lines, the improvements should be communicated to the governing body of the organisation which might intervene in the improvement activity. Furthermore, the internal audit as well as the external audit should be notified of the changes made to the processes. Because of the independent nature of the audit instances, they are not allowed to provide feedback on the proposed process improvements.

Insight in process improvement might result in early detection for process changes which might affect the external audit activities with respect to guideline 2. Therefore the IT auditor should consider process improvements for the purpose of the audit of SAP GRC PC. Moreover, the insight used for process improvement might be valuable input for the external IT audit as well.

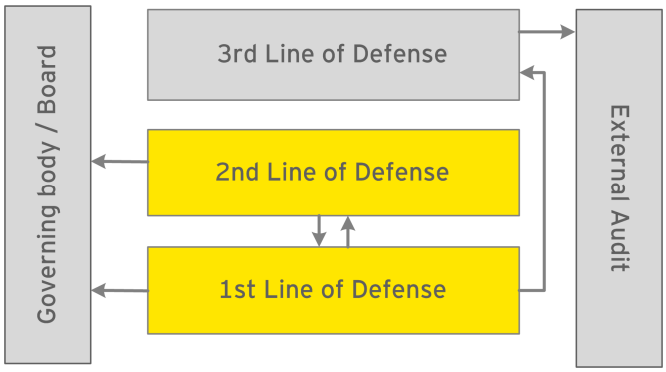


Figure 17 - Process improvement loop

Guideline 35: The system improvement loop might provide relevant information regarding the IT audit of SAP GRC PC

Although not directly identified by van Niekerk (2013), just like improving business processes, the underlying IT system could be improved as well. van Niekerk (2013, p. 27) identifies a learning cycle "based on incidents and finding" to improve the risk and control framework. Likewise, a learning cycle can be used to for system improvement.

The learning cycle as identified by van Niekerk (2013) is taken as a starting point to establish the system improvement loop as visualised in Figure 18. It could be that process improvements are insufficient to properly address the root cause of the deficiencies. Consequently it might be needed to improve the system underlying the business process. This is a more rigorous improvement compared to the improvement of a business process because it will have a significant impact on the IT environment across the organisation as a whole. Furthermore, other processes which are supported by the same system should be adapted accordingly. Just like process improvements, system improvements are typically initiated by the first and second lines. The main difference is that system improvements have a higher impact across the organisation and might require significant (financial) investments. As a result, the governing body of the organisation is actively involved in the improvement process. Moreover, more control owners are involved when an entire system will be improved which increases the pressure on the operational management. The audit instances still have to be independent, but their opinion might be asked since they have to rely on the output of the system.

Insight in the system improvement loop is of relevance for the external IT audit of SAP GRC PC because changes made to IT systems directly affect the monitoring functionality as established in SAP GRC PC with respect to guideline 23. Besides affecting the business rule, the compatibility of the source system with the target system might be influenced as well with respect to guideline 15. To ensure the monitoring activity and system compatibility, the IT auditor should assess the system improvement process.

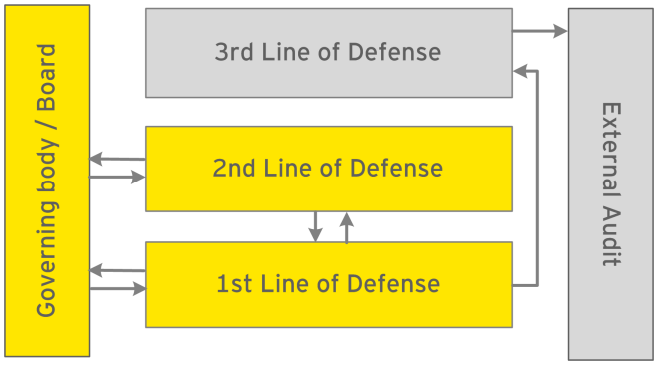


Figure 18 - System improvement loop

Guideline 36: It is of importance that the people who have to work with SAP GRC PC recognize its added value

According to respondent D, there is always a part of the audit that cannot be covered by technology. Consequently the IT auditor should gain insight in the people who interact with SAP GRC PC and who uses the CCM functionality.

As stressed by respondent B, the people who have to work with SAP GRC PC should acknowledge its added value. The attitude of those people is critical for a successful implementation of the monitoring functionality.

There is always a part of the audit that cannot be covered by technology such as the interpretation of the deficiencies and how these deficiencies might affect the business continuity. As a result, there will always be people involved in establishing and operating the monitoring functionality of SAP GRC PC. It is of importance that these people recognize the added value of the monitoring functionality for their daily activities. If the people within the organisation start working around SAP GRC PC, the monitoring functionality will not bring the added value promised to the business and becomes a redundant investment. The people who have to establish and operate the monitoring functionality are the first and second line. According to misperception 1 as discussed in Chapter 3, it is likely that the operating and compliance teams are willing to use SAP GRC PC to improve their way of working.

Guideline 37: There should be clear follow-up procedures defined within the organisation to properly deal with deficiencies

Running a business rule is not the end of the monitoring activity (Respondent E). For instance, a rule might notice whether a configuration setting is changed, than there has to be a process which describes how this notification should be dealt with. For example, consider an organisation which monitors whether a person has approved his own order. If such an event has occurred and is identified by SAP GRC PC, than somebody should react to this event and take the necessary measures to prevent a risk from occurring. After all, if nobody deals with the exceptions, there is no control at all. The IT auditor should perform an assessment how exceptions are followed-up.

According to respondent B, the IT auditor should check whether the people who have to deal with the output of SAP GRC PC, actually know what to do by assessing the organisation's follow-up procedures.

The output of SAP GRC PC is not the end of the monitoring activity. It should be made explicit who should receive the monitoring output and how the output should be followed-up in a proper manner. This should be made explicit within the organisation by defining follow-up procedures. Having a proper follow-up procedure is of critical importance; if there is no follow-up on the identified deficiencies, the monitoring functionality as a whole fails. Consequently, the IT auditor should assess these procedures for the purpose of the IT audit of SAP GRC PC.

Guideline 38: The right people within the organisations should be trained to work with the follow-up procedures to adequately deal with the deficiencies

According to respondent B, besides that there has to be a follow-up procedure made explicit by the organisation, the people who have to work with this procedure should be trained accordingly.

The IT auditor should not only check whether exceptions have been followed up, it should also be assessed whether they are followed up in a proper manner (respondent E). The monitoring data should be correctly interpreted by the right entity. The IT auditor should question and discuss how the results are interpreted and dealt with by the people within the organisation.

Besides that there has to be follow-up procedures, the people who are expected to use these procedures should be trained accordingly. After all, if the people within the organisation, don't know how to work with these procedures, the monitoring as a whole is likely to fail because the deficiencies are not followed up in a proper manner. In the assessment of the organisational embedding of SAP GRC PC, the IT auditor should assess whether the right people within the organisation are trained well to work with the procedures.

Guideline 39: The execution of the follow-up procedures should be documented

Besides that there should be proper follow-up procedures to deal with exceptions, these procedures should be documented in a way the IT auditor could understand what happens when an exception occurs. A proper and clear follow up documentation is key for the IT auditor whether or not to rely on the CCM functionality of SAP GRC PC (Respondent E).

According to respondent E, The IT auditor wants assurance that the follow up procedures worked properly. Therefore, the findings of the follow-up procedure should be documented as well. From the perspective of the IT auditor the documentation should include (1) what the exceptions are and (2) how the exceptions are dealt with.

After the result of the follow-up procedures are documented, the IT auditor should ensure himself that the monitoring reports are complete (Respondent B). The question is how does the IT auditor know that the reports and warnings from SAP GRC PC are reliable? The IT auditor should ensure himself that all issues that should be reported, are actually reported.

Besides that the organisations should have formulated proper follow-up procedures and have trained the right people to work with these procedures, the execution of the procedures should be documented. There seems to be two main reasons for documentation. First, as elaborated on in guideline 34 and 35, the deficiencies could be used for process and even system improvements. In order to make these improvements, the deficiencies should be documented in a way that they can be analysed to reveal the root cause of the deficiencies and hence contribute to process or system improvement. Second, for the IT auditor to rely on the monitoring results of SAP GRC PC regarding the operating effectiveness of a control, the IT auditor should have insight in the deficiencies and how these deficiencies are followed-up. So for the purpose of the external IT audit, it is of relevance that the deficiencies are properly documented. Moreover, the integrity of this documentation should be ensured. It should be noticed that the integrity of the documentation regarding the follow-up procedures differs from the integrity of the data being monitored with respect to guideline 21, and the integrity of the monitoring results provided by SAP GRC PC as safeguarded collectively with the guidelines from Chapter 5.

6.2 External reporting

Guideline 40: The reporting of the findings of the IT audit of SAP GRC PC does not differ compared to the IT audit of other audit objects

According to respondent A, C and D, the reporting of the findings of the audit of SAP GRC PC will not significantly differ from the reporting of the findings in a traditional audit. The IT auditor should include in the conclusion that the organisation has implemented SAP GRC PC. Furthermore, the IT auditor should endorse why it is of importance to have a CCM functionality. In general, having a CCM functionality is for the IT auditor a sign that the organisation is matured in addressing and managing risk and controls. For the organisation, the opinion of the external auditor is of importance since the have invested a lot of money in the implementation of SAP GRC PC. As a result, the IT auditor should report on the results of the audit of SAP GRC PC.

According to the interviews with IT auditors, it could be concluded that there are no significant differences in the audit of SAP GRC PC when it comes to reporting the findings of the audit. Although, the IT auditor might consider to include a motivation why it is good/bad that the organisation makes use of the monitoring functionality of SAP GRC PC.

Guideline 41: Evidence regarding the assessment of SAP GRC PC will be different compared to evidence regarding the assessment of controls in a source system

According to respondent E, besides the evidence with respect to the ITGCs, the evidence of auditing SAP GRC PC will be different from the evidence of a traditional audit. Consider for instance the situation in which the IT auditor is assessing a procurement process. Then the IT auditor is likely to consider how segregation of duties is established by means of controls. In the traditional audit, the IT auditor gathers evidence regarding the controls in the source system themselves while in the audit of SAP GRC PC the IT auditor gathers evidence regarding the analyses over the controls as formulated in the target system (Respondent E and A). Although it is hard to say how this evidence should look like, it will be definitely different. After all, IT auditors are going to rely on the work of others instead of relying on their own audit activities. The audit objective is not a control as is the case in a traditional audit, but it is a business rule which is used to monitor the control. It is the question if the reliance on a business rule is the same as testing a control. That is a theoretical discussion. The IT auditor does not assess the control itself but assesses whether there are exceptions to the desire that people cannot approve their own orders. If there are any exceptions, the control works by definition not properly. In this scenario, the auditor is required to ignore the controls and make use of substantive procedures in order to provide assurance.

Although currently it might be unsure how specific evidence for the IT audit of SAP GRC PC should look like, the IT auditor should be aware that the evidence will be different. The different nature of evidence rises due the fact that the IT auditor is not required to gather evidence regarding the controls themselves in the source system but to gather evidence regarding the analysis defined in the target system to monitor the controls in the source system. In guideline 42, it will be explored what evidence might be relevant to derive for the purpose of the IT audit of SAP GRC PC.

Guideline 42: Evidence regarding the IT audit of SAP GRC PC might include but is not limited to the business rules, follow-up documentation, ITGCs of SAP GRC PC, control existence in the source system, and the log file of SAP GRC PC

The IT auditor should gather evidence concerning the following things (Respondent B):

- *The application controls which are the business rules*
- *IT-dependent controls which are used to follow up on exceptions*
- *ITGCs.*
- *The authorization within SAP GRC PC*

According to respondent E, first of all, the IT auditor should gather evidence regarding the follow up on exceptions. This includes the documentation of the procedures as well as a reliable report in which it is stated how the procedures are executed for each exception. Furthermore, the IT auditor should gather evidence regarding the existence of business rules. This could be screenshots or other copies of the rule logic. Moreover, the IT auditor should gather evidence regarding the management of SAP GRC which corresponds to evidence regarding the ITGCs of SAP GRC PC.

According to respondent A, the IT auditor is likely to make screenshots of the configuration tables as well as the business rules which could be used as evidence in the audit documentation. Moreover, the IT auditor should gather evidence that the monitoring functionality was enabled during a specified period of time. Here the log file of SAP GRC PC could be used as evidence.

Whereas in guideline 41 it was stated that evidence for the audit of SAP GRC PC will look different, this guideline provides insight into the kind of evidence that might be suitable in the audit of SAP GRC PC. First of all, it should be noticed that the respondents did not came up with a complete and univocal list of aspects that should be included as evidence for the IT audit of SAP GRC PC. Consequently, the aspects provided by the respondents should not be interpreted as an exhaustive list but merely as a starting point. According to the respondents, evidence should encompass but is not limited to the business rules, follow-up documentation, ITGCs of SAP GRC PC, control existence in the source system, and the log file of SAP GRC PC. The way the IT auditor should document this evidence (e.g. screenshots or client documentation) is dependent on the context of the audit and should be determined by the IT auditor using his professional judgement.

6.3 Conclusion

What are the relevant guidelines regarding the organisational embedding in the IT audit of SAP GRC PC in the pharmaceutical industry?

Beforehand, it was unknown what guidelines could be expected because SAP GRC PC itself is currently not used for external IT audit purposes and hence the organisational embedding is a relatively unexplored area for IT auditors. It turned out that seven guidelines are of relevance for the IT audit of SAP GRC PC which are (1) to rely on the monitoring results regarding the operating effectiveness of a control the communication between operational management and internal auditors, together with the communication between the internal auditors and external auditors should be assessed, (2) the process improvement process might provide relevant information regarding the IT audit of SAP GRC PC, (3) the system improvement process might provide relevant information regarding the IT audit of SAP GRC PC, (4) it is of importance that the people who have to work with SAP GRC PC recognize its added value, (5) there should be clear follow-up procedures defined within the organisation to properly deal with deficiencies, (6) The right people within the organisations should be trained to work with the follow-up procedures to adequately deal with the deficiencies and, (7) the execution of the follow-up procedures should be documented.

What are the relevant guidelines regarding external reporting in the IT audit of SAP GRC PC in the pharmaceutical industry?

Beforehand, it was expected that the although the evidence might have another feeling, the reporting itself will not be different. Indeed it was observed that the reporting of the findings of the IT audit of SAP GRC PC does not differ compared to the IT audit of other audit objects. However regarding the evidence gathered by the IT auditor two guidelines were made: (1) the evidence regarding the assessment of SAP GRC PC will be different compared to evidence regarding the assessment of controls in a source system, and (2) evidence regarding the IT audit of SAP GRC PC might include but is not limited to the business rules, follow-up documentation, ITGCs of SAP GRC PC, control existence in the source system, and the log file of SAP GRC PC.

7

A set of guidelines

In this chapter, the components of the final artifact as discussed in Chapters 2 – 6 will be laid down into a comprehensive artifact (7.1). The outline of the artifact corresponds to the contours of the frame of reference as discussed in Chapter 2, whereas the guidelines placed within the frame of reference correspond to the guidelines as proposed in Chapters 3 – 6. Furthermore, an effort is made to classify the guidelines in terms of context, adequacy of the design, and operating effectiveness which reveals how an answer to the main research question is embedded in the artifact (7.2). Finally, the main findings will be exposed and discussed in more detail (7.3).

7.1 Artifact design

As stated in section 1.5, the design objective was to create a set of guidelines, that function as a frame of reference for assessing the adequacy of the design and operating effectiveness of SAP GRC PC in the pharmaceutical industry. This resulted in the artifact as presented in Figure 19 in which an answer to the main research question is embedded. The artifact is constructed by merging the components as discussed in Chapters 2 – 6. The actual design of the artifact is straightforward since its structure, and the guidelines themselves are already extensively discussed in previous chapters. Now, first an effort will be made to clarify how an answer to the main research question is embedded in the artifact. Furthermore, the most relevant findings, which are marked in the artifact, will be elaborated on in more detail.

7.2 An answer to the main research question

The main research question was formulated as: "*How should the adequacy of the design and operating effectiveness of a continuous controls monitoring system in the pharmaceutical industry be assessed from the perspective of the external IT auditor?*". Although the introduction and main research question imply that the adequacy of the design and operating effectiveness are two separated aspects, in fact they are intertwined and dependent on each other. Despite their interrelatedness, an effort is made to classify guidelines which is presented in Table 12. It should be noticed that this classification should be interpreted with care for two reasons.

First of all, the monitoring functionality of SAP GRC PC could not be operating effective if the adequacy of the design is lacking. Typically, by testing the adequacy of the design the IT auditor assesses whether the monitoring functionality is established properly at a specific period in time. In fact, a snapshot of the design is made. On the other hand, the operating effectiveness is tested in order to assess whether the design has not changed during a period of time. Typically, the operating effectiveness of an audit object is tested by assessing ITGCs. Obviously, if the adequacy of the design is not ensured, it makes no sense to assess the operating effectiveness since the auditor will not rely on the monitoring results provided by SAP GRC PC.

Moreover, the design adequacy and operating effectiveness of SAP GRC PC are dependent on the environment in which SAP GRC PC resides. Consider for instance the risk that that mathematical formulas used to determine the proportion of ingredients for the production of a medicine are inaccurately executed within an application. This is a specific risk within the pharmaceutical industry and hence requires specific controls to be properly mitigated. Consequently, such specific controls should be targeted by means of SAP GRC PC in a particular way which is of influence on how an IT auditor should assess the operating effectiveness and adequacy of the design of SAP GRC PC. Both remarks should be carefully considered while interpreting the classification as presented in Table 12.

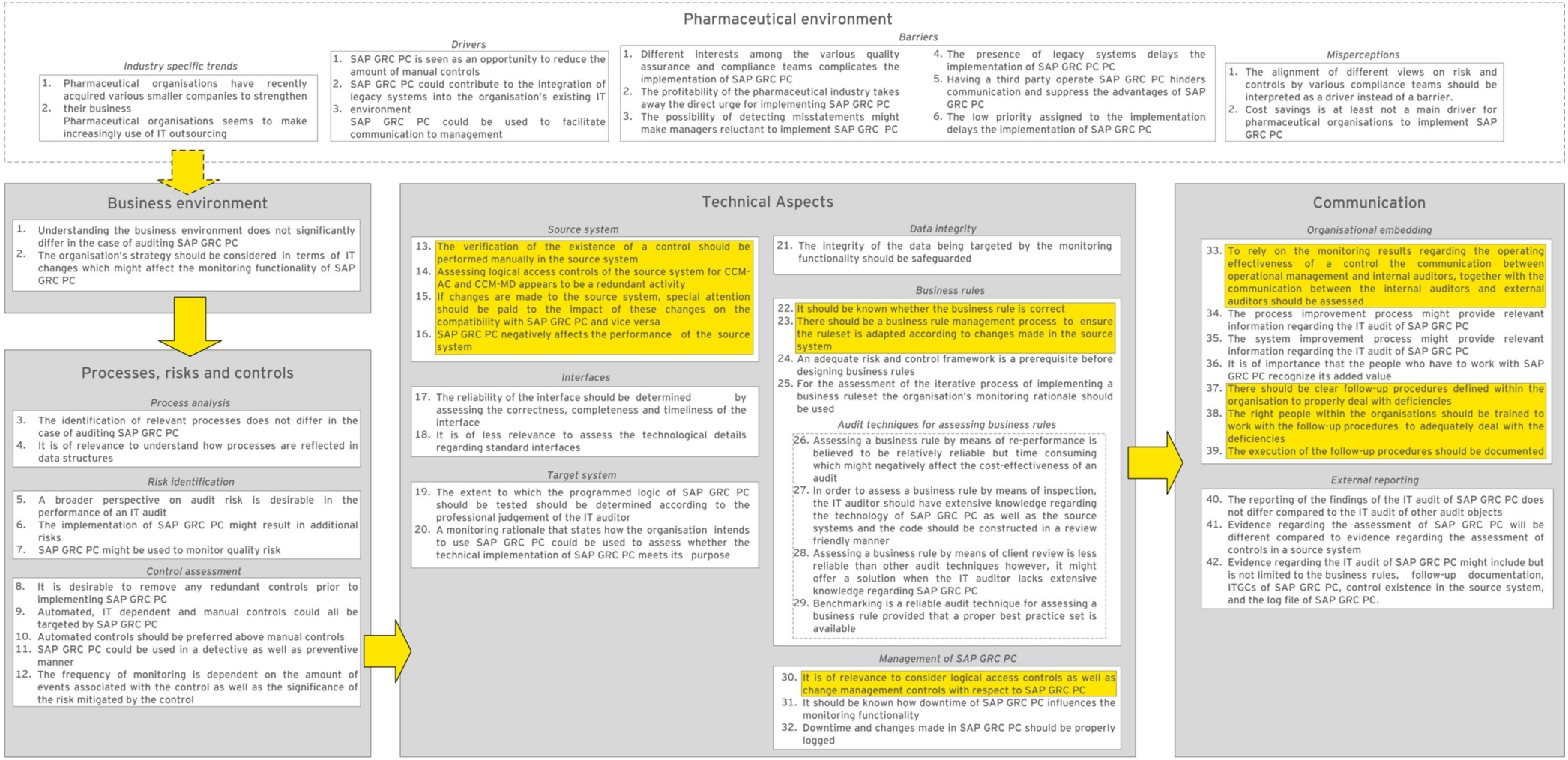


Figure 19 – a set of guidelines

Table 12 - Guideline classification

Area of the artifact	Contextual guidelines	Guidelines regarding the assessment of the design adequacy of SAP GRC PC	Guidelines regarding the operating effectiveness of SAP GRC PC
Business environment	1, 2		
Processes, risks, and controls	3, 5, 6, 7	4	
Technical aspects regarding the architecture	16	13, 17, 18, 19, 20	14, 15
Technical aspects regarding the monitoring functionality	24	22, 23, 25, 26, 27, 28, 29	21, 30, 21, 32
Communication	33, 34, 35, 36, 38, 40, 41, 42		37, 39

7.3 Main findings

In this section, the main findings will be discussed. The guidelines that encompasses concepts that are either new or should be approached in another manner, are of special interest for the IT auditors. Within the artifact the guidelines that met both criteria and that had led to discussions during the interviews are classified as main findings and are marked in the artifact. The majority of these findings are derived according to the interviews instead of desk research. This makes sense because the most interesting results are new and hence not yet discussed in audit literature. However, that does not imply that these findings come out of thin air. On the contrary, the IT auditors pointed out these findings with fundamental audit principles in mind. To illustrate this, the main findings are related to the underlying, well-established audit principles which are presented in Table 13. Now the seven most interesting findings will be discussed in more detail.

Control existence

In a traditional audit, the IT auditor is required to test each individual control in the source system. The introduction of SAP GRC PC raises the question whether the IT auditor could rely on the target system to assure the existence of a control, or that the IT auditor should always go back to the source system to verify the existence of a control in every situation. This is considered a main finding since this question was not of relevance in a traditional audit. To illustrate this point, consider an empty deficiency report provided by the target system. An empty deficiency report could either mean that the control is operating effective or that the control does not exist or function as intended. After all, if the control does not exist or does not function properly, no deficiencies will be reported. It turned out that under no conditions the IT auditor could blindly rely on the monitoring results provided by the target system, which is embedded in guideline 13. The existence of the control should always be assured in the source system at least once. If the existence of the control is assured a single time, a scenario might be considered in which the existence of the control does not have to be assured every time in the future provided that certain preconditions are met. However, identifying these preconditions was not discussed in the interviews and hence no hard claims regarding these preconditions could be made.

ITGCs of the source system

In a traditional audit, ITGCs are tested to provide reasonable assurance regarding the operating effectiveness of a control provided that the adequacy of the design is already established. By means of CCM, continuous insight in the operating effectiveness of a control is provided which give rise to the question whether it is still of relevance to assess the ITGCs of the source system. The respondents who participated in the interviews were equivocal regarding this question, especially when considering logical access controls. Because this question is not of relevance in a traditional audit and there was discussion among the respondents, this is considered a main finding. Taking into account the arguments of the respondents, it is concluded that testing logical access controls in the case configuration data is being target to monitor the operating effectiveness of a control is a redundant activity, which is reflected in guideline 14. In the case transactional data is being targeted the logical access controls are a prerequisite to rely on the insights regarding the operating effectiveness of a control. The difference between targeting configuration data and transactional

data is that although beforehand it is known what data irregularities look like, in the case of targeting transactional data, it is beforehand unknown what the targeted data itself will look like in contrast to configuration data. Consequently the integrity of the data being targeted should be ensured which is done by testing ITGCs, including logical access controls. This line of reasoning will now be illustrated by means of two examples.

Consider the scenario in which a configuration database table is monitored that represents an automated control in an ERP system. This control is monitored by comparing the data in the database table which resides in the source system to the data in a benchmark table which resides in the target system. If the values significantly differ from each other, SAP GRC PC will report the deficiency to an appointed entity who will interpret the deficiency and take action if needed. In this case, it might be a redundant activity to test logical access controls. Logical access controls should ensure that no unauthorized individuals could modify the values in the database table by limiting access to the source system only to authorized individuals. These logical access controls are considered redundant if any modifications to the database table are continuously monitored, provided that deficiencies are properly followed up. It should be noticed that the CCM system itself might follow up the deficiency as well by restoring the modified values according to the benchmark values directly after an unauthorized individual has changed the control settings.

On the contrary, if an automated control is monitored by targeting transactional data, logical access controls are a prerequisite for ensuring the integrity of that data. Consider for instance a control which enforces that each invoice which exceeds a predetermined amount of money should be initiated and approved by two different individuals. Such a control is based on what is referred to by IT auditors as the four eyes principle. Continuously targeting the transactional data and compare the User-IDs of the individuals who initiated and approved the invoice to each other and to a list of User-IDs of individuals who may not approve an invoice, provides insight into the operating effectiveness of the control. It should be noticed that if irregular transactions (i.e. an invoice has been initiated and approved by the same individual) are identified, this indicates that a control is not operating effective. However, if no transactional irregularities are discovered this does not imply that the control is operating effectiveness since it might be luck that no irregular transactions have been taken place[9]. With that notion in mind, the operating effectiveness of the control could only be assured provided that the adequacy of the design is already established and the integrity of the data being monitored is ensured. The integrity of the data being monitored is (at least partly) safeguarded by logical access controls which ensure that no unauthorized individuals could alter the transactional data (e.g. modify the User-IDs) being targeted to monitor the control. Obviously if the integrity of the data being targeted (i.e. User-IDs) is incorrect, this will result in false insight into the operating effectiveness of the control. So it is argued that logical access controls are not redundant in the case transactional data is being targeted.

Besides that assessing logical access controls might be a redundant activity, if controls are monitored by targeting configuration data, no evidence was found that indicates that assessing other ITGCs such as system development controls, program change management controls, security controls or system backup and recovery controls is a redundant activity as well. For instance, as regards to system change management controls, if changes are made to the source system the impact of these changes should be assessed in terms of compatibility with the target system, which is reflected in guideline 15.

ITGCs of the target system

With the introduction of SAP GRC PC as a top layer over automated controls, it was questioned whether it is of relevance to consider ITGCs regarding the target system. This is currently unknown since in traditional audits only ITGCs of the source system are considered; a target system was absent in the old situation. Consequently, considering ITGCs of the target system is considered a main finding. It turned out that it is of relevance to consider ITGCs of the target system, which is reflected in guideline 30. This could be illustrated by considering, once again, the example in which a

[9] This line of reasoning is elaborated on in more detail in section 1.1.5, in which the relevance of the concepts of CDA and CCM in relation to continuous assurance are discussed based on the work of Vasarhelyi (2011).

database table is monitored that represents an automated control in an ERP system. This control is monitored by comparing the data in the database table which resides in the source system to the data in a benchmark table which resides in the target system. If the integrity of the benchmark data is lacking, it could not be assured that the configuration data that represents a control deviates from what it should be, and hence no assurance regarding the operating effectiveness of a control could be provided. Because the benchmark data resides in the target system, the integrity of the benchmark data should be assured by assessing ITGCs of the target system. Moreover, the monitoring logic used to compare the database table in the source system with the benchmark table in the target system resides in the target system as well. Consequently, assessing the ITGCs of the target system also ensures the integrity of the monitoring logic which is of particular relevance to ensure the operating effectiveness of a control.

Assessing business rules

In traditional audits, the operating effectiveness of a control is not continuously monitored by means of a CCM system. In order to assure the reliability of the monitoring results regarding the operating effectiveness of a controls, the IT auditor should assess the monitoring logic underling the monitoring functionality used to establish the monitoring results. In SAP GRC PC, this monitoring logic is captured within business rules. So in order to rely on the monitoring results, the IT auditor should assess the correctness of a business rule which is reflected in guideline 22. Assessing a business rule is considered a main finding since this activity is new in the audit of SAP GRC PC. According to the interviews and desk research, four audit techniques that might be used for the assessment of a business rule are identified (guidelines 26 – 29). It should be noticed that the identification of these techniques does not rule out the possibility that there are other relevant techniques as well.

Business rule management process

As already argued for it is of relevance to assess the ITGCs of the target system. These ITGCs include system change management controls. System change management controls should ensure the source system is still compatible with the target system after changes are made to the source system, and vice versa. However, the system change management controls do not take into account the changes in terms of the business rule. Therefore it is argued that a business rule change management process should be in place, which is reflected in guideline 23. To illustrate this point, consider once again the example in which a database table is monitored that represents an automated control in an ERP system. This control is monitored by comparing the data in the database table which resides in the source system to the data in a benchmark table which resides in the target system. The actual comparison is made according to the monitoring logic that is captured in the business rule which resides in the target system. It should be noticed that if the structure of the database table in the source system is altered, the business rule should be altered accordingly, and vice versa. This should be ensured by the business rule management process. So in the traditional audit situation, only changes made to the source system in relation to the target system are of relevance. These changes are taken into account by testing ITGCs. In the situation in which SAP GRC PC is implemented, changes made to the source system should be considered in terms of the business rules as well which should be assessed by reviewing the business rule management process. Because considering changes in terms of business rules is new, this is considered a main finding. It could be argued that considering changes in terms of business rules might be classified as testing ITGCs of the source system. In this research, it is chosen to make the business rule management process a separate main finding to stress its importance in the audit of SAP GRC PC.

System performance

The target system is coupled to the source system in order to monitor the controls. It turned out that coupling the target system to the source system might negatively influence the performance of the source system, which is reflected by guideline 16. The decrease in system performance is the result of the business rules that target data which resides in the source system. On first sight, a decreasing system performance might not be a relevant observation regarding the assessment of an organisation's financial statements. However, if the system performance decreases, the organisation

is likely to compensate for this by decreasing the monitoring frequency. After all, if the business rule is executed less frequent, this will limit the impact of the monitoring functionality on the performance of the source system. Obviously, a decreasing monitoring frequency results in less insights regarding the operating effectiveness of a control which is of relevance in the assessment of an organisation's financial statements. Because the IT auditor should consider system performance in a wider context compared to a traditional audit, system performance is considered a main finding.

Organisational embedding

It is of relevance to consider what course of action the IT auditor should take if the monitoring results contain deficiencies. This is a new situation for IT auditors and hence classified as a main finding, since in a traditional audit the IT auditor is not relying on the monitoring results provided by SAP GRC PC. In order to determine whether the monitoring results regarding the operating effectiveness are still of relevance for the external IT audit if deficiencies are reported, it should be assessed whether the deficiencies are properly followed up within the organisation. This is where the organisational embedding of SAP GRC PC comes into play. The organisational embedding refers to the use of SAP GRC PC inside an organisation. It turned out that if deficiencies are reported, the IT auditor might determine whether or not to rely on the monitoring results by considering whether the deficiencies are reported and communicated to the right individuals (guideline 33), whether there are clear follow up procedures to deal with the deficiencies (guideline 37), whether the individuals are properly trained to execute the follow up procedures (guideline 38) and whether the follow-up procedures are properly documented after execution (guideline 39).

Table 13 - Theoretical foundation of the main findings

Main finding	Theoretical foundation
Control existence	According to Blokdijk (2004, p. 185), the IT auditor should assess control risk which encompasses three aspects: "*the design, the existence, and the actual operation of the controls*".
ITGCs of the source system	According to Van Praat and Suerink (2013), the work of Clark and Wilson (1987) provides a solid theoretical foundation for assessing ITGCs. The Clark/Wilson-model defines conditions to ensure information integrity. In the audit methodology these conditions are taking as a starting point to ensure the integrity of data that represents controls. For instance, Clark and Wilson (1987) state that a system should be surrounded by clear identification and authentication mechanisms which correspond to logical access controls that are part of the ITGCs.
ITGCs of the target system	
Assessing business rules	Here the underlying theoretical foundation is that the IT auditor should ensure the reliability of audit evidence which is stated in ISA 500 (IFAC, 2009c). If the IT auditor uses the monitoring results as audit evidence to ensure the operating effectiveness of controls, the reliability of the monitoring report should be ensured. Since the monitoring results are automatically generated by executing business rules, the IT auditor should assess the correctness of business rules.
Business rule management process	Here the same underlying theoretical foundation applies as for testing ITGCs, since a change management process regarding business rules might be classified as part of the ITGCs as well. To illustrate this, consider the Clark/Wilson-model again. Clark and Wilson (1987) state that information in a system might only be changed according to strict rules and by fixed procedures which is considered the theoretical foundation underlying the business rule management process.
System performance	The IT auditor forms an opinion of an audit object by taking into account four quality aspects: efficiency, effectiveness, reliability and continuity (Van Praat & Suerink, 2013). System performance relates to the continuity since a decreasing system performance might hamper the continuity of the source system. The theoretical foundation underlying the system performance guideline is that the IT auditor should take into account the continuity processing information in the performance of an IT audit.
Organisational embedding	The underlying theoretical foundation is that audit evidence should be "appropriate" (IFAC, 2009c). If the IT auditor uses the monitoring results as audit evidence to ensure the operating effectiveness of controls, the appropriateness of the monitoring report should be ensured. In the case the monitoring report contains deficiencies, it should be assessed whether these deficiencies are followed-up in a proper manner. This is accomplished by assessing the organisational embedding of SAP GRC PC. According to Van Praat and Suerink (2013), organisational and procedural descriptions could be used as audit evidence as well. Adding the evidence regarding the follow-up procedures might compensate for the deficiencies and classify the monitoring results as appropriate evidence regardless of the deficiencies.

EVALUATION

8

Evaluation

Verschuren and Hartog (2005, p. 738) define evaluation as: "to compare separate parts of a designing process with selected touchstones or criteria (in the broadest sense of the word), and to draw a conclusion in the sense of satisfactory or unsatisfactory". The evaluation methodology is often divided into (1) a plan evaluation which "implies an assessment of the quality of the design on paper", (2) a process evaluation which is aimed at evaluating the design process, and (3) a product evaluation which involves evaluating the value of the design results together with the short and long terms effects of the designed artifact (Verschuren & Hartog, 2005, p. 739). In this chapter, a plan evaluation (8.1) as well as a process evaluation (8.2) will be performed. A product evaluation is not feasible since no pharmaceutical organisations were found to have SAP GRC PC fully implemented. Consequently, the designed artifact could not be applied in a real world situation to evaluate its value for the performance of an IT audit in the context of assuring the reliability of an organisation's financial statements. Nor was it possible to evaluate the short and long term effects of the guidelines on the audit IT audit profession.

8.1 Plan evaluation

As already stated, a plan evaluation entails an assessment of the design on paper. According to Verschuren and Hartog (2005) a plan evaluation should evaluate whether the design goal is met with respect to the design requirements, assumptions and structural specifications. The design goal, requirements, assumptions, and specifications should be evaluated individually and in relation to each other. However, in this research these factors are not made explicit in the way as assumed by Verschuren and Hartog (2005). Instead the research framework of Hevner et al. (2004) is applied. By relating the research framework of Hevner et al. (2004) with respect to the work of Verschuren and Hartog (2005) it could be argued that the design goal corresponds to the business need and that the requirements, assumptions, and specifications are implicitly included in the research relevance. After all, relevance is defined as the extent to which the business need is addressed. A similar line of reasoning is applied by Peffers et al. (2007) who argue that the objectives of a solution are implicitly included in the relevance as defined in the research framework proposed by Hevner et al. (2004).

So a plan evaluation could be performed by evaluating the individual parts of the artifact and evaluating the artifact with respect to its relevance. In order to do so, the IT auditors that have participated in the interviews were asked to fill in an evaluation form in which they were asked for their opinions regarding (1) the structure of the frame of reference, (2) the guidelines, and (3) the relevance of the artifact. The pharmaceutical environment was not included as part of the evaluation form since IT auditors are believed to have limited expertise regarding the industry context. The review form can be found in appendix 5. Here (1) and (2) are used to evaluate the design of the individual parts of the artifact on paper whereas (3) evaluates the relevance of the artifact. It should be noticed that asking the respondents for their opinions regarding the artifact is not a product evaluation since the artifact is not tested in a real-world situation.

The artifact is a set of guidelines that function as a frame of reference for the construction of an audit plan that could be used for the performance of an IT audit regarding SAP GRC PC. To evaluate the artifact, first the structure of the frame of reference will be evaluated where after the guidelines itself will be evaluated. A full discussion of the evaluation results is presented in Appendix 6. The evaluation criteria that will be used for the performance of the plan evaluation are: *clearness*,

acceptance, *interrelatedness, and consistency with the GAM.* The evaluation criteria are elaborated on in Table 14. The criteria are established according to a framework for assurance engagements as proposed by the Dutch association of IT auditors NOREA. According to this framework, norms should have the following five characteristics: relevance, completeness, reliability, neutrality, and intelligibility (NOREA, 2013). Because in this research guidelines are designed instead of norms, the characteristics are tailored to be applicable for the purpose of this research. In Table 14, the relation between the evaluation criteria used in this research and the characteristics proposed by NOREA (2013) are elaborated on. It should be noticed that reliability and neutrality are not included in the evaluation criteria. The reliability of the guidelines refers to whether the guidelines are applicable in various situations which currently cannot be evaluated since the artifact is not yet applied within different real-world situations. Neutrality is of less relevance for guidelines since, in contrast to norms, guideline are not hard measurements to which an audit object is tested.

Table 14 - Evaluation criteria

Evaluation criteria	Description	Relation to NOREA (2013)
Clearness	Clearness refers to whether aspects being evaluated are clear on first sight for the users of the artifact (i.e. external IT auditors). The clearness is derived according to the comments of the IT auditors.	The clearness corresponds to the intelligibility characteristic as identified by NOREA (2013). A clear guideline is unambiguous which is in line with the definition of intelligibility, but also encompasses that the guideline is clear on plain sight. This is of special importance since intensive discussions are captured into single guidelines.
Acceptance	The acceptance of aspects being evaluated refers to whether IT auditors accept the aspect as part of the artifact. The acceptance is derived according to the ratings provided by the IT auditors.	The acceptance corresponds to the relevance characteristic as identified by NOREA (2013). Some guidelines could be of relevance in an IT audit but could not be accepted as part of the artifact. Because the evaluation is aimed at the artifact it is decided to make use of acceptance.
Interrelatedness	The interrelatedness reveals whether the individual aspects of the artifact are dependent on each other or contradictory. The interrelatedness is derived according to the comments of the IT auditors.	Revealing contradictories should ensure the unambiguity of the guidelines which correspond to the intelligibility characteristic, whereas revealing dependencies should ensure the completeness characteristic as identified by NOREA (2013)
Consistency with the GAM	The consistency with the GAM refers to the relation of the artifact with respect to the GAM. The consistency with the GAM is derived according to the comments of the IT auditors. It should be noticed that this evaluation criteria will only be used for evaluating the structure of the frame of reference.	N.A.

8.1.1 Evaluating the frame of reference

An extensive discussion of the evaluation results is provided in Appendix 6. An overview of the evaluation findings regarding the evaluation of the contours of the frame of reference is provided in Table 15. In this section, only the global opinion of the IT auditors will be elaborated on.

Clearness

The clearness of the aspects was not called into question by the IT auditors. This is not surprising since the aspects were identified according to the GAM and IT audit literature (Gantz, 2013; Lindgreen et al., 2005; Van Praat & Suerink, 2013) of which it was expected that the concepts were known among IT auditors.

Acceptance

As visualised in Figure 12 in section 2.3, the areas that are considered either new or should be approached in an alternative way are the control assessment, technical aspects (i.e. technical architecture and CCM functionality of SAP GRC PC), and organisational embedding. As can be

derived from Table 15, the IT auditors accept unanimously the structure of the frame of reference except for respondent B who questioned whether the organisational embedding as part of the communication is relevant in the context of assuring the reliability of financial statements. If the IT auditor wants to rely on the monitoring results provided by SAP GRC PC, these results have to be communicated via internal stakeholders of the organisation since they are responsible for operating SAP GRC PC. Consequently, it was decided to accept this area as part of the frame of reference.

Interrelatedness

The aspects of the frame of reference are related to each other as indicated by the arrows between the different aspects. The respondents did not call the interrelatedness of the aspects into question. It is believed that the IT auditors did not argue with the sequence since it is in line with activities within the GAM.

Consistency with the GAM

As noted by respondent B, the areas of the frame of reference correspond to aspects within the GAM but were formulated in a different way. The different names were the result of the nature of the research in which various sources not related to the GAM were consulted as well. Since this research was conducted in cooperation with a Big4 audit firm, and to increase the applicability of the artefact into practice, it is decided to include references to the GAM. However, it should be noticed that not every aspect (e.g. organisational embedding) fit within the GAM in its current form.

Table 15 - Evaluation results regarding the frame of reference

Aspect	Resp. A	Resp. B	Resp. C	Resp. D	Resp. E
Business environment	+	+	+	+	+
Processes, risks and controls	+	+	+	+	+
Technical aspects	+	+	+	+	+
Technical architecture	+	+	+	+	+
CCM functionality of SAP GRC PC	+	+	+	+	+
Communication	+	–	+	+	+

* "+" indicates that the respondent accept the aspect as part of the artifact

** "–" indicates that the respondent deny the aspect as part of the artifact

*** A marked row indicates that there is a respondent who denies the aspect

8.1.2 Evaluating the guidelines

An extensive discussion of the evaluation results is provided in Appendix 6. An overview of the evaluation findings regarding the guidelines is provided in Table 16. In this section, only the global opinion of the IT auditors will be elaborated on.

Clearness

As regards to the clearness of the guidelines, it turned out that various concepts such as a monitoring rationale, quality risk, process improvement loop, and system improvement loop where not clear on first sight. Moreover, respondent E explicitly noted that certain guidelines needs more explanation to be applicable into practice. The reason for the unclearness is either that the concept is specific for the pharmaceutical industry, is derived from literature, or is created by the author. To increase the applicability of the artifact into practice it is decided to clarify these concepts within the artifact. Moreover, the individual guidelines are formulated in a different manner. It turned out that the different formulation troubled the clearness of the guidelines. Consequently, it is decided to reformulate the guidelines in the same way. Because the artifact is mainly designed for IT auditors, the guidelines will be reformulated with the focus on the IT auditor.

Table 16 - Evaluation results regarding the normative guideline

Aspect	Guideline	Resp. A	Resp. B	Resp. C	Resp. D	Resp. E
Business environment	1	+	0	+	+	+
	2	+	+	0	+	+
Process analysis	3	+	+	+	+	+
	4	+	+	0	+	+
Risk identification	5	+	?	0	+	?
	6	+	–	–	+	+
	7	+/–	?	+	+	?
Control assessment	8	+	+	0	–	–
	9	+	+	0	+	–
	10	+	+	0	+	0
	11	+	+	+	+	+
	12	+	–	+	0	+
Source system	13	+	–	+	+	0
	14	No resp.	–	0	–	–
	15	+	+	+	+	+
Interfaces	16	–	+	0	0	0
	17	+	+	+	+	+
	18	+	+	0	0	0
Target system	19	+	+	+	+	–
	20	+	?	0	?	–
Data integrity	21	+	+	+	+	+
Business rules	22	+	+	+	+	+
	23	+	+	0	+	+
	24	+	–	+	+	0
	25	+	?	+	?	?
	26	+	–	–	–	+
	27	+	+	+	+	–
	28	–	+	–	–	0
	29	+	+	0	+	+
Management of SAP GRC PC	30	+	+	+	+	+
	31	+	+	0	+	+
	32	+	+	0	+	0
Organisational embedding	33	–	–	+	+	–
	34	+	+	?	+	?
	35	+	+	?	+	?
	36	+	+	+	+	+
	37	+	+	+	+	+
	38	+	+	+	+	+
	39	+	+	+	+	+
External reporting	40	+	+	0	+	+
	41	+	+	+	+	+
	42	+	+	–	+	0

* “+” indicates that the respondent accept the aspect as part of the artifact
** “0“ indicates that the respondent is neutral regarding the aspect as part of the artifact
*** “–” indicates that the respondent deny the aspect as part of the artifact
**** “?” indicates that aspect is not clear to the respondent
***** A marked row indicates that there is a respondent who denies the aspect

Acceptance

As regards to the acceptance of the guidelines, it turned out that there is a lot of discussion among the IT auditors themselves. The respondents appear to be equivocal regarding the guidelines and often their opinions were contradictory. It is believed that this is partly the result of the artifact being in its initial stage of design. This highlights the importance of the performance of a product evaluation in which the artifact is tested into practice. However, in order to execute a product evaluation, there should be pharmaceutical organisations that have fully implemented SAP GRC PC which is currently not the case.

Furthermore, it is believed that the guidelines were formulated in too detailed manner which is concluded by interpreting the comments of the IT auditors which were often only related to a specific part of the guideline. Formulating guidelines in a too strict manner jeopardise their applicability in to practice since there is little room for professional judgement which plays an important role in the IT audit profession. On the other hand, formulating the guidelines in a too flexible manner might result in hollow guidelines meaning that the guidelines do not provide sufficient guidance to be applicable into practice. Taking into account both notions it is believed that the guidelines should be formulated in a more narrow way to increase its acceptance among IT audit practitioners.

Besides that that the guidelines should be formulated in a more flexible way the decision to make use of guidelines, with respect to the discussion in section 1.5, seems the be legitimate. The novelty and complexity of the topic resulting in the discussion among IT auditors evidenced that the guidelines should not impose any strict obligations to IT auditors and that there should be room for flexibility. Because of the contradictions among IT auditors regarding the guidelines it is concluded that future research is needed to improve the artifact before the guidelines could become widely adopted within the IT audit community.

Interrelatedness

Although not specifically asked for in the evaluation form, the IT auditors included numerous comments in which they state the interdependencies of the guidelines. This indicates the importance of making the interrelatedness of the guidelines explicit within the artifact. Especially guidelines that were considered preconditions to rely on other guidelines are of relevance for the IT auditors to be aware of when using the artifact into practice.

8.1.3 Evaluating the relevance of the artifact

The relevance of the artifact corresponds to the extent to which the business need is fulfilled which coincide with the contribution of the artifact to the business environment as discussed in section 1.6. The contribution to the business environment is twofold: on the one hand the artifact is believed to provide a more consistent level of assurance regarding the organisation's financial statements in the real-time economy, while on the other hand the artifact is believed to increase the quality of the external IT audit. In the evaluation form, the IT auditors were asked for their opinions regarding both relevance aspects. The results are presented in Table 17.

Table 17 - Evaluation results regarding the relevance of the artifact

Relevance aspect	Resp. A	Resp. B	Resp. C	Resp. D	Resp. E
A more consistent level of assurance	+	+	+	+	+
Quality of the external IT audit	+	-	+	+	+

* "+" indicates that the respondent accept the relevance aspect

** "–" indicates that the respondent deny the aspect as part of the artifact

*** A marked row indicates that there is a respondent who denies the aspect

A more consistent level of assurance

The respondents agreed upon the relevance of the artifact in relation to the provision of a more consistent level of assurance of financial statements in the real-time economy. Respondent B argued that the introduction of SAP GRC PC enables an organisation to provide more assurance regarding the extent to which the risks within their processes are mitigated. Obviously, an increase in the assurance of risk mitigating enables a more consistent level of assurance regarding the

organisation's financial statements. Since the artifact enables the external IT auditor to rely on a claim of the organisation that risks are mitigated with a more consistent level of assurance by relying on the monitoring results provided by SAP GRC PC regarding the operating effectiveness of the controls used to mitigate these risks, it is believed that the artifact is relevant to meet the business need of continuous assurance.

Quality of the external IT audit

Four of the respondents agreed that the artifact will increase the quality of the external IT audit (Respondents A, C, D, and E). Respondent B noticed that not the quality but the efficiency of the IT audit will increase because the IT auditor is no longer required to assess the operating effectiveness of each control individually. It is indeed a legitimate argument to state that the efficiency will increase. However, the quality increases as well. Currently, the operating effectiveness is estimated based on samples. By relying on the monitoring results regarding the operating effectiveness of controls, the operating effectiveness of each control could be determined with certainty and hence the quality of the external IT audit will increase.

8.2 Process evaluation

As already stated a process evaluation is aimed at evaluating the design process. It is believed that by ensuring the quality of the design process, this will increase the quality of the artifact to be designed as well. The quality of the process is often ensured by following general process criteria which are referred to in the literature as design guidelines (Verschuren & Hartog, 2005). The design guidelines to ensure process quality should not be confused with the guidelines that together form the design artifact in this research. According to Verschuren and Hartog (2005, p. 746), design guidelines "*are essentially an articulation of a design methodology*". Because in this research the design framework of Hevner et al. (2004) is used, the process evaluation should be performed accordingly. Therefore the design science research guidelines as proposed by Hevner et al. (2004) will be taken into account as presented in Table 18.

Table 18 - Design-science research guidelines adapted from (Hevner et al., 2004, p. 83)

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Guideline 1: Design as an artifact

According to Hevner et al. (2004, p. 82) the designed artifact "*must be described effectively, enabling its implementation and application in an appropriate domain*". The final design is considered a viable artifact since the guidelines could be used of the shelf to construct an audit plan to perform an IT audit of SAP GRC PC within the pharmaceutical industry. To ensure that the artifact is applicable in the IT audit domain, the artifact is designed according to semi-structured interviews with IT auditors themselves. Moreover, to ensure that the artifact is consistent with the current practices of the IT audit community, close attention is paid to the consistency of the artifact with respect to the GAM. Finally, to ensure the IT auditors knows how to apply the artifact within the

pharmaceutical industry, semi-structured interviews with pharmaceutical organisations are conducted to provide context to the business environment as part of the artifact.

Guideline 2: Problem relevance

Problem relevance is ensured by making explicit the business need that will be fulfilled by means of the artifact. In this research, the identified business need is to provide continuous assurance of an organisation's financial statements in the real-time economy as elaborated on section 1.6. Besides defining the business need itself, it is explained how the artifact is contributing to the business need. This is done by elaborating on the problem of audit timeliness. It is believed that the artifact enables IT auditors to address the problem of audit timeliness by auditing SAP GRC PC and hence assessing the operating effectiveness of controls with a more consistent level of assurance. Addressing the problem of audit timeliness contributes to the provision of continuous assurance in the real-time economy since the operating effectiveness is no longer determined in a retrospective fashion. Moreover, it is believed that the quality of the external IT audit itself increases as well since the IT auditor is no longer required to estimate the operating effectiveness of a control based on samples.

Guideline 3: Design evaluation

The artifact is evaluated according to a plan evaluation and process evaluation which are rigorously demonstrated evaluation methods (Verschuren & Hartog, 2005). However, an important limitation is that the artifact cannot be demonstrated into practice because no pharmaceutical organisations were found that have implemented and operationalised SAP GRC PC to monitor the operating effectiveness of controls continuously. During the execution of the research it was considered to organise a workshop in which the artifact could be applied to a fictional case. Such a workshop might come close to a real product evaluation. However, due to the fictional character of a case, the results are believed to be of limited value. Due to time constraints and the limited extent to which the results are believed to provide meaningful insights, it was decided not to design such an workshop.

Guideline 4: Research contributions

According to Hevner et al. (2004, p. 87), "*effective design-science research must provide clear contributions in the areas of the design artifact, design construction knowledge (i.e., foundations), and/or design evaluation knowledge (i.e., methodologies)*". First of all, the contribution in the area of the design artifact is the artifact itself, which is not uncommon in design science research (Hevner et al., 2004). The contribution of the artifact as a foundation could be explained as follows. The artifact is constructed according to existing foundations including risk and control theory, audit standards, and audit theory. These well-established foundations are applied within an unexplored research domain. The way these foundations are applied might function as a foundation for future research in the domain of continuous assurance, continuous auditing and continuous controls monitoring. Furthermore, the concept of architectural principles which is a foundation in enterprise engineering research is applied within the field of IT auditing. This is considered a relevant research contribution as well. Moreover, applying the research methodologies (i.e. desk research and semi-structured interviews) is considered a research contribution. Especially the way both methodologies are intertwined in order to derive relevant guidelines is considered a relevant contribution to the knowledge base.

Guideline 5: Research rigor

To ensure research rigor the well-known and broadly accepted research methodologies including desk research and semi-structured interviews are used to design the artifact. Furthermore, foundations from the knowledge base as visualised in Figure 5 in section 1.6 are used to construct the artifact. These foundations include: risk and control theory, audit standards, and CA theory. It should be noticed research did not explicitly link to audit standards in particular, but these are implicitly applied by taking into account the GAM. After all, the GAM is based on best practice standards such as COBIT and ITIL.

Guideline 6: Design as a search process

Within this research it is recognized that the design of the artifact is an incremental process. This is evidenced by a first improvement of the artifact according to the plan evaluation. Moreover it is recognized that this first improvement of the artifact is not the end station of the design. It is believed that improvements to the artifact should be made by evaluating the artifact in relation to the opinions of a more diverse group of IT auditors. Moreover it is believed that various relevant improvements will result from the execution of a product evaluation in which the design is demonstrated into practice.

Guideline 7: Communication of the research

The design will be communicated in various ways. First of all, the contributions to the knowledge base, which are of particular relevance for researchers, are communicated by means of a scientific article and this research report which will be made available in a public repository of the TU Delft. Moreover, a public presentation on the subject matter will be given. Second, the contributions to the environment, which are of particular relevance for IT auditors, are communicated by means of the artifact itself. This encompasses the frame of reference including the guidelines accompanied with the necessary explanatory notes consistent with the current knowledge of IT audit practitioners. Moreover, the artifact will be communicated to IT auditors via a private presentation within a Big4 audit firm.

8.3 Conclusion

The evaluation was conducted according to the study of Verschuren and Hartog (2005). Considering the plan evaluation, the artifact was evaluated in terms of clearness, acceptance and interrelatedness. The plan evaluation was conducted by asking the respondents to provide feedback regarding the structure of the artifact, the guidelines, and the relevance of the artifact. The feedback was received by means of an evaluation form. The respondents were largely on the same page regarding the structure and relevance of the artifact. However, there appears to be many inconsistencies among the respondents concerning the individual guidelines. Some of the inconsistencies resulted from unclear aspects within the artifact while some of the inconsistencies resulted from opposing opinions. It is believed that the opposing opinions originate from the novelty of using a CCM system (i.e. SAP GRC PC) for the purpose of the external audit and hence illustrates the complexity of the topic. According to the plan evaluation numerous points of improvement were identified which are presented in Table 19. Despite these improvements, it is believed to derive various other points of improvement when performing a product evaluation. However, because of the limited use of SAP GRC PC into practice, at this moment it turned out to be infeasible to perform a product evaluation of SAP GRC PC in the pharmaceutical industry. The initial design of the artifact is improved according to Table 19 as visualised in Figure 20. Considering the plan evaluation, the design science research guidelines of Hevner et al. (2004) were taken into account. It appears that all guidelines are followed during the execution of this research in a satisfactory manner.

Table 19 - Points of improvement according to the plan evaluation

Part of the artifact	Points of improvement
Guideline 2	• Relate to guideline 20 and 29
Guideline 4	• Relate to guidelines 26 -29
Guideline 5	• Clarify quality risk
Guideline 7	• Clarify quality risk
Guideline 12	• Relate to guideline 16 • Reformulate risk significance • Add “risk appetite”
Guideline 13	• Remove “manual” part
Guideline 14	• Clarify CCM-AC, CCM-MD, CCM-T • Relate to guideline 21 • Include data integrity as precondition • Add explanatory notes
Guideline 19	• Relate to guideline 22
Guideline 20	• Clarify monitoring rationale
Guideline 21	• Clarify target system and monitoring system • Reformulate “data targeted”
Guideline 22	• Clarify correctness
Guideline 24	• Exclude from frame of reference
Guideline 25	• Clarify monitoring rationale
Guideline 26	• Remove “time consuming” and “cost effective”
Guideline 27	• Add “knowledge regarding source system”
Guideline 28	• Exclude from frame of reference
Guideline 29	• Add “precondition that business rules are in best practice set”
Guideline 33	• Focus on relation to external auditor
Guideline 34	• Clarify process improvement
Guideline 35	• Clarify system improvement
New guideline	• Add guideline regarding changes made to the risk and control framework
Structure	• Relate to GAM • Abolish the “management of SAP GRC PC” area and transfer the associated guidelines to the “target system” area • Clarify the relation of guidelines to the testing of ITGCs • Add coherence by reformulating the guidelines in the same manner

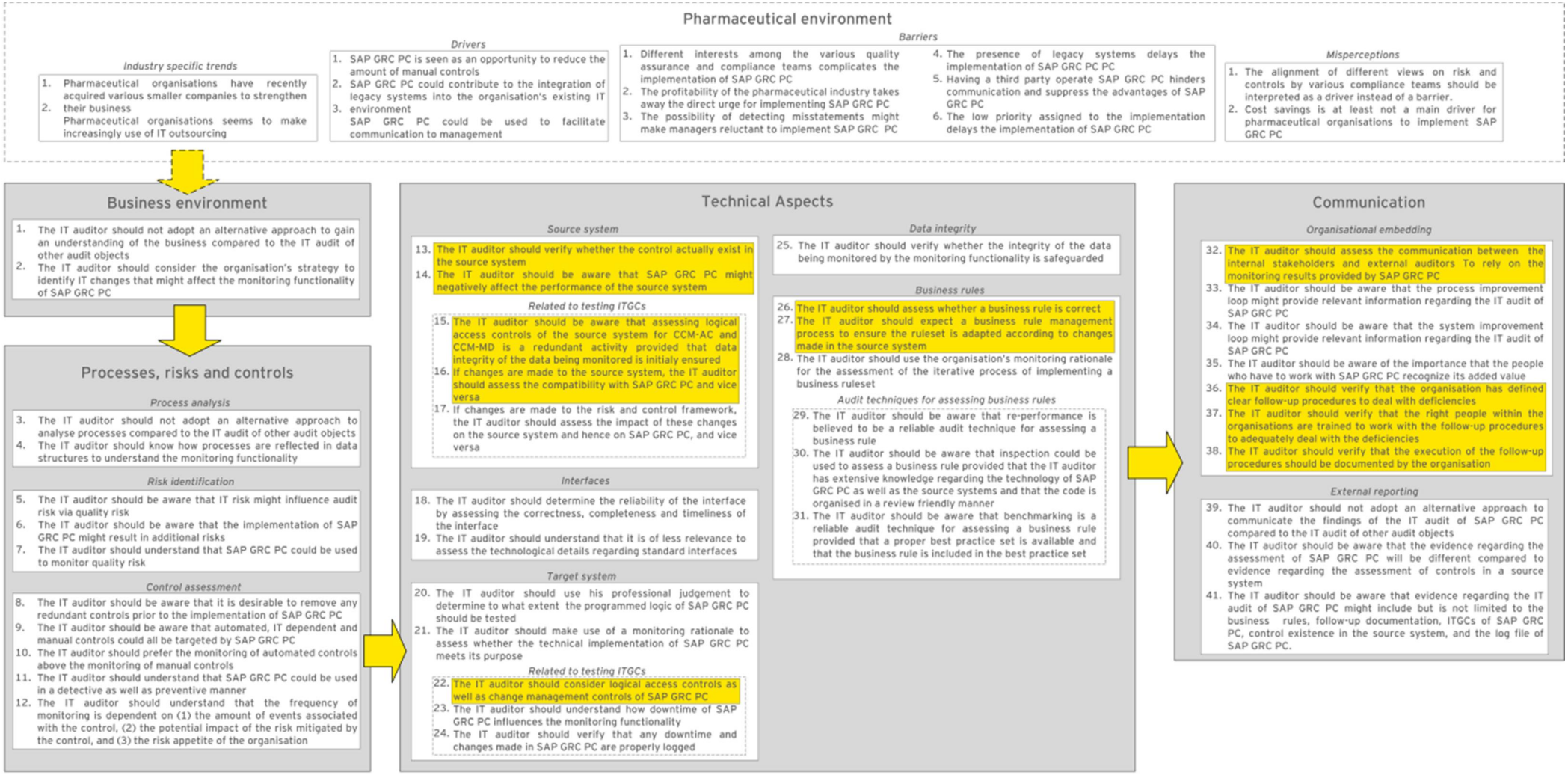


Figure 20 – A redesign of the set of guidelines

CONCLUSIONS

9

Conclusions and reflection

In this chapter, the main findings (9.1) will be discussed together with the theoretical contribution (9.2), the societal relevance (9.3), and the contributions to the audit community (9.4). Moreover the limitations of the research will be stated (9.5) where after areas for future research are proposed (9.6) and a reflection on the research is provided.

9.1 Conclusion

In this section, an answer to the main research question will be provided and the main findings of the research will be pointed forward. This research was focussed on exploring the use of a CCM system (i.e. SAP GRC PC) for the purpose of the external IT audit. At this moment IT auditors are testing ITGCs on the application level to estimate the operating effectiveness of controls. The introduction of CCM systems allowed for continuously monitoring the operating effectiveness of controls. However, to rely on the monitoring results for the purpose of the external IT audit, the CCM system itself should be audited. This research explored what areas should be addressed in the IT audit of a CCM system by answering the following main research question: "*How should the adequacy of the design and operating effectiveness of a continuous controls monitoring system be assessed in the pharmaceutical industry from the perspective of the external IT auditor?"*.

9.1.1 Answering the main research question

An answer to the main research question is embedded in the designed artifact. The final artifact is a set of guidelines that function as a frame of reference for constructing an audit plan to perform an IT audit regarding SAP GRC PC in the pharmaceutical industry. In this audit plan, the IT auditor states how the adequacy of the design and operating effectiveness of SAP GRC PC will be assessed. To guide the IT auditor in establishing the audit plan, in total 41 guidelines were formulated that could be classified into four different areas: (1) business environment, (2) processes, risks, and controls, (3) technical aspects and (4) communication. The IT auditor should address these areas which is in accordance with the audit methodology of a Big4 audit firm.

It turned out that the first two areas are not of particular relevance since they should not be approached in a significant different manner compared to the IT audit of other audit objects. Consequently, only twelve guidelines were formulated in these two areas. One important notion should be added to this conclusion. It turned out that IT auditors are relatively unfamiliar with how pharmaceutical organisations intend to use SAP GRC PC within their business. Therefore, an effort was made to identify and include industry specific aspects as part of the artifact.

The third area regarding the technical aspects turned out to be of particular relevance and encompasses nineteen guidelines. On the one hand, the guidelines regarding the technical aspects guide the IT auditor in determining relevant aspects regarding the adequacy of the design of SAP GRC PC; they provide guidance in identifying technical details regarding the implementation of SAP GRC PC. On the other hand, the guidelines regarding the technical aspects guide the IT auditor in determining relevant aspects regarding the operating effectiveness of SAP GRC PC; they provide guidance in identifying the preconditions that should be met to ensure the operating effective during a specified period of time.

The fourth area regarding the communication, in which ten guidelines were identified, turned out to be of relevance as well. Especially the organisational embedding of SAP GRC PC which is considered new in the audit of a CCM system. If the organisational embedding is inadequately established, it could be that the deficiencies are not communicated to the responsible instances or that the deficiencies are not properly followed up. In this case, the IT auditor could not rely on the monitoring results to assure the operating effectiveness of a control.

So to guide the IT auditor in determining what aspects to address to ensure the adequacy of the design and operating effectiveness of SAP GRC PC, 41 guidelines in four different areas were identified. In the following paragraph the main findings and corresponding guidelines will be stated.

9.1.2 Main findings

In this section the most relevant guidelines will be elaborated on. A guideline is considered of relevance if it addresses a new aspect or state that an aspect should be addressed differently compared to the performance of a general IT audit. In total 7 main findings were identified which are related to a schematic overview of a CCM system in Figure 21. It should be noticed that the numbering of the guidelines in some cases differ from the numbering in Chapter 7, this is due to the redesign of the artifact in Chapter 8 according to the evaluation results.

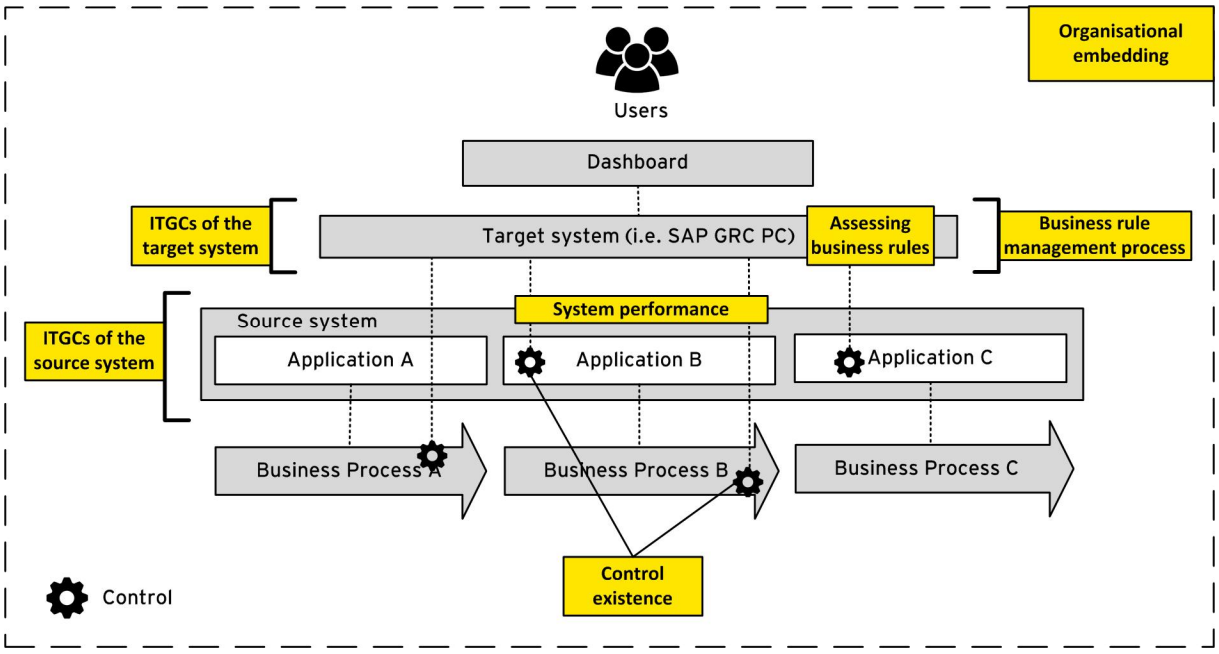


Figure 21 - Relating the main findings to the schematic overview of a CCM system

Control existence

In a traditional audit, the IT auditor is required to test the design of each individual control in the source system. The introduction of SAP GRC PC raises the question whether the IT auditor could rely on the target system to assure the existence of a control, or that the IT auditor should always go back to the source system to verify the existence of a control in every situation. To illustrate this finding: an empty deficiency report could either mean that there are no deficiencies or that there is no control. It was concluded that the IT auditor should always go back to the source system to verify that the control as presented in SAP GRC PC actually exists, which is reflected in guideline 13.

ITGCs of the source system

In a traditional audit, ITGCs are tested to provide reasonable assurance regarding the operating effectiveness of a control provided that the adequacy of the design is already established. By means of CCM, continuous insight in the operating effectiveness of a control is provided which give rise to the question whether it is still of relevance to assess the ITGCs of the source system. It is concluded that testing logical access controls in the case configuration data is being targeted to monitor the operating effectiveness of a control is a redundant activity, provided that any deficiencies are

properly followed up. On the other hand, in the case transactional data is being targeted the logical access controls are a prerequisite to rely on the insights regarding the operating effectiveness of a control. The difference between targeting configuration data and transactional data is that although beforehand it is known what data irregularities look like, in the case transactional data is targeted, it is beforehand unknown what the targeted data will look like in contrast to configuration data. This finding corresponds to guideline 15 in the artifact. It should be noticed that no evidence was found that other ITGCs has become redundant with the introduction of SAP GRC PC. In fact, it turned out that change management controls are of special importance in the new situation since now the compatibility of the source system with the target system should be assessed if changes are made to the source system. This finding is reflected in guideline 16.

ITGCs of the target system

With the introduction of SAP GRC PC, it was questioned whether it is of relevance to consider ITGCs of the target system. This is currently unknown since in traditional audits only ITGCs of the source system are considered; a target system was absent in the old situation. It turned out that it is of relevance to assess ITGCs of the target system. After all, if changes made to the benchmark data used to identify deficiencies or to the monitoring logic (i.e. business rules) this has a significant impact on the reliability of the monitoring results. This finding corresponds to guideline 22 in the artifact.

Assessing business rules

In traditional audits the operating effectiveness of a control is not continuously monitored by means of a CCM system. Consequently, the IT auditor is not likely to be familiar with monitoring logic used to continuously monitor the operating effectiveness of a control. Therefore attention was paid how the IT auditor should assess the monitoring logic. It turned out that the monitoring logic is captured in business rules and that it is of utmost importance that the business rule is correct. Obviously, if the business rule is incorrect, the monitoring results are not reliable and the IT auditor could not rely on the monitoring results. Moreover, wrong business rules could provide a false sense of security if an incorrect business rule remains unnoticed. This finding corresponds to guideline 26 in the artifact.

Business rule management process

As already argued for it is of relevance to assess the ITGCs of the target system. These ITGCs include system change management controls. System change management controls should ensure the source system is still compatible with the target system after changes are made to the source system, and vice versa. However, the system change management controls do not take into account the changes in terms of the business rule. Therefore it is argued that a business rule change management process should be in place, which is reflected in guideline 27. It could be argued that considering changes in terms of business rules might be classified as testing ITGCs of the source system. In this research, it is chosen to make the business rule management process a separate main finding to stress its importance in the audit of SAP GRC PC.

System performance

The introduction of SAP GRC PC could result in a decrease in system performance of a source system. Coupling the target system to the source system might negatively influence the performance of the source system, which is the result of executing business rules that target data which resides in the source system. It turned out that it is of particular relevance to consider the decrease of system performance since organisations might compensate for the decreasing performance by reducing the monitoring frequency which is reflected in guideline 14. This is of relevance since a decrease in the monitoring frequency directly affects the reliability of the monitoring results.

Organisational embedding

With the introduction of SAP GRC PC, the IT auditor might rely on the monitoring results for determining the operating effectiveness of a control. If no deficiencies are reported, and the monitoring functionality is properly established, the IT auditor could decide to rely on the monitoring

results. However, it was questioned what course of action IT auditors should take if deficiencies are reported. It is believed that the IT auditor still could rely on the monitoring results if the deficiencies are properly dealt with. This implies that the IT auditor assess the communication between stakeholders (guideline 32), assesses whether the organisation has defined clear follow-up procedures (guideline 36), assesses whether the organisation has trained the responsible individuals to execute the follow-up procedures (guideline 37), and that the results of the follow-up procedures are properly documented (guideline 38).

9.2 Theoretical contributions

A research into CCM

This research contributes to the exploration of CA practices by conducting a research into CCM systems. Currently, there are only a limited amount of studies that explore the use of a CCM system into practice, based on the MCL architecture as proposed by Vasarhelyi et al. (2004). The first two studies in this field were conducted anno 2006. Alles et al. (2006), and Alles et al. (2008) report on a research in which they implemented a continuous auditing system for continuous monitoring of business process controls (CMBPC) at the German manufacturing conglomerate Siemens AG. Furthermore, Kuhn and Sutton (2006) designed a continuous auditing system for testing financial transactions in the aftermath of the bankruptcy of the former American telecom operator Worldcom.

This research is similar to those studies since it takes the implementation of a CCM system (i.e. SAP GRC PC) in a real environment (i.e. the pharmaceutical industry) as a starting point. Besides SAP GRC PC and the pharmaceutical industry have not yet been explored within CCM studies, this research distinguishes from the existing literature, by adopting the perspective of the external IT auditor. This is in line with Sutton (2000) who argues based on Glaser et al. (1968) that a given phenomenon (i.e. CCM) should be studied from numerous perspectives until a consistent pattern arises which eventually might lead to new theory.

It could be questioned why it is of relevance to explore the use of a CCM system into practice. This could be explained as follows. It is believed that CA, and therewith CCM, as a phenomenon could potentially address the problem of audit timeliness (Chan & Vasarhelyi, 2011). Although the problem of audit timeliness is not new (Rezaee et al., 2002; Sutton, 2000), it appears that the problem is still not addressed in a satisfactory manner and becomes even more urgent in the real-time economy (Chan & Vasarhelyi, 2011; Chiu et al., 2014; Vasarhelyi, 2011). It is believed that in order to explore whether the claim that CCM could address the problem of audit timeliness is true, first a better understanding of the use of CCM into practice should be obtained.

Research methodologies

Applying the research methodologies (i.e. desk research and semi-structured interviews) is considered a research contribution as well. The relevance of this contribution is limited since semi-structured interviews and desk research are considered well established methodologies. However, the way both methodologies are intertwined in order to derive relevant guidelines is new and might function as a valuable starting point for other researches.

9.3 Contributions to the IT audit community

Auditing a CCM system

This research contributes to the IT audit community by designing an artifact that could be used for the performance of an IT audit of a CCM system. The designed artifact supports the IT auditor in assessing the adequacy of the design and operating effectiveness of SAP GRC PC. It could be questioned why it is of relevance for IT auditors to audit a CCM system. This could be explained as follows. It is believed that auditing a CCM system could assure the reliability of the monitoring results which might increase the efficiency and effectiveness of the external IT audit. On the one hand the efficiency might increase because the IT auditor is no longer required to assess the operating effectiveness of each control individually. On the other hand, the effectiveness might increase since the IT auditor is no longer required to estimate the operating effectiveness of a control in a retrospective fashion. It should be noticed that it was not investigated whether the efficiency and

effectiveness of the external IT audit will actually increase. The IT auditor himself should determine whether it is of relevance to make use of the monitoring results for the purpose of the external IT audit. What this research contributed, is an artifact that could be used to assess the operating effectiveness and adequacy of the design of a CCM system which is a prerequisite for relying on the monitoring results provided by that system.

Guidance in a changing profession

This research provides an artifact that is aimed at guiding the IT auditor in the performance of an audit of a CCM system. A set of guidelines that could be used for assessing the adequacy of the design and operating effectiveness of a CCM system is considered new in the IT audit profession. There seems no other artifacts that provide guidance regarding a particular audit object in the same manner as the artifact designed in this research. The contribution of the artifact to the audit profession could be explained by taking into account that the IT audit profession is currently subjected to change. In the real-time economy, the traditional audit paradigm seems to be outdated. This is claimed by Sutton (2000, p. 1) who stated that "*the audit profession is desperately trying to catch up with the changes in the business and financial world*", as well as by Chan and Vasarhelyi (2011, p. 152) who stated that the audit profession "*has not kept pace with the real-time economy*". Both claims implicitly call for new innovative approaches. This research contributes to this call by designing a unique artifact. Instead of approaching the audit object using the general audit methodology, this research approaches the audit object using an artifact tailored specifically for the object of interest. Because this research is the first to explore the use of guidelines in the audit profession, the real value of the artifact is unclear and should be explored in the future.

9.4 Societal relevance

An organisation's management is responsible for preparing financial statements on an annual basis. The reason for producing financial statements is to communicate the financial position and performance of that organisation towards stakeholders. Stakeholders might be shareholders or investors who rely on the statements to make economic decisions, or other members of society such as banks, suppliers and customers. Because stakeholders are not involved in managing the organisation, an independent external auditor is asked to assure the reliability of the financial statements. The problem faced by external auditors today is that they cannot assure the reliability of financial information continuously as demanded by the stakeholders in the real-time economy. The societal relevance of the artifact, provided that the underlying claim that assessing a CCM system addresses the problem of audit timeliness is true, is that the artifact might contribute to the provision of continuous assurance regarding financial information in the real-time economy.

9.5 Limitations

Generalizability

Four limitations were identified with respect to the generalizability of the research. The first limitation arises due the limited amount of IT auditors that have participated in the semi-structured interviews. The criteria for selecting the IT auditors were (1) the IT auditor should be familiar with CCM and (2) the IT auditor should be familiar with auditing in the pharmaceutical industry. It turned out that respondents who met both criteria were extremely rare. This was mainly due the fact that CCM practices are only used to a limited extent into practice. Consequently only five respondents who met at least one of the criteria were found to be willing to participate in the interviews. Furthermore, the IT auditors were related to the same Big4 audit firm. The fact that all respondents have the same background endangers the generalizability of the findings.

Second, the research was aimed at the pharmaceutical industry. The motivation for the pharmaceutical industry was that it is believed that pharmaceutical organisations are relatively advanced in the use of CCM practices due to the high risk nature of their business. Consequently, the artifact is only applicable in pharmaceutical industry and cannot be generalised to other industries without additional research.

Third, it turned out that various software applications might be used to establish a CCM functionality. For the purpose of this research it was decided to focus on SAP GRC PC since this

systems appeared to be most popular among pharmaceutical organisations and the system is well documented. Consequently, the findings are focused on SAP GRC PC in particular and cannot be generalised without additional research.

A fourth limitation is that the GAM is taken as a starting point. Although it is believed that the GAM is a representative reflection of well-established aspects of the audit methodology, the use of the GAM entails some limitations as well. For instance, the GAM might be slightly different from other audit methodologies designed by other Big4 audit firms which limit the generalizability of the artifact in combination with other audit methodologies. However, since all methodologies are based on the same best practices and standards, this limitation is believed to be of less relevance.

Methodology

Moreover, three methodological limitations were identified. First of all, a limitation arises due to the use of desk research. Despite the considerable effort to capture all relevant researches in the field of CCM, there remains the possibility that relevant studies are overlooked or wrongly classified as irrelevant. This possibility is inextricably linked to the performance of desk research and is considered a limitation of the methodology.

A second limitation arises due to the use of semi-structured interviews. Because of the novelty of the topic it was decided to make use of semi-structured interviews in order to capture aspects that where not taken into account beforehand as well. This gives rise to the possibility that relevant aspects are overlooked. This limitation is amplified by the use of a limited pool of respondents and should be taken into account when considering the research findings. Moreover there is the possibility that an interpretation error has been made although this limitation is at least partly addressed by means of the evaluation.

A third limitation arise due to the absence of a product evaluation. It turned out that it was not possible to perform a product evaluations since no organisation was found to have fully implemented SAP GRC PC in such a mature way that IT auditors could use it for the performance of an IT audit. It is believed that a product evaluation might provide valuable insights and points for improvement regarding the relevance and design of the artifact and hence the absence of a product evaluation is considered a limitation.

9.6 Future research

With respect to the main findings and the limitations of this research, three areas for future research could be identified. First of all, relevant future research contributions might focus on increasing the generalizability of the artifact. The generalizability of the artifact might be increased by (1) studying the applicability of the artifact in other industries, (2) improving the aspects of the artifact by taken into account audit methodologies created by other Big4 audit firms, (3) improving the artifact by considering other CCM systems (e.g. BWISE i2i or ARIS R&CM), or (4) studying the aspects of the artifact in accordance with a more diversified pool of respondents.

Furthermore, in this research the CCM functionality of SAP GRC PC is used to design the artifact. The technical architecture of SAP GRC PC is based on the MCL architecture as proposed by Vasarhelyi et al. (2004). It would be relevant to study whether it is possible for the IT auditor to use a CCM system based on an EAM architecture as well. It appears to be unknown what the impact will be on the external audit activities if EAMs are used to monitor the operating effectiveness of controls. For instance, in order to assess EAMs, the IT auditor is required to operate directly in the core applications underlying an organisation's business processes. It might be that the organisation is reluctant to let the IT auditor work directly into their core systems. Moreover, it could be questioned whether it is desirable to consider EAMs from the perspective of the external IT auditor.

Moreover, the artifact is currently not yet tested into practice which is considered a limitation. Applying the artifact in real-world situations is believed to result in valuable insights that could be used to further improve the artifact, especially regarding the guidelines to which the respondents were equivocal. Future research is needed to explore the use of the artifact into practice.

9.7 Reflection

Boundaries of the research

First of all, the research was scoped to a single software package to establish the monitoring functionality namely SAP GRC PC. I think that it was a good decision to focus on a single application instead of comparing various packages because of the explorative nature of the research. On the other hand, I think that the artifact will look different if an application based on the EAM architecture was selected. The guidelines regarding the monitoring logic (i.e. the business rules) would have been different because the monitoring logic will be part of the source system. Another application based on the MCL architecture would result in more or less the same artifact.

Furthermore, the research was scoped to the pharmaceutical industry. I don't expect the artifact to be significantly different if another industry was taken as a starting point. The main difference will be that organisations operate in another business environment and have different processes and risks. However, the environment, processes and risks seems not to have a significant influence on the monitoring functionality itself. Considering that the main findings of this research relate to the technical aspects and organisational embedding, I think that these findings would have come to light when considering another industry as well.

Moreover, the research was conducted in cooperation with a Big4 audit firm. In my opinion this have not affected the outcome of the research. Although the input for this research was mainly derived from practitioners from this particular firm, it is believed that the IT auditors at other firms would have provided mostly the same input and reviews because they have the same post-graduate educational background and reason with the same methodologies in mind.

Research methodologies

As regards to the research methodologies, I have made use of desk research and semi structured interviews. I felt comfortable using desk research. The main issue I experienced was that the audit profession makes use of their own complex methodologies and professional jargon with which I was not familiar at the beginning of this research. Consequently, I had some start-up struggles capturing the most relevant literature and concepts relevant to the topic.

Making use of semi-structured interviews to collect data was new to me. At the beginning I had some difficulty with the formulation of the questions. On the one hand I wanted to address some specific areas while, on the other hand I would give the respondents the opportunity to address new areas to capture the most novel areas that were not stated in the audit literature. I experienced the use of probes, as proposed by Harrell and Bradley (2009) very helpful with this matter.

Artifact design

First of all, I experienced some difficulties with defining what the final artifact should be. While performing an IT audit, this is done by testing the audit object against norms and standards. The artifact designed in this research are guidelines that guide the auditor in appointing relevant areas that should be assessed in the IT audit of SAP GRC PC by using norms and standards. Although, in the audit profession, there are rules and criteria for defining of norms and standards, it is unclear to what extent these rules and criteria apply to the formulation of guidelines. Looking at other research disciplines such as enterprise architecture troubled this question even more, since guidelines, principles, and norms are used in another context and seem to have other meanings. With this discussion in mind a new definition of a guideline was proposed tailored for the purpose of this research.

When it became clear how the guidelines should be formulated, I was struggling with capturing the underlying discussion into a single unambiguous guideline that met the definition of a guideline as discussed in Chapter 1. During the evaluation it became clear that the guidelines needed to be reformulated. I think that some of the guidelines could be sharpened in the future, if the artifact is used into practice.

Furthermore, I was struggling with the tension between the scientific demands and practical demands. Science demands that the guidelines are well founded in academic literature while practitioners demands that the guidelines point out the most relevant aspects in the IT audit of SAP GRC PC regardless of their scientific background. I felt this struggle especially during the interviews

were I was often focussing on gathering as much as possible information regarding the most novel aspects while paying less attention on why the IT auditors consider precisely these aspects of significance. On the other hand, I was aware of the fact that the IT auditors were responding based on their knowledge of the audit methodology and that their responses did not came out of thin air. Although the underlying theoretical backgrounds of the main findings are elaborated on in Table 13, it could be made more clear what the academic background is of the other guidelines. However, due to time constraints it turned out not to be feasible to elaborate on the theoretical background of all the 41 guidelines.

Another issue I experienced when processing the result derived from desk research and the interviews was that the amount of information relevant to the topic was overwhelming. This is the result of the explorative nature of the research. In the end, no less than a total of 41 guidelines were formulated. Because of the great amount of guidelines I had the feeling that I was not able to elaborate on all of them in detail. Consequently I have identified 7 main findings and elaborated on those. Identifying the main findings made me rethink the relevance of the other guidelines and aspects of the artifact which are not part of the main findings. Because the artifact is in the initial stage of design, I decided to include all 41 guidelines as part of the artifact. However, it could very well be that in the future some guidelines turn out to be redundant and should be excluded from the artifact. I think that it will become more clear which guidelines are redundant when the artifact is applied within a real-world situation which stresses the importance of future research.

10

References

AICPA. (1983). Statement on Auditing Standards 47 *Audit Risk and Materiality in Conducting an Audit*

AICPA. (2006). Statement on Auditing Standards 109 *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*.

Alles, M., Brennan, G., Kogan, A., & Vasarhelyi, M. A. (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems, 7*(2), 137-161.

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting continuous auditing theory into practice: Lessons from two pilot implementations. *Journal of Information Systems, 22*(2), 195-214.

Blokdijk, J. (2004). Tests of control in the audit risk model: effective? Efficient? *International Journal of Auditing, 8*(2), 185-194.

Boritz, J. E. (2004). Managing Enterprise Information Integrity: Security, Control and Audit Issues. Chicago: Information Technology Governance Institute.

Caldwell, F., & Proctor, P. E. (2009). Continuous Controls Monitoring for Transactions: The Next Frontier for GRC Automation. *Gartner, January*.

Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems, 12*(2), 152-160.

Chiu, V., Liu, Q., & Vasarhelyi, M. A. (2014). The development and intellectual structure of continuous auditing research. *Journal of Accounting Literature, 33*(1), 37-57.

CICA/AICPA. (1999). Continuous auditing. Toronto, Canada: The Canadian Institute of Chartered Accountants.

Clark, D. D., & Wilson, D. R. (1987). *A comparison of commercial and military computer security policies.* Paper presented at the 2012 IEEE Symposium on Security and Privacy.

COSO. (1992). Internal Control – Integrated Framework. *The Committee of Sponsoring Organizations of the Treadway Commission*.

COSO. (2004). Enterprise Risk Management – An Integrated Framework. *The Committee of Sponsoring Organizations of the Treadway Commission*.

Cukier, K. N., & Mayer-Schoenberger, V. (2013). The Rise of Big Data: How It's Changing the Way We Think About the World. *Foreign Affairs, 92*(3), 28-40.

Davenport, T. H. (1993). *Process innovation: reengineering work through information technology*: Harvard Business Press.

Debreceny, R. S., Gray, G. L., Ng, J. J.-J., Lee, K. S.-P., & Yau, W.-F. (2005). Embedded audit modules in enterprise resource planning systems: Implementation and functionality. *Journal of Information Systems, 19*(2), 7-27.

Dietz, J. L., & Hoogervorst, J. A. (2008). *Enterprise ontology in enterprise engineering.* Paper presented at the Proceedings of the 2008 ACM symposium on Applied computing.

Eilifsen, A., Knechel, W. R., & Wallage, P. (2001). Application of the business risk audit model: A field study. *Accounting Horizons, 15*(3), 193-207.

Eimers, P. (2006). Het audit risico model is spinglevend! *Maandblad voor Accountancy en Bedrijfseconomie*, 76-83.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review, 14*(4), 532-550.

Elder, R. J., & Allen, R. D. (2003). A longitudinal field investigation of auditor risk assessments and sample size decisions. *The Accounting Review, 78*(4), 983-1002.

Elliott, R. K. (2002). Twenty-first century assurance. *Auditing: A Journal of Practice & Theory, 21*(1), 139-146.
EY. (2013). Maximizing value from your lines of defense *Insights on governance, risk and compliance*.
EY. (2014). Unlocking the power of SAP's governance, risk and compliance technology *Insights on governance, risk and compliance*.
FDA. (2013). Guidance for industry: oversight of clinical investigations–a risk-based approach to monitoring. *Washington, DC: US Department of Health and Human Services*, 0910-0733.
FDA. (2014). Code of Federal Regulations Title 21 *Subpart A (general provisions), Section 312.3 (definitions and interpretations)*.
FERMA/ECIIA. (2010). Guidance on the 8th EU Company Law Directive, article 41 *Guidance for boards and audit committees*. Brussels: Federation of European Risk Management Associations (FERMA) and European Confederation of Institutes of Internal Auditing (ECIIA).
Flowerday, S., & Von Solms, R. (2005). Real-time information integrity= system integrity+ data integrity+ continuous assurances. *Computers & Security, 24*(8), 604-613.
Gantz, S. D. (2013). *The Basics of IT Audit: Purposes, Processes, and Practical Information*: Elsevier.
Glaser, B. G., Strauss, A. L., & Strutzel, E. (1968). The Discovery of Grounded Theory; Strategies for Qualitative Research. *Nursing Research, 17*(4), 364.
Gonzalez, G. C., Sharma, P. N., & Galletta, D. F. (2012). The antecedents of the use of continuous auditing in the internal auditing context. *International Journal of Accounting Information Systems, 13*(3), 248-262.
Groomer, S. M., & Murthy, U. S. (1989). Continuous auditing of database applications: An embedded audit module approach. *Journal of Information Systems, 3*(2), 53-69.
GTAG. (2009). Auditing Application Controls *Global Technology Audit Guide*. USA: The Institute of Internal Auditors.
GTAG. (2012). Information Technology Risk and Controls *Global Technology Audit Guide*. USA: The Institute of Internal Auditors.
Harrell, M. C., & Bradley, M. A. (2009). Data collection methods. Semi-structured interviews and focus groups: DTIC Document.
Hevner, v. A. R., Salvatore T, M., Jinsoo, P., & Sudha, R. (2004). Design science in information systems research. *MIS quarterly, 28*(1), 75-105.
ICH. (2005). ICH Harmonised Tripartite Guideline: Quality Risk Management Q9.
IFAC. (2009a). ISA 200 *Overall Objectives Of The Independent Auditor And The Conduct Of An Audit In Accordance With International Standards On Auditing*: International Auditing and Assurance Standards Board (IAASB), International Federation of Accountants (IFAC).
IFAC. (2009b). ISA 315 *Identifying and Assessing the Risk of Material Misstatement Through Understanding the Entity and its Environment*: International Auditing and Assurance Standards Board (IAASB), International Federation of Accountants (IFAC).
IFAC. (2009c). ISA 500 *Audit Evidence*: International Auditing and Assurance Standards Board (IAASB), International Federation of Accountants (IFAC).
IFAC. (2013). ISA 610 *Using the Work of Internal Auditors*: International Auditing and Assurance Standards Board (IAASB), International Federation of Accountants (IFAC).
IIA. (2013). The Three Lines of Defense in Effective Risk Management and Control. In T. I. o. I. A. (IIA) (Ed.), *International Professional Practices Framework (IPPF)*.
ISACA. (2011). The Three Lines of Defence Related to Risk Governance. *ISACA Journal, 5*.
Johnstone, K. M., & Bedard, J. C. (2001). Engagement planning, bid pricing, and client response in the market for initial attest engagements. *The Accounting Review, 76*(2), 199-220.
Kloosterman, H. (2004). Wat is eigenlijk risicoanalyse in de accountantscontrole? *Maandblad voor Accountancy en Bedrijfseconomie*, 570-578.
Knechel, W. R. (2001). *Auditing: assurance & risk*: South-Western Pub.
Knechel, W. R. (2007). The business risk audit: Origins, obstacles and opportunities. *Accounting, Organizations and Society, 32*(4), 383-408.
Kogan, A., Sudit, E. F., & Vasarhelyi, M. A. (1999). Continuous online auditing: A program of research. *Journal of Information Systems, 13*(2), 87-103.
Kuhn, J. R., & Sutton, S. G. (2006). Learning from WorldCom: Implications for fraud detection through continuous assurance. *Journal of Emerging Technologies in Accounting, 3*(1), 61-80.
Kuhn, J. R., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The current state and future directions. *Journal of Information Systems, 24*(1), 91-112.

Lemon, W. M., Tatum, K. W., & Turley, W. S. (2000). *Developments in the audit methodologies of large accounting firms*: ABG Professional Information London, UK.
Lindgreen, E., Veltman, P., & Fijneman, R. (2005). Grondslagen IT-auditing. Vol 1.
Mock, T. J., & Wright, A. M. (1999). Are audit program plans risk-adjusted? *Auditing: A Journal of Practice & Theory, 18*(1), 55-74.
Nelson, M., & Ambrosini, J. (2007). Enterprise Risk Management and Controls-Monitoring Automation Can Reduce Compliance Costs. *Bank Accounting & Finance*.
NOREA. (2013). C1 – Raamwerk Assurance-opdrachten door IT-auditors.
Op't Land, M., & Proper, H. (2007). *Impact of principles on enterprise engineering.* Paper presented at the Relevant rigour–Rigorous relevance: Proceedings: 15th European Conference on Information Systems (ECIS 2007), St. Gallen, Switzerland, June 2007.
Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems, 24*(3), 45-77.
POB. (2000). The Panel on Audit Effectiveness: Report and Recommendations: Public Oversight Board.
Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*(6), 849-855.
Proper, E., & Greefhorst, D. (2011). Principles in an enterprise architecture context. *Journal of Enterprise Architecture, 7*(1), 8-16.
PwC. (2015a). How can pharmaceutical and life sciences companies strategically engage global outsourcing? *Global Pharmaceuticals and Life Sciences Industry Group*.
PwC. (2015b). Three Lines of Defense model. Retrieved 19 May, 2015, from http://www.pwc.nl/nl/governance-risk-compliance/three-lines-of-defense-model.jhtml
Racz, N., Weippl, E., & Seufert, A. (2010). *A frame of reference for research of integrated governance, risk and compliance (GRC).* Paper presented at the Communications and Multimedia Security.
Rezaee, Z., Elam, R., & Sharbatoghlie, A. (2001). Continuous auditing: the audit of the future. *Managerial Auditing Journal, 16*(3), 150-158.
Rezaee, Z., Sharbatoghlie, A., Elam, R., & McMickle, P. L. (2002). Continuous auditing: Building automated auditing capability. *Auditing: A Journal of Practice & Theory, 21*(1), 147-163.
Sudhalkar, A. (2011). SAP Business Objects Process Control 10.0 Automated Monitoring Overview. *Official SAP Documentation*.
Sutton, S. G. (2000). The changing face of accounting in an information technology dominated world. *International Journal of Accounting Information Systems, 1*(1), 1-8.
TOGAF. (2004). TOGAF - The Open Group Architectural Framework.
van Niekerk, S. (2013). *Evaluating the '3-Lines of Defense Model', Reaching for Effective Risk Management and Control.* TU Delft, Delft.
Van Praat, J., & Suerink, H. (2013). *Inleiding ICT-auditing*. The Hague: Sdu uitgevers
Vasarhelyi, M. A. (2011). The Coming Age of Continuous Assurance. *Insights, 9*, 23-39.
Vasarhelyi, M. A., Alles, M., Kuenkaikaew, S., & Littley, J. (2012). The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. *International Journal of Accounting Information Systems, 13*(3), 267-281.
Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting, 1*(1), 1-21.
Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. *Auditing: A Journal of Practice & Theory, 10*(1), 110-125.
Vasarhelyi, M. A., Romero, S., Kuenkaikaew, S., & Littley, J. (2012). Adopting continuous auditing/continuous monitoring in internal audit. *ISACA Journal, 3*, 31.
Verschuren, P., & Hartog, R. (2005). Evaluation in design-oriented research. *Quality and Quantity, 39*(6), 733-762.
Yin, R. K. (1984). *Case study research*. Beverly Hills, CA: Sage Publications.
Zmud, R. (1997). "Editor's Comments". *MIS quarterly, 21*(2), xxi-xxii.

APPENDICES

Appendix 1. Semi-structured interview protocols

In this appendix, the semi-structured interview protocols are presented. The protocols are constructed according a research regarding semi-structured interviews provided by the non-profit research organisation RAND (Harrell & Bradley, 2009). First, the protocol for the pharmaceutical organisations is presented. This protocol is provided English. The protocol composed for the interviews with the IT auditors was only constructed in Dutch since all the respondents were Dutch speaking.

Semi-structured interview protocol pharmaceutical organisations

Introduction

My name is Tim Sweep and currently I'm in the final stage of my masters Systems Engineering, Policy Analysis and Management at the TU Delft. Moreover, I follow an Information Architecture track. For the purpose of my master thesis I conduct a research into the audit of the continuous controls monitoring functionality of SAP GRC in pharmaceutical organisations by external IT auditors. The component of SAP GRC which could be used for CCM is the PC component (SAP GRC PC). The reason for approaching you for an interview is because I'm interested in the motives of pharmaceutical organisations whether or not to implement SAP GRC PC.

** Do you have any questions regarding my thesis at this moment?**

Duration

The interview will approximately take one hour. I will update you on the time we have per part of the interview.

Is it a problem for you if the interview will last a bit longer than expected beforehand?

Anonymity

All interviews I conduct for the purpose of my thesis will be processed anonymous. Your name will not be included in the report. I want to ask you if I may record the interview? This will allow me to focus on our conversation instead of making notes. The recording will only be used for writing a short report of the interview and will not be made public.

Data processing

In the report, I will use the insights derived from the interviews to formulate guidelines. These guidelines will be structured in a way they could be used as a frame of reference that might be used by an IT auditor to perform an audit regarding SAP GRC PC. The research will be published in a public repository of the TU Delft. There will not be any other kind of documentation made public.

** Do you have any questions so far?**

PART 1: Introduction (5 min)

Questions	Motives
1a. Could you please tell me something about yourself? PROBE: education PROBE: work experience PROBE: function within the organisation 1b. Could you elaborate on your experience with SAP GRC? PROBE: In your opinion, which functionalities does SAP GRC have? 1c. Could you elaborate on your experience with CCM? PROBE: What is in your opinion the concept of CCM?	1a-c. The backgrounds of the interviewees might be used to assign weights to certain responses.

PART 2: Motives from the pharmaceutical industry (45 min)

Area	Questions	Motives
SAP GRC in general (15min)	2a. What are drivers for implementing SAP GRC within your organisation? PROBE: Could you elaborate on these drivers? PROBE: Which stakeholders are proponents of implementing SAP GRC? Why? 2b. What are barriers for implementing SAP GRC within your organisation? PROBE: Could you elaborate on these barriers? PROBE: Which stakeholders are opponents of implementing SAP GRC? Why? 3. Does your organisation have implemented SAP GRC at this moment? PROBE: According to which of the abovementioned drivers/barriers, why? PROBE: Who is responsible for implementing SAP GRC (or should be responsible)? 4a. For which processes and applications do you consider implementing SAP GRC valuable? PROBE: Could you elaborate on this? 4b. How could SAP GRC be used to support these processes and applications? PROBE: Could you elaborate on this?	2a-b. The motive of this question is to gain insight into the drivers and barriers for the implementation of SAP GRC. 3. The purpose of this question is to identify the most relevant drivers and barriers for SAP GRC. 4a-b. The purpose of this question is to identify the processes and applications for which SAP GRC might be used.
CCM functionality of SAP GRC (15min)	5a. Which advantages do you recognize for monitoring controls continuously? PROBE: Could you elaborate on these advantages? 5b. Which disadvantages do you recognize for monitoring controls continuously? PROBE: Could you elaborate on these disadvantages? 6. Is the CCM functionality (PC) a driver for the organisation to implement a SAP GRC suite? PROBE: Could you elaborate on this? 7a. For which processes and applications do you think it is relevant to use the CCM functionality of SAP GRC? PROBE: Could you elaborate on this? 7b. How could the CCM functionality of SAP GRC be used to support these processes and applications? PROBE: Could you elaborate on this?	5a-b. The motivation for this question is to gain insight into the advantages and disadvantages of CCM. 6. The motivation for this question is to gain insight into the importance of the CCM functionality of SAP GRC.. 7a-b. The purpose of this question is to identify processes and applications in which CCM could be useful.
Relation to external audit	8a. According to your experience, What is the relation between an implemented SAP GRC suite in which CCM	8. The motivation for this question is to gain insights into

(15min)	functionality is established and the activities of the external IT auditor? PROBE: Could CCM be used to decrease the intensity of audit activities of the external IT auditor? PROBE: Could CCM be used to make the organisation more transparent for the external IT auditor? 8b. According to your experience, What is the relation between an implemented SAP GRC suite in which CCM functionality is established and the activities of the financial auditor? PROBE: Could CCM be used to decrease the intensity of audit activities of the financial auditor? PROBE: Could CCM be used to make the organisation more transparent for the financial auditor?	the relation between the CCM functionality of Sap GRC and the activities of the external auditor from a business perspective.

PART 3: Closing (10min)

Questions	Motivation
7. Are there any important things remained undiscussed during the interview? PROBE: Which things do you want add according to what we have already discussed?	7. According to the expertise of the respondents, they might provide relevant input for the research to which not enough attention is paid during the interview.

Semi-structured interview protocol external IT auditors

Introduction

My name is Tim Sweep and currently I'm in the final stage of my masters Systems Engineering, Policy Analysis and Management at the TU Delft. Moreover, I follow an Information Architecture track. For the purpose of my master thesis I conduct a research into the audit of the continuous controls monitoring functionality of SAP GRC in pharmaceutical organisations by external IT auditors. The component of SAP GRC which could be used for CCM is the PC component (SAP GRC PC). The reason for approaching you for the interview is because I'm interested in how, according to external IT auditors, SAP GRC PC should be audited.

** Do you have any questions regarding my thesis at this moment?**

Duration

The interview will approximately take one hour. I will update you on the time we have per part of the interview.

Is it a problem for you if the interview will last a bit longer than expected beforehand?

Anonymity

All interviews I conduct for the purpose of my thesis will be processed anonymous. Your name will not be included in the report. I want to ask you if I may record the interview? This will allow me to focus on our conversation instead of making notes. The recording will only be used for writing a short report of the interview and will not be made public.

Data processing

In the report, I will use the insights derived from the interviews to formulate guidelines. These guidelines will be structured in a way they could be used as a frame of reference that might be used by an IT auditor to perform an audit regarding SAP GRC PC. The research will be published in a public repository of the TU Delft. There will not be any other kind of documentation made public.

** Do you have any questions so far?**

Deel 1: Introductie (5min)

Vragen	motivatie
1a. Kunt u iets meer over u zelf vertellen? PROBE: opleiding PROBE: relevante werkervaring PROBE: functie binnen organisatie? 1b. Kunt u iets meer vertellen over uw ervaring met SAP GRC? PROBE: Wat verstaat u onder het concept SAP GRC? 1c. Kunt u iets meer vertellen over uw ervaring met CCM? PROBE: Wat is uw definitie van CCM?	1. De achtergronden van de respondenten kunnen wellicht gebruikt worden voor het wegen van verschillende antwoorden.

Deel 2: Ontwerpeisen en aannames (45 min)

Gebied	Vragen	Motivatie
Structuur (5min)	2. Aan welke gebieden moet een IT auditor aandacht besteden bij het auditen van de CCM functionaliteit van SAP GRC? PROBE: business environment, risico en controls, technologie, en audit proces.	2. Rechtvaardigen opnemen business environment, risico en controls, technologie, en audit proces als gebieden waarbinnen ontwerpeisen en aannames

		geformuleerd worden.
Business environment (10min)	3a. In welke aspecten van de bedrijfsomgeving zal een IT auditor inzicht moeten verkrijgen om tot een gedegen beoordeling van de CCM functionaliteit van SAP GRC te komen? PROBE: In hoeverre is het belangrijk om inzicht te krijgen in de bedrijfsprocessen en ondersteunende applicaties? PROBE: In hoeverre is het relevant om de link tussen CCM en de bedrijfsstrategie te begrijpen? PROBE: In hoeverre verschilt het in kaart brengen van de business environment voor het auditen van de CCM functionaliteit van SAP GRC met het in kaart brengen van de business environment voor een andere audit? 3b. Zijn er voorwaarden waaraan de business environment moet voldoen om de CCM functionaliteit van SAP GRC te kunnen gebruiken? PROBE: Is het gebruik van CCM relevant voor alle applicaties/processen?	3a. Inzicht krijgen in de ontwerpeisen vanuit de business environment. 3b. Inzicht krijgen in de aannames vanuit de business environment.
Risico en controls (10min)	4a. Met SAP GRC kunnen alleen geautomatiseerde controls worden gemonitord. Bent u van mening dat het auditen van de CCM functionaliteit van SAP GRC voldoende kan zijn voor het afdekken van een risico? PROBE: Hoe belangrijk zijn de geautomatiseerde controls ten opzichte van de IT dependent controls en manual controls? 4b. Hoe zou een IT auditor moeten bepalen of het monitoren van controls met SAP GRC voldoende is om een risico af te dekken? 4c. Bent u van mening dat alle geautomatiseerde controls continu gemonitord moeten worden? PROBE: Welke controls wel / niet? PROBE: In welke mate speelt de grootte van het afgedekte risico een rol bij het bepalen van welke controls wel of niet continu gemonitord moeten worden? 4d. Hoe zou een IT auditor moeten bepalen met welke regelmaat (continu/wekelijks/maandelijks) een control gemonitord moet worden? PROBE: In welke mate speelt de grootte van het afgedekte risico een rol bij het bepalen van de regelmaat? PROBE: In welke mate spelen andere controls die hetzelfde risico afdekken een rol bij het bepalen van de regelmaat? 4e. Zitten er additionele risico's aan het gebruik van de CCM functionaliteit van SAP GRC? PROBE: technologische risico's? PROBE: hoe verhouden deze risico's zich ten opzichte	4a-e: Inzicht krijgen in de ontwerpeisen op het gebied van risico en controls

	van de additionele risico's van andere applicaties? 4f. Zijn er randvoorwaarden waaraan de risico's en controls moeten voldoen zodat ze kunnen worden gemonitord met SAP GRC?	 4f. Inzicht krijgen in de aannames op het gebied van risico en controls.
SAP GRC technologie (10min)	5a. In welke technologische aspecten zal een IT auditor inzicht moeten verkrijgen om tot een gedegen beoordeling van de CCM functionaliteit van SAP GRC te komen? PROBE: Hoe zal een IT auditor de integriteit van de data vast kunnen stellen? PROBE: nadruk op mechaniek 5b. Aan welke technologische eisen zal de CCM functionaliteit van SAP GRC moeten voldoen om op de output te kunnen bouwen voor de externe IT audit? PROBE: nadruk op output 5c. Zijn er technologische eisen waaraan het IT-landschap van een organisatie moet voldoen voordat controls continu gemonitord kunnen worden met SAP GRC? PROBE: Welke geautomatiseerde controls kunnen niet gemonitord worden met SAP GRC? (configuratie tabellen wel maar hoe zit het met hard coded controls?)	5a-b. Inzicht krijgen in de technologische ontwerpeisen. 5c. Inzicht krijgen in de technologische randvoorwaarden.
Audit proces (10min)	6a. Hoe zal een IT auditor de CCM functionaliteit van SAP GRC moeten beoordelen? PROBE: Naar welke aspecten van de CCM functionaliteit van SAP GRC zal de IT auditor moeten kijken? PROBE: Hoe kan de IT auditor zichzelf ervan verzekeren dat de control weergegeven in het dashboard ook daadwerkelijk bestaat en werkt? PROBE: Hoe verhoud dit zich tot het beoordelen van andere audit objecten? 6b. Aan welke eisen moet geschikt bewijsmateriaal voor het auditen van de CCM functionaliteit van SAP GRC voldoen? PROBE: Hoe zit dit met bewijs materiaal om vast te stellen of de weergegeven controls in het dashboard ook daadwerkelijk bestaan? PROBE: Hoe verhoudt dit zich tot de eisen aan geschikt bewijsmateriaal voor andere audits? 6c. Hoe zou een IT auditor zijn conclusies van de audit van SAP GRC moeten formuleren en rapporteren? PROBE: Hoe moet een IT auditor met de output van het dashboard omgaan? (flagging vs automatisch terugzetten configuraties) PROBE: Hoe verhoudt dit zich tot de rapportage van de conclusies van een ander audit object?	6a-c: Inzicht krijgen in de ontwerpeisen op het gebied van het audit proces.

Deel 3: Afsluiting (10 min)

Vragen	Motivatie
7a. Op welke van de vier besproken gebieden heeft u de meeste expertise? 7b. Zijn er gebieden waar u onvoldoende vanaf waardoor uw antwoorden minder betrouwbaar zijn? 7c. Zijn er naar uw mening relevante dingen onbesproken gebleven? PROBE: Welke dingen zou u nog willen bespreken?	7a-b: Als respondenten verschillende antwoorden geven kan hun achtergrond wellicht gebruikt worden voor het wegen van de verschillende antwoorden. 7c. Gezien de expertise van de respondenten zouden zij relevante input kunnen leveren voor het onderzoek waar nog niet in voldoende mate bij stil gestaan is gedurende het interview.

Appendix 2. Explanatory notes on audit risk, IT risk, and quality risk

Audit risk

Definition

Audit risk made its appearance in the audit profession during the 1970s with the development of the audit risk model (ARM). The American Institute of Certified Public Accountants (AICPA) was the first to standardize the ARM with the publication of their Statement on Auditing Standards (SAS) No. 47 (AICPA, 1983). Audit risk can be defined as "the risk that the auditor expresses an inappropriate audit opinion whether the financial statements are materially misstated" (IFAC, 2009a). According to this definition, audit risk is of particular importance for the financial auditor, who is responsible for assessing an organisation's financial statements.

Method

The ARM expresses audit risk as a function of inherent risk, control risk and detection risk as visualised in Figure 22. In Table 20 the definitions of the components of the ARM are provided as stated in the ISA 200 (IFAC, 2009a).

Table 20 - Risk concepts

Risk concept	Definition
Audit risk	Audit risk is the risk that the auditor expresses an inappropriate audit opinion whether the financial statements are materially misstated
Risk of material misstatements	"Risk of material misstatements is the risk that the financial statements are materially misstated prior to audit. This consists of two components, described as follows at the assertion level: inherent risk and control risk."
Inherent risk	"Inherent risk is the susceptibility of an assertion about a class of transaction, account balance or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls."
Control risk	"Control risk is the risk that a misstatement that could occur in an assertion about a class of transaction, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's internal control."
Detection risk	"Detection risk is the risk that the procedures performed by the auditor to reduce audit risk to an acceptably low level will not detect a misstatement that exists and that could be material, either individually or when aggregated with other misstatements."

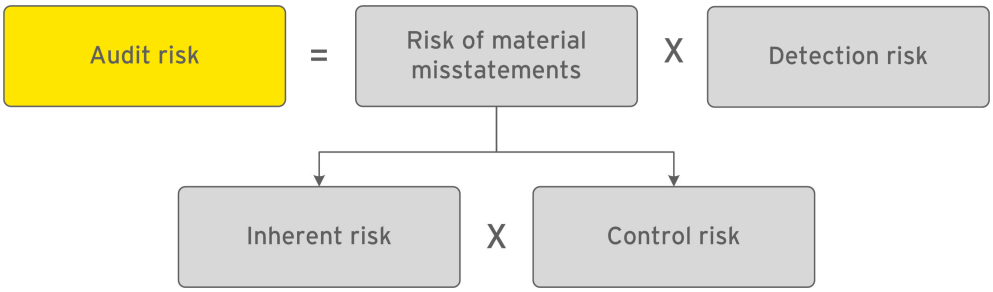


Figure 22 - Audit Risk Model

Examples

The inherent risk depends on the susceptibility of an assertion. The susceptibility of an assertion increases for instance when the organisation is newly established because of an acquisition or merger. Another example of which increases the susceptibility of an assertion is the complexity of the organisations business. For instance, if a financial institution trades in highly complex financial products. If the susceptibility increases, the inherent risk increases as well.

The control risk is related to an organisation's internal control structure. If the organisation has an adequate control framework, the likelihood that a misstatement will be prevented increases which decreases the control risk. In other words, if for instance an organisation does not have a proper segregation of duty policy, this increases the control risk.

Detection risks occur due to the limitations of audit procedures. Sampling for instance is commonly used in audit procedures which by definition, means that only a part of the population is taken into account which increases the detection risk. Also professional judgement increases the detection risk because there is the probability of misjudgement. Other factors that could be considered limitations of audit procedures are: the scope of the audit, time constraints, auditor independence or management representations.

IT risk

Definition

An IT risk can be defined as the technical risk that an organisation faces through the use of IT (GTAG, 2012). An external IT auditor supports the financial auditor by analysing the risks within the IT environment of an organisation that could affect the audit risk. More specifically, the IT auditor assess the IT components of the internal control structure which is related to the control risk and hence provide insight in the audit risk as can be derived from the ARM.

Method

The starting point of the IT risk assessment is a description of the IT components and their relations which together forms the organisation's IT environment. Assessing risks arising from the IT environment of modern organisations is complex because of the many interrelations and variety of IT components. Moreover, the IT environment differs greatly between organisations, even for organisation within the same industry. Consequently, there is not a single best practice methodology that could be used for assessing IT risks. However, IT risks seems to arise for the largest part from three areas: IT infrastructure, IT projects and outsourcing (GTAG, 2012).

Examples

Identifying risks within the IT infrastructure encompasses the identification of vulnerabilities arising from individual IT components, the interfaces between IT components within the organisation or the interfaces with IT components from the external environment. Moreover, the people who are interacting with the infrastructure might be a potential source of risks as well. Because the IT infrastructure of modern organisations, even for organisations within the same industry such as pharmaceuticals, differs greatly from each other, there is no standardized set of risks that could be used off the shelf. However, in the ISA 315, the IFAC described numerous examples of IT risks that could originate from the IT infrastructure such as inaccurately processing data, unauthorized access to data, unauthorized data changes in master files, to systems or to programs, inappropriate manual intervention, or inability to access data (IFAC, 2009b).

Because IT is to a great extent subjected to change, a lot of IT projects are executed within the IT environment to keep the IT environment topical. As regards to IT projects, potential risks are the risk of insufficient or inadequate resources, poor project management, or insufficient technical expertise (GTAG, 2012).

Outsourcing activities such as Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) are becoming more popular. Consequently, the risks associated with outsourcing are becoming more significant. Typical risks associated with outsourcing are the financial strength and stability of the service provider, or its internal control structure (GTAG, 2012).

Quality risk

Definition

While audit risk and IT risk is especially of interest for external auditors, quality risk management is of critical interest for pharmaceutical organisations. Quality risk can be defined as the risk that a set of inherent properties of a product, system, or process does not fulfils predefined requirements (ICH,

2005). The development and use of medicines inevitably entails an amount of risk. The risk of insufficient quality throughout the entire drug lifecycle is an important part of the entire amount of risk since it might result in serious health issues or even death to patients. Therefore it is of critical importance that the quality of processes concerning the development, manufacturing, distribution and inspection of a drug is safeguarded by properly assessing quality risks.

Method

A commonly used guideline for quality risk management is the ICH Q9 which is developed in by the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) (ICH, 2005). Within the ICH project, various stakeholders including governmental bodies from Japan, the United States and the European Union as well as experts from the pharmaceutical industry collaborated to establish the ICH Q9 guideline. The ICH Q9 guideline "specifically provides guidance on the principles and some of the tools of quality risk management that can enable more effective and consistent risk-based decisions, by both regulators and industry, regarding the quality of drug substances and drug products across the product lifecycle" (ICH, 2005). An important part of the guideline is the quality risk management process which is presented in
Figure 23.

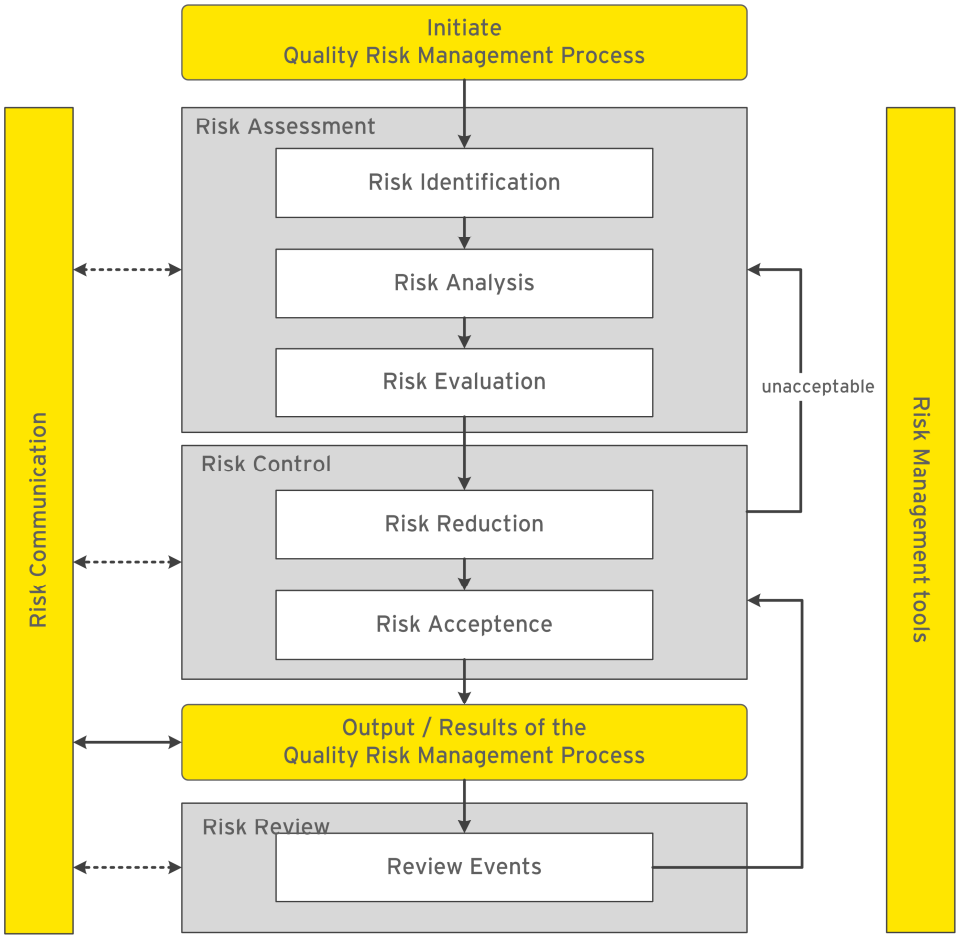


Figure 23 – Quality Risk Management Process adopted from (ICH, 2005, p. 2)

Examples

The guideline provides a non-exhaustive list of areas where quality risks might occur including: drug development, facilities and equipment, materials management, production, laboratory control and stability testing, packaging and labelling, or regulatory inspections. For each of these areas the guideline provides detailed examples.

Appendix 3. Explanatory notes on the internal control structure

Controls can be classified in various ways (GTAG, 2012). From the perspective of the IT auditor, the internal control structure is most often approached by the model as presented in Figure 8. Now all the components of the model will be discussed in more detail.

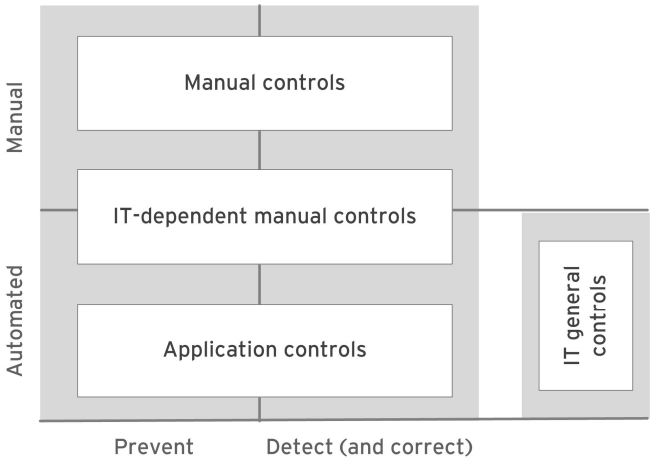


Figure 24 - internal control structure adopted from the GAM

First of all, as can be seen in the figure, a distinction is made between manual controls and automated controls. The difference between both is straightforward: automated controls are executed within automated systems (e.g. ERP systems or individual applications) and manual controls are executed by humans. Second, a distinction is made between prevent and detect and correct controls. Preventive controls prevent an error or incident from occurring. When an error or incident could not be prevented, detective controls could detect the errors or incidents after their occurrence. There are also controls that correct the error or incident after detection. An example of a preventive control is an access control which prevent unauthorized access to a system. This preventive control is considered a manual control when the physical access of a person is limited to certain systems. When access is controlled virtually by the system (e.g. password) the control is considered an automated one. An example of a detective control is a control that analyses the account numbers on invoices and detect inactive accounts or accounts that are marked as suspicious. This detective control can be either manual when the invoices are analysed by a person or automated when the invoices are analysed automatically within a system.

Moreover, according to the GAM of a Big4 audit firm, IT auditors distinguish three categories of controls: manual controls, IT dependent controls, and application controls. As already explained, manual controls are those controls executed by humans. IT-dependent controls are controls in which a person is dependent on the automated output from a computerized environment. An example of an IT-dependent control is a control which requires a person to approve automatically generated purchase orders. Notwithstanding the relevance of manual and IT-dependent controls, the work of an IT auditor is to a greater extent focused on application controls when assessing the adequacy of the design and operating effectiveness of a CCM functionality. Application controls are those controls that are specific to a program or application supporting a particular business process (GTAG, 2009). Roughly, there are five types of application controls: input controls which are used to control the data entered into a business process, processing controls which are used to control the processing of data within a business process, output controls which are used to control the data that flows out of a business process, integrity controls which are used to control the integrity of the data being processed or stored, and management trial controls which are used to keep track of data within the business process by composing a so called audit trail (GTAG, 2009). An example of an application control is a control which enforces that only orders with an approved order number can be processed.

Besides the three categories of controls there is another type of control which is referred to as IT general controls (ITGCs). Although it might be suggested by the figure that ITGCs are solely

automated, in fact ITGCs can be manual controls as well. The reason for positioning like that in the figure is because effective ITGCs are a precondition to rely on automated controls. As opposed to application controls, ITGCs are not bounded to a specific business process but affect all applications, programs and system components within an organisation. According to GTAG (2012), the objectives of ITGCs are "to ensure the appropriate development and implementation of applications, as well as the integrity of program and data files and of computer operations". Roughly, there are six kinds of ITGCS: logical access controls, system development controls, program change management controls, security controls, system backup and recovery controls, and computer operation controls (GTAG, 2009).

Appendix 4. Explanatory notes on the Three Lines of Defense model

In this appendix the Three Lines of Defense model will be elaborated on which is presented in Figure 11. As can be seen in the figure, the three lines of defense report to the governing bodies and senior management of the organisation. The governing bodies and senior management have essential roles in the Three Lines of Defense model since they are collectively responsible and accountable for establishing proper governance structures and processes to ensure the organisation's objectives are achieved. Communicating and dealing with the deficiencies as reported by SAP GRC PC should be part of the organisation's governance structure and hence fall under the responsibility of the governing bodies and senior management.

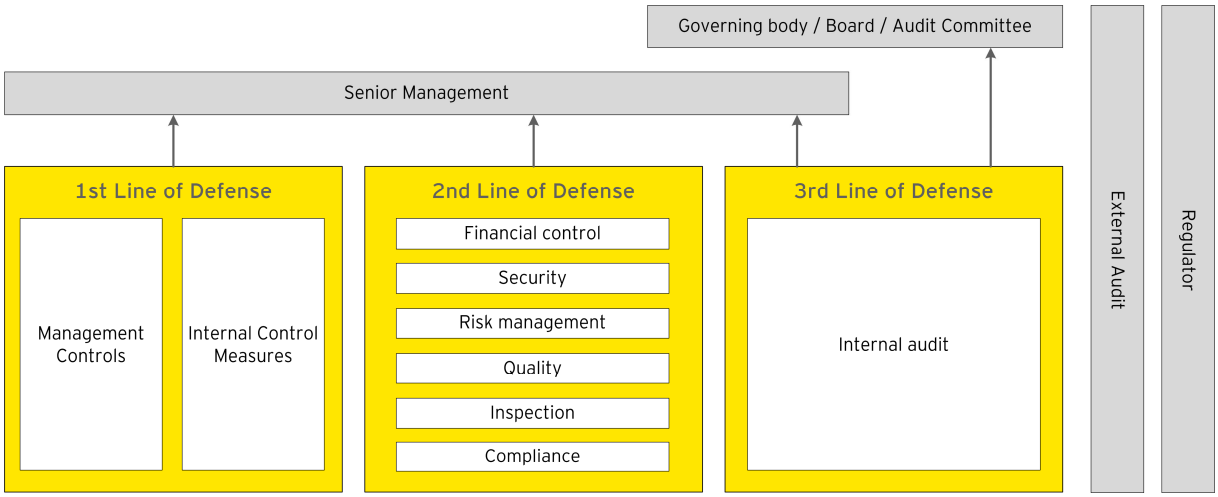


Figure 25 - Three Lines of Defense model adapted from IIA (2013, p. 2)

The first line of defense is the *operational management* of the organisation. Operational management *"has ownership, responsibility and accountability for assessing, controlling and mitigating risks together with maintaining effective internal controls*" (FERMA/ECIIA, 2010). So the basic activities of operational managers are (1) to identify and assesses risks and (2) designing and operating controls to mitigate the risks. An important part of these activities is to communicate information regarding their activities to all relevant entities within the organisation. Furthermore, it is for the operational managers to propose business improvements they deem necessary. The activities of the operational manager are executed on a daily basis. It is utopia that no deficiencies occur within the first line of defense and that operational management functions flawless. This stresses the need for an oversight entity which is embodied in the second line of defense.

The second line of defense are the risk management and compliance functions of the organisation. The risk management and compliance functions "*facilitates and monitors the implementation of effective risk management practices by operational management and assists the risk owners in defining the target risk exposure and reporting adequate risk related information through the organisation*" (FERMA/ECIIA, 2010). The second line of defense evaluates whether the first line of defense is arranged properly and functions as intended. Typically the second line of defense could directly intervene in the activities executed by the first line of defense in operating the risk and control framework. Because of their intervention power, the second line of defense cannot be considered truly independent from the first line of defense. Consequently, the second line is not the appropriate entity to perform internal audit activities regarding risk management and the internal control structure. This is why it is important to have a third line of defense.

The third line of defense are the internal auditors. Internal auditors "*will, through a risk based approach, provide assurance to the organisation's board and senior management, on how effectively the organisation assesses and manages its risks, including the manner in which the first and second lines of defence operate*" (FERMA/ECIIA, 2010). The third line of defense is considered the most independent body within the organisation. The activities of the third line of defense might include to

audit whether the organisation's risk and control approach meets recognized international standards or to audit whether the reporting of all relevant findings are properly communicated to the governing body (IIA, 2013).

Special attention should be paid to the regulative bodies and external auditors which resides outside the organisation. Especially in the pharmaceutical industry, regulative bodies such as the FDA play an important role in the organisation's overall governance structure. Regulative bodies force organisation's to meet certain industry specific regulation. Consequently, the organisation is required to show compliance to this regulation by designing and implementing controls according to the regulation and communicate on the operating effectiveness of the control to the regulative body. As regards to the external auditors, they provide assurance to stakeholders outside the organisation. As already stated in the introduction these stakeholders include the shareholders, investors, banks suppliers, customers, and other members of society. These stakeholders want assurance on the financial statements of the organisation from a truly independent body. Since the internal audit team is part of the organisation itself, they are not truly independent while the external auditor is[10]. Despite the complementary relationship between the internal auditor and external auditor, the external auditor relies on the evaluation of the risk and control structure made by the internal auditor in his assessment (FERMA/ECIIA, 2010).

[10] It should be noticed that the external auditor is paid by the organisation being audited. Consequently, it could be argued whether the external auditor itself is truly independent.

Appendix 5. Evaluation form

In this appendix, the evaluation form as sent to the respondents is presented. Since the IT auditors all have Dutch backgrounds, the evaluation form was created in Dutch. The initial version of the artifact was together with the evaluation form sent to the respondents. It should be noticed that the formulation of the guidelines in the initial version of the artifact are in certain cases slightly different from the formulation of the guidelines in the questions as presented in the review form. However, in essence the guidelines were the same. This was due the fact that at the time the respondents were asked for their opinions, the initial version of the artifact still had to be finalised.

Introduction

Uit de interviews en literatuuronderzoek heb ik heb ik een aantal guidelines afgeleid. Deze guidelines zou een IT auditor moeten volgen om een IT audit uit te oefenen op SAP GRC PC . De guidelines moeten geïnterpreteerd worden als een aanvulling op de GAM. De guidelines zijn gecategoriseerd naar audit fase en weergegeven in het diagram op de volgende bladzijde. Ik zou graag uw feedback vragen over (1) de structuur van het diagram zelf (2) de guidelines en (3) de relevantie van het geheel aan guidelines. De vragen staan onder het diagram.

Deel 1 Diagram structuur

De onderstaande vragen gaan over de structuur van het diagram. Kunt u ten minste commentaar geven als u het oneens bent met de vraag? Natuurlijk is commentaar ook welkom als u het eens bent met de vraag.

Vraag	eens/oneens/neutraal	Commentaar
Wat vindt u van het opnemen van “business environment” als audit fase?		
Wat vindt u van het opnemen van “processes, risks and controls” als audit fase?		
Wat vindt u van het opnemen van “technological aspects” als audit fase?		
Wat vindt u van het opnemen van “organisational embedding” als audit fase?		

Vraag	eens/oneens/neutraal	commentaar
Wat vindt u van het het opnemen van de “technological architecture” als onderdeel van de technological aspects?		
Wat vindt u van het het opnemen van de “CCM functionality of SAP GRC PC” als onderdeel van de technological aspects?		

Vraag	
Zou u iets willen veranderen aan de structuur van het diagram?	
Heeft u verder nog opmerkingen over de structuur van het diagram?	

Deel 2 Guidelines

Een guideline moet worden gezien al een guideline die de IT auditor moet volgen bij het auditen van SAP GRC PC in de farmaceutische industrie.

Het diagram is opgedeeld in 12 blokken met guidelines. De onderstaande tabellen komen overeen met deze blokken en bevatten de guidelines zoals weergegeven in het diagram. Kunt u in onderstaande tabellen aangeven of u het eens, oneens of neutraal bent over het opnemen van dit guideline? Kunt u ten minste commentaar geven als u het oneens bent met de vraag? Natuurlijk is commentaar ook welkom als u het eens bent met de vraag. Verder wordt er per blok gevraagd of u nog belangrijke guidelines mist die een IT auditor moet volgen bij het auditen van SAP GRC PC.

Guidelines regarding understanding the business

Guideline	eens/oneens/neutraal	commentaar
1. Understanding the business environment does not significantly differ in the case of auditing SAP GRC PC		
2. The IT auditor should take into account the organisation's strategy from a monitoring perspective		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding process analyses

Observations	eens/oneens/neutraal	commentaar
3. The identification of relevant processes does not differ in the case of auditing SAP GRC PC		
4. It should be known how processes are translated to data structures in the underlying IT environment		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding risk identification

Guideline	eens/oneens/neutraal	commentaar
5. IT risk might influence audit risk via quality risk		
6. The implementation of CCM itself introduces additional risks.		
7. CCM systems used to monitor controls regarding quality risk should be part of the IT audit		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding control assessment

Guideline	eens/oneens/neutraal	commentaar
8. Any redundant controls should be excluded from the organisation's internal control structure prior the establishment of SAP GRC PC.		
9. Manual, IT dependent, and automated controls could all be monitored by means of CCM as established in SAP GRC.		
10. Automated controls are preferred above manual controls		
11. CCM meets the need of organisations and IT auditors because it has a detective nature as well as a preventive nature		
12. The frequency of monitoring is dependent on the amount of events associated with the control as well as the significance of the risk mitigated by the control.		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding the source system

Guideline	eens/oneens/neutraal	commentaar
13. The existence of a control should be manually verified in the source system		
14. The logical access controls of the source system in the case for CCM-AC and CCM-MD is an redundant activity		
15. It should be known how changes made to the source system affects the compatibility with SAP GRC PC and vice versa.		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding the interfaces

Guideline	eens/oneens/neutraal	commentaar
16. It should be known to what extent the monitoring functionality affects the performance of the source system		
17. The interface should be assessed in terms of correctness, completeness and timeliness.		
18. It is of less relevance to assess the technological details of standard interfaces		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding the target system

Guideline	eens/oneens/neutraal	commentaar
19. The extent to which the programmed logic of SAP GRC PC should be assessed is determined by the IT auditor using his professional judgement.		
20. A monitoring rationale could be used to assess if the target system meets its purpose		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding data integrity

Guideline	eens/oneens/neutraal	commentaar
21. The integrity of the data being targeted by the monitoring functionality has to be safeguarded.		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding business rules

Guideline	eens/oneens/neutraal	commentaar
22. It should be known whether the business rule is correct		
23. A business rule management processes is required to translate changes to the source system in terms of the business ruleset		
28. An adequate risk and control framework is a prerequisite before designing business rules		
29. For the assessment of the iterative process of implementing a business ruleset the organisation's monitoring rationale should be used		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding the assessment of business rules

Guideline	eens/oneens/neutraal	commentaar
24. Re-performing a business rule is reliable but time consuming and cost-ineffective		
25. Inspection requires the IT auditor to have the extensive knowledge of SAP GRC PC and requires that the business rules are formulated in a review friendly manner.		
26. Client review might be less reliable compared to other audit techniques but could be applied whenever the IT auditor lacks extensive knowledge regarding SAP GRC PC.		

27. Benchmarking is a reliable audit technique for assessing a business rule provided that a proper best practice set is available		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding the management of SAP GRC PC

Guideline	eens/oneens/neutraal	commentaar
30. It is of relevance to consider logical access controls as well as change management controls with respect to SAP GRC PC		
31. It should be known how downtime of SAP GRC PC influences the monitoring functionality		
32. Downtime and changes made in SAP GRC PC should be properly logged		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding organisational embedding

Guideline	eens/oneens/neutraal	commentaar
33. To rely on the monitoring results regarding the operating effectiveness of a control the communication between operational management and internal auditors, together with the communication between the internal auditors and external auditors should be assessed		
34. The process improvement process might provide relevant information regarding the IT audit of SAP GRC PC		
35. The system improvement process might provide relevant information regarding the IT audit of SAP GRC PC		
36. It is of importance that the people who have to work with SAP GRC PC recognize its added value		
37. There should be clear follow-up procedures defined within the organisation to properly deal with deficiencies		
38. The right people within the organisations should be trained to work with the follow-up procedures to adequately deal with the deficiencies		
39. The execution of the follow-up procedures should be documented		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Guidelines regarding external reporting

Guideline	eens/oneens/neutraal	commentaar
40. The reporting of the findings of the IT audit of SAP GRC PC does not differ compared to the IT audit of other audit objects		
41. Evidence regarding the assessment of SAP GRC PC will be different compared to evidence regarding the assessment of controls in a source system.		
42. Evidence regarding the IT audit of SAP GRC PC might include but is not limited to the business rules, follow-up documentation, ITGCs of SAP GRC PC, control existence in the source system, and the log file of SAP GRC PC.		

Mist u in deze fase van de audit guidelines? Zo ja welke?

Deel 3 Relevantie van het geheel aan guidelines

Zou u op de volgende stellingen willen reageren?

If the IT auditor could rely on the monitoring results provided by SAP GRC PC, this will improve the quality of the external IT audit.

Using the monitoring results of SAP GRC PC allows the financial auditor to provide a more consistent level of assurance regarding an organisation's financial statements in the real-time economy.

Appendix 6. Plan evaluation

In this appendix the frame of reference as well as the guidelines will be evaluated by means of a plan evaluation. In order to do so, the responses from the IT auditors stated in the evaluation form will be taken into account and discussed. The evaluation criteria that are considered of relevance for the discussion are: *clearness, acceptance*, *interrelatedness* and *Consistency with the GAM*. The evaluation criteria are elaborated on in Table 14.

Table 21 - Evaluation criteria

Evaluation criteria	Description
Clearness	Clearness refers to whether aspects being evaluated are clear on first sight for the users of the artifact (i.e. external IT auditors). The clearness is derived according to the comments of the IT auditors.
Acceptance	The acceptance of aspects being evaluated refers to whether IT auditors accept the aspect as part of the artifact. The acceptance is derived according to the ratings provided by the IT auditors.
Interrelatedness	The interrelatedness reveals whether the individual aspects of the artifact are dependent on each other or contradictory. The interrelatedness is derived according to the comments of the IT auditors.
Consistency with the GAM	The consistency with the GAM refers to the relation of the artifact with respect to the GAM. The consistency with the GAM is derived according to the comments of the IT auditors. It should be noticed that this evaluation criteria will only be used for evaluating the structure of the frame of reference.

Evaluating the frame of reference

Table 22 - Evaluation results regarding the frame of reference

Aspect	Resp. A	Resp. B	Resp. C	Resp. D	Resp. E
Business environment	+	+	+	+	+
Processes, risks and controls	+	+	+	+	+
Technological aspects	+	+	+	+	+
Technical architecture	+	+	+	+	+
CCM functionality of SAP GRC PC	+	+	+	+	+
Communication	+	–	+	+	+

* "+" indicates that the respondent accept the aspect as part of the artifact

** "–" indicates that the respondent deny the aspect as part of the artifact

*** A marked row indicates that there is a respondent who denies the aspect

Communication

Respondent B questioned whether the organisational embedding as part of the communication is relevant in the context of assuring the reliability of financial statements. Indeed it could be argued that a proper follow up within the organisation is not directly of relevance for the financial audit. However, IT auditors do not operate SAP GRC PC themselves. The monitoring results are communicated via the internal stakeholders. Therefore, the IT auditor should assess whether the monitoring results are communicated completely and unaltered. Without the assessment of the organisational embedding it is not possible to rely on the monitoring results for assuring the reliability of the financial statements. Actually, following this line of reasoning, it could be argued that all other activities are pointless if the communication is not assured. Moreover, the guidelines that are part of the organisational embedding are considered relevant for the audit of SAP GRC PC as will be discussed later on. Consequently, it is decided to accept all aspects of the artifact.

Additional notions

The aspects of the artifact correspond directly to aspects within the GAM. The business environment corresponds to *understand the business*; processes, risks and controls correspond respectively to *identify SCOTs*, *understand SCOTs*, and *execute test of controls*; technical aspects correspond to

understand IT environment; only communication is not directly referred to in the GAM. It was questioned why different names were used since this might mislead the IT auditors who have to work with the artefact in accordance with the GAM (Respondent B). The different names were the result of the nature of the research in which various sources not related to the GAM were consulted. Since this research was conducted in cooperation with a Big4 audit firm, and to increase the applicability of the artefact into practice, it is decided to include references to the GAM.

Evaluating the guidelines regarding the business environment

Table 23 - Evaluation results regarding the guidelines related to the business environment

Aspect	Guideline	Resp. A	Resp. B	Resp. C	Resp. D	Resp. E
Business environment	1	+	0	+	+	+
	2	+	+	0	+	+

* "+" indicates that the respondent accept the aspect as part of the artifact

** "0" indicates that the respondent is neutral regarding the aspect as part of the artifact

Guideline 2

It was noticed that guideline 2 is related to guideline 20 and 29 since the organisation's strategy regarding IT should be reflected in the monitoring rationale (Respondent A). If the organisation's strategy and monitoring rationale are inconsecutive, this might endanger the applicability of guideline 20 and 29. This relation should be made explicit within the artifact.

Additional notions

According to Table 23, it appears that both guidelines are accepted as part of the artefact. Moreover, it was argued that a guideline should be included which refers to the identification of industry specific characteristics (Respondent B). It was assumed that identifying industry specific characteristics was part of understanding the business environment. When consulting the GAM, indeed it turned out that industry specific characteristics are part of gaining an understanding of the business environment. Consequently, it is decided not to include a separated guideline regarding the industry specific characteristics.

Evaluating the guidelines regarding processes, risks and controls

Guideline 4

Respondent E noticed that guideline 4 is related to the guidelines involved with the assessment of a business rule (i.e. guidelines 26 – 29) since insight into the data structures allows the IT auditor to determine whether the business rule targets the right data. This relation will be made explicit in the artifact.

Guideline 5

This guideline states that IT auditors should adapt a broader perspective on audit risk in the pharmaceutical industry and take into account quality risk since IT risk might influence audit risk via quality risk. It turned out that it was not clear what is meant with quality risk which should be clarified within the artifact.

Guideline 6

As can be derived from Table 24, two respondents did not accept guideline 6 as part of the artifact while the other respondents did. Respondent C argued that the additional risk resulting from the use of SAP GRC PC does not affect the processes themselves. This indeed is true. However, the fact remains that the use of SAP GRC PC introduces the additional risk of insufficient or incorrect knowledge as explained in section 4.2. Furthermore, respondent B argued that the use of SAP GRC PC does not affect the IT risk. This seems to be incorrect. The risk of insufficient or incorrect knowledge results directly from the use of SAP GRC PC and according to the definition of IT risk as

used in this research (GTAG, 2012) this qualifies as IT risk. Consequently, the discussion is decided in favour of the majority of respondents and hence the guideline 6 will be accepted.

Table 24 - Evaluation results regarding the guidelines related to processes, risks and controls

Aspect	Guideline	Resp. A	Resp. B	Resp. C	Resp. D	Resp. E
Processes analysis	3	+	+	+	+	+
	4	+	+	0	+	+
Risk identification	5	+	?	0	+	?
	6	+	–	–	+	+
	7	+/–	?	+	+	?
Control assessment	8	+	+	0	–	–
	9	+	+	0	+	–
	10	+	+	0	+	0
	11	+	+	+	+	+
	12	+	–	+	0	+

* "+" indicates that the respondent accept the aspect as part of the artifact
** "0" indicates that the respondent is neutral regarding the aspect as part of the artifact
*** "–" indicates that the respondent deny the aspect as part of the artifact
**** "?" indicates that aspect is not clear to the respondent
***** A marked row indicates that there is a respondent who denies the aspect

Guideline 7

Just like guideline 5, the meaning of guideline 7 was called into question because it appears to be unclear what is meant with quality risk. Therefore it is decided to clarify quality risk in the artifact.

Guideline 8

Two of the respondents did not accept guideline 8 as part of the artifact. Respondent D argued that redundant controls should not be removed until SAP GRC PC has been established because it might be needed to rely on them in the case SAP GRC PC does not function properly. This is not true; a redundant control could always be removed from the internal control structure, otherwise the control would not be redundant. Furthermore, it should be noticed that SAP GRC PC itself does not replace any control. Therefore, there it will never be the case that controls being monitored will not function as a result of the monitoring activity as suggested by respondent D. Moreover, respondent E argued that it is simply not necessary to remove redundant controls. This is a legitimate argument. However, the reason for including this guideline is to prevent that significant effort is put in establishing the monitoring functionality for redundant controls. Obviously, if the organisation is not planning to monitor redundant controls, this guideline is less applicable. However, the guideline itself seems not to be wrong. Therefore, it is decided to include the guideline in the artifact.

Guideline 9

Respondent E questioned whether manual controls could be monitored. As regards to the documentation of SAP GRC PC, it could be derived that there is the possibility to monitor automated self-assessment lists. So it is possible to monitor manual controls, although it should be noticed that this cannot be continuous due to the incremental nature of manual controls. Taking into account the that respondent E has no experience with SAP GRC PC whereas the auditors who accepted the guideline did, it is decided to accept the guideline as part of the artifact.

Guideline 12

Respondent B argued that the risk appetite should be part of guideline 12 as well. This seems to be a legitimate argument; after all, if the organisation is risk averse the monitoring functionality should be increased regardless of the amount of events associated with the risk and the significance of the risk. Therefore it is decided to include risk appetite as part of guideline 12. Furthermore, respondent A noticed that the significance of the risk corresponds with its impact. It appears that the term "risk

impact" is more accepted within the audit community compared to risk significance. Consequently, it is decided to reformulate the guideline.

Additional notions

Furthermore, respondent A noticed that risk identification is in particular related to the insight derived from the business environment understanding. This relation is covered in the artifact by means of the arrow between the business environment area and the processes, risks and controls area. It is believed that the findings resulting from the business environment are of relevance for processes and controls as well. Therefore it is decided not to change the arrow within the artifact.

Evaluating the guidelines regarding the technological aspects

Table 25 - Evaluation results regarding the guidelines related to the technological aspects

Aspect	Guideline	Resp. A	Resp. B	Resp. C	Resp. D	Resp. E
Source system	13	+	–	+	+	0
	14	No resp.	–	0	–	–
	15	+	+	+	+	+
Interfaces	16	–	+	0	0	0
	17	+	+	+	+	+
	18	+	+	0	0	0
Target system	19	+	+	+	+	–
	20	+	?	0	?	–
Data integrity	21	+	+	+	+	+
Business rules	22	+	+	+	+	+
	23	+	+	0	+	+
	24	+	–	+	+	0
	25	+	?	+	?	?
	26	+	–	–	–	+
	27	+	+	+	+	–
	28	–	+	–	–	0
	29	+	+	0	+	+
Management of SAP GRC PC	30	+	+	+	+	+
	31	+	+	0	+	+
	32	+	+	0	+	0

* "+" indicates that the respondent accept the aspect as part of the artifact

** "0" indicates that the respondent is neutral regarding the aspect as part of the artifact

*** "–" indicates that the respondent deny the aspect as part of the artifact

**** "?" indicates that aspect is not clear to the respondent

***** A marked row indicates that there is a respondent who denies the aspect

Guideline 13

As can be derived from Table 25, respondent B did not accept the guideline 13 as part of the artifact. It was argued that the existence of a control could be verified automatically by means of applications such as Approva Bizrights which could be used to automatically assess the existence of application controls. According to this argument, the guideline will be rephrased in a way that it is no longer suggested that the existence of a control should be manually verified. However, the need for verifying the existence of the control within the source system remains.

Guideline 14

As regards to guideline 14, none of the respondents accepted the guideline as part of the artifact. The argument for not accepting the guideline is that the integrity of the source data should always be assured if that data is targeted by SAP GRC PC. Indeed it should be included that the integrity of data being targeted by CCM-AC and CCM-MD is a strict pre-condition for this guideline. Moreover,

when interpreting the responses, it was concluded that the guideline requires additional explanation regarding the underlying line of reasoning as discussed in 5.1.1. Therefore, it is decided to add explanatory notes with respect to guideline 14. Moreover, it appears that the concepts of CCM-AC and CCM-MD were not clear to all of the respondents. Therefore it is decided to clarify the concepts within the artifact. Finally, there appears to be a relation between guideline 14 and 21 since data integrity of the data being monitored is a prerequisite for following guideline 14. This relation will be made clear in the artifact.

Guideline 16

Respondent A questioned guideline 16 since the performance of the source system is not of relevance for the performance of an IT audit for assuring the reliability of the financial statements. For the same reason three of the respondents were neutral about the inclusion of the guideline as part of the artifact. Based on this argument indeed the guideline could be discarded. However, respondent B noticed that this guideline is valid since organisations are likely to decrease the frequency of executing a business rule if this negatively affect the performance of the source system. Decreasing the monitoring frequency is of influence on the performance of an IT audit since less assurance is provided regarding the operating effectiveness of a control. It should be noticed that this line of reasoning is new and not part of the discussion in section 5.1.2. Nevertheless, it appears to of relevance to accept guideline 16 as part of the artefact. Furthermore, there appears to be a relation between guidelines 16 and 12 since a decrease in the performance of the source system due to the monitoring activity is likely to result in a decreasing monitoring frequency to limit the impact of executing the business rules on the source system.

Guideline 19

Guideline 19 is not accepted as part of the artifact by respondent E. It was argued that the IT auditor should ensure himself at least once that SAP GRC PC functions as intended. It should be noticed that this argument is not incompatible with the guideline since the guideline appeals to the professional judgement of the IT auditor. Since the guideline in its current form leaves room for the argument of respondent E and the other respondents all accept the guideline, it is decided to accept the guideline as part of the artifact. Moreover, guidelines 19 and 22 turned out to be interrelated. If the programmed logic of SAP GRC PC itself contained errors, a correctly formulated business rule might still perform the wrong analyses. Therefor guideline 19 has to be taken into account prior to considering guideline 22.

Guideline 20

With respect to guidelines 20 and 25, it appears to be unclear what is meant with a monitoring rationale. This is not surprisingly since a monitoring rationale is currently not used for the performance of an IT audit and is new in the audit of SAP GRC PC. Consequently it should a monitoring rationale should be clarified within the artifact. Moreover, for the same reason not to accept guideline 19, respondent E discarded guideline 20 as well. However, this seems not to be a legitimate argument since this guideline intends to compare the technical implementation of the guideline with a monitoring rationale rather than assessing the technical implementation itself. It is believed that the unclearness of a “monitoring rationale” resulted in discarding the guideline. For now it is decided to accept the guideline 20.

Guideline 21

According to the comments regarding guideline 21, it is concluded that it is not clear that the targeted data actually is the data that resides in the source system. Consequently guideline 21 will be reformulated accordingly. Moreover, this notion is reason to clarify what is meant with source system and target system to prevent any misunderstandings.

Guideline 22

Respondents C and E argued that “correctness” of a business rule as stated in guideline 22 should be made explicit. Since assessing a business is a new activity in the performance of an audit, it

should be expected that not every IT auditor is familiar with the correctness of a business rule. Consequently, the it will be clarified what is meant with correctness within the artifact.

Guideline 24

Respondent B questioned whether guideline 24 is a prerequisite for formulating business rules or that it is merely a prerequisite for using SAP GRC PC. Here an interpretation error has occurred. After all, guideline 24 was constructed according to a notion made by respondent B himself. Because the adequacy of the control framework as a prerequisite for implementing SAP GRC PC is already implicitly stated within guidelines 8 and 10, it is decided to remove guideline 24 from the artifact.

Guideline 26

With respect to guideline 26, respondents B and E called into question whether re-performance indeed is cost ineffective and time consuming. Moreover, respondent C questioned whether time consuming and cost effectiveness should play a role in determining the audit technique. Based on these responses it is decided to discard the time-consuming and cost-effectiveness part of the guideline. However, the guideline itself will be accepted since re-performing still seems to be a valid audit technique for assessing business rules. It will be up to the professional judgement of the IT auditor whether or not to make use of re-performance in a particular situation.

Guideline 27

Guideline 27 was called into question because extensive knowledge regarding the source system should be included in the guideline. This seems to be a legitimate argument because understanding the underlying data structures typical for the source system is a pre-requisite to assess the correctness of a business rule. Therefore it is decided to include knowledge regarding the source system within the guideline.

Guideline 28

Three of the respondents did not accept guideline 28. All three of them explicitly stated that an IT auditor who lacks extensive knowledge regarding SAP GRC PC should not perform an audit of SAP GRC PC. It is decided to exclude guideline 28 from the artifact.

Guideline 29

Respondent A accepted guideline 29, but remarked that it might not always be the case that the controls as established within an organisation correspond exactly to the controls described within the best practice rule set. Consequently, it is decided to make this pre-condition part of the guideline.

Guidelines 30 – 32

Respondent B noticed that guideline 30 corresponds to testing the ITGCs of the target system (i.e. SAP GRC PC). This should be made explicit in the artefact since testing ITGCs is important for performing an IT audit. Moreover respondent C noticed that guideline 31 and 32 should be covered by means of a backup and recovery procedure and business continuity management (BCM). In addition, respondent C stated that an incident management process should solve issues in a timely manner. In fact, back-up and recovery, and incident management are ensured by testing ITGCs as well. Taking into account the notion of respondents B and C, it will be made clear within the artifact, that guidelines 30 – 32 correspond with testing the ITGCs of the target system.

Restructuring the management of SAP GRC PC

According to the discussion regarding guidelines 30 – 32, It is decided to restructure the artifact. Besides that it will be made clear what guidelines are related to testing ITGCs, the guidelines regarding the ITGCs of SAP GRC PC will be transferred to the set of guidelines regarding the “target system” area. This equates to abolish the “management of SAP GRC PC” area and transfer the associated guidelines to the “target system” area. Moreover, it will be made clear what guidelines regarding the source system refer to the testing of ITGCs as well.

A new guideline

Respondent B argued that in the artefact only changes made to the source system that affects the design of the business rules are covered as stated by guideline 23. This is a necessary guideline but entails only half the story; changes made to the risk and control framework should be taken into account as well. This indeed seems to be a legitimate argument and therefore it is decided to include a guideline taking into account changes made to the risk and control framework as well.

Evaluating the guidelines regarding communication

Table 26 - Evaluation results regarding the guidelines related to the communication

Aspect	Guideline	Resp. A	Resp. B	Resp. C	Resp. D	Resp. E
Organisational embedding	33	–	–	+	+	–
	34	+	+	?	+	?
	35	+	+	?	+	?
	36	+	+	+	+	+
	37	+	+	+	+	+
	38	+	+	+	+	+
	39	+	+	+	+	+
External reporting	40	+	+	0	+	+
	41	+	+	+	+	+
	42	+	+	–	+	0

* "+" indicates that the respondent accept the aspect as part of the artifact

** "0" indicates that the respondent is neutral regarding the aspect as part of the artifact

*** "–" indicates that the respondent deny the aspect as part of the artifact

**** "?" indicates that aspect is not clear to the respondent

***** A marked row indicates that there is a respondent who denies the aspect

Guidelines 33

Three of the respondents did not accept guideline 33 as part of the artifact. Their main argument was that assessing the communication between in the internal stakeholders is not directly of relevance for the performance of an IT audit from the perspective of the auditor. The IT auditor wants to ensure that the impact of a risk is properly mitigated to assure the reliability of financial statements. The way a risk is mitigated is of relevance from a business perspective but not directly from an IT audit perspective. Consequently, it is decided to reformulate the guideline in a way that the emphasize is on the communication towards the external IT auditor. After all, the monitoring results remain of interest for the IT auditor to assess the operating effectiveness of controls.

Guidelines 34

For two of the respondents it turned out to be unclear what was meant with process improvement. This will be clarified within the artifact.

Guidelines 35

For two of the respondents it turned out to be unclear what was meant with system improvement. This will be clarified within the artifact.

Guidelines 41 – 42

Respondent B suggested to transfer the guidelines regarding evidence to the business rules guidelines. Considering this notion, is was decided to leave the guidelines in their current position. Transferring the guidelines to the business rules might suggest that only evidence regarding business rules is of relevance while other evidence such as evidence regarding risks and controls is of relevance as well.

Guidelines 42

As can be derived from Table 26, one of the respondents did not accept this guideline as part of the artefact. The reason for discarding the guideline was that all evidence used to formulate conclusions

should be included. This is implicitly included in the guideline by stating “but is not limited to”. Because the majority of the respondents accept the guideline in its current form, it is decided to leave the guideline unaltered part of the artifact.