

Trust Is Good, Control Is Cheaper: Introduction

The necessity of overcoming risks and establishing an internal control system (ICS) is at the very top of the agenda for top management in organizations and has brought audit and consultancy companies good business for many years.

Can the implementation of legal requirements have a deeper meaning and benefit beyond simply complying with legislation? Of course it can – if you do it correctly. Experience from practice shows the following:

Why compliance?

- One aspect that is often neglected is the fact that due to its traditional orientation on compliance, an ICS can also include the monitoring of business processes with regard to efficiency, profitability, and performance. Therefore, an ICS is not just about legislation.
- Even if the compliance is only in the sense of legislative compliance, this is generally more cost-effective as non-compliance can be expensive (as shown, for example, by the bribery scandal at SIEMENS in 2006, which was covered extensively in the press).
- As a set of rules issued by the state in the exercise of its regulatory role, compliance protects the general public from many evils. You may remember the spectacular bankruptcies of ENRON, FLOWTEX, etc. Amongst other things, they were caused by manipulation of external financial reporting.
- Various compliance initiatives require that complex processes in an organization are described cleanly (often for the first time). It is easier to control transparent processes, and the controls identified also benefit business operation.
- An inefficient compliance management process uses up a lot of resources. Automating this process can ease the workload for the organization's management considerably.
- And last but not least: compliance can have direct financial advantages, such as lower capital lockup as a result of more precise or risk-specific equity definition, or cheaper credit due to an improved rating by rating agencies.

Thus, there are numerous reasons for considering compliance requirements as something other than just a necessary evil. However, efficient implementation of these requirements and setting up an effective ICS were, and still are, not easy:

Why is compliance a challenge?

- The complex ERP environment requires specific know-how, and in the case of IT-supported business processes, it is not always clear what risks they bear and what control mechanisms are in place.
- Neglecting compliance requirements during the implementation of an SAP system can have serious consequences. Hindsight is always a great thing – but not considering compliance requirements when implementing SAP generally makes you poorer. Implementing SAP is a costly undertaking and a subsequent redesign is time-consuming and expensive.
- Controls must be lived: it is not the controls that are correctly documented and tested that are effective, but those that are actually executed. However, without a check, compliance is unimaginable – but the automation that is often missing

in practice causes a great deal of administrative effort. Microsoft Excel sheets, e-mails, and manual system evaluations often dominate the audit and ICS world, and real-time reporting is frequently not possible.

- The automation of an ICS could provide answers to many of the questions that currently occupy the world of compliance:
 - How can you bring operative and audit-specific views of control mechanisms together?
 - Is real-time reporting of the status of compliance available at the push of a button?
 - How can you map the ICS so that the different requirements of risk management, internal audit, external financial statement audit, and industry-specific control are fulfilled efficiently?

How to do it
correctly

In order to implement an ICS correctly, you have to bring together many parts of the puzzle:

- Internal ICS and compliance objectives with regard to efficiency, profitability, and performance
- Legal requirements and their effect on today's world of ERP-supported processes
- "Translation" of the compliance requirements into the language of a respective ERP system – for example, SAP ERP
- Design and structure of an ICS model in the IT environment
- Automation of an ICS compliance process
- Automation of test and monitoring scenarios through integration
- Handling of internal and external audit as well as risk management integration.

The highly topical and exciting overview and the vision of the automated ICS and compliance processes in the SAP ERP environment of a well-managed organization, in which the individual pieces of the puzzle come together, motivated me to write this book.

Subject, Structure, and Content of the Book

Ever-increasing
requirements

The big wave of legislation-driven ICS projects was triggered by the Sarbanes-Oxley Act in 2002. It also affected all European companies listed on the US stock exchange. Gradually, the requirements and risks etc. to be made transparent and minimized by the ICS encroached on other organizations in Europe through EU directives and other local legal initiatives. Overall, the worldwide trend, regardless of whether we consider the impending introduction of China SOX or developments in other emerging markets, shows that a functioning ICS, as a compliance requirement demanded by the state, is establishing itself quickly.

Compliance as part
of GRC

The topic of governance, risk, and compliance as a single concept (referred to as an integrated GRC approach) appeared on the market only recently, and the merging of GRC with the topics of strategy and performance is a very new trend. It is reflected in relevant software solutions as well as recognized reference models. Thus, it is no longer appropriate to consider compliance in isolation.

In this book, compliance is understood as the process, mapped in an ICS, that is intended to guarantee conformity with legal requirements and internal policies and objectives (in particular, efficiency and profitability). An ICS was already known before the age of the computer, but new special features have arisen with the progress of information technology: the transaction audit as an audit approach, and in particular, the consideration of the ICS and the software-specific application controls within the framework of external audit have become established as mandatory. The answer to the question of what that all means for organizations whose processes run with ERP support must be clearly structured and described.

ICS in the IT environment

The last few years have seen an increase in the number of software products on the market that allow you to design the ICS process efficiently – where applicable, in interaction with risk management. However, the basic understanding of the processes in an IT-supported compliance management process is not delivered with the software.

Compliance at the push of a button

As you have seen, there are numerous puzzle pieces around the highly topical issues of ICS and compliance. You have to bring them together to get a good overview. This book considers the connection of compliance with the other parts of GRC (corporate governance and risk management), insofar as this is required by the integration view, in order to indicate the possible synergies and to explain the integrated GRC approach. This book, however, focuses on ICS compliance itself. It looks at this topic from the view of an SAP ERP-dominated IT environment, and develops it, from a design perspective, in three stages:

Concept of this book

1. From legislation to concept
2. From concept to content
3. From concept and content to automation

Figure 1 summarizes the idea and structure of this book.

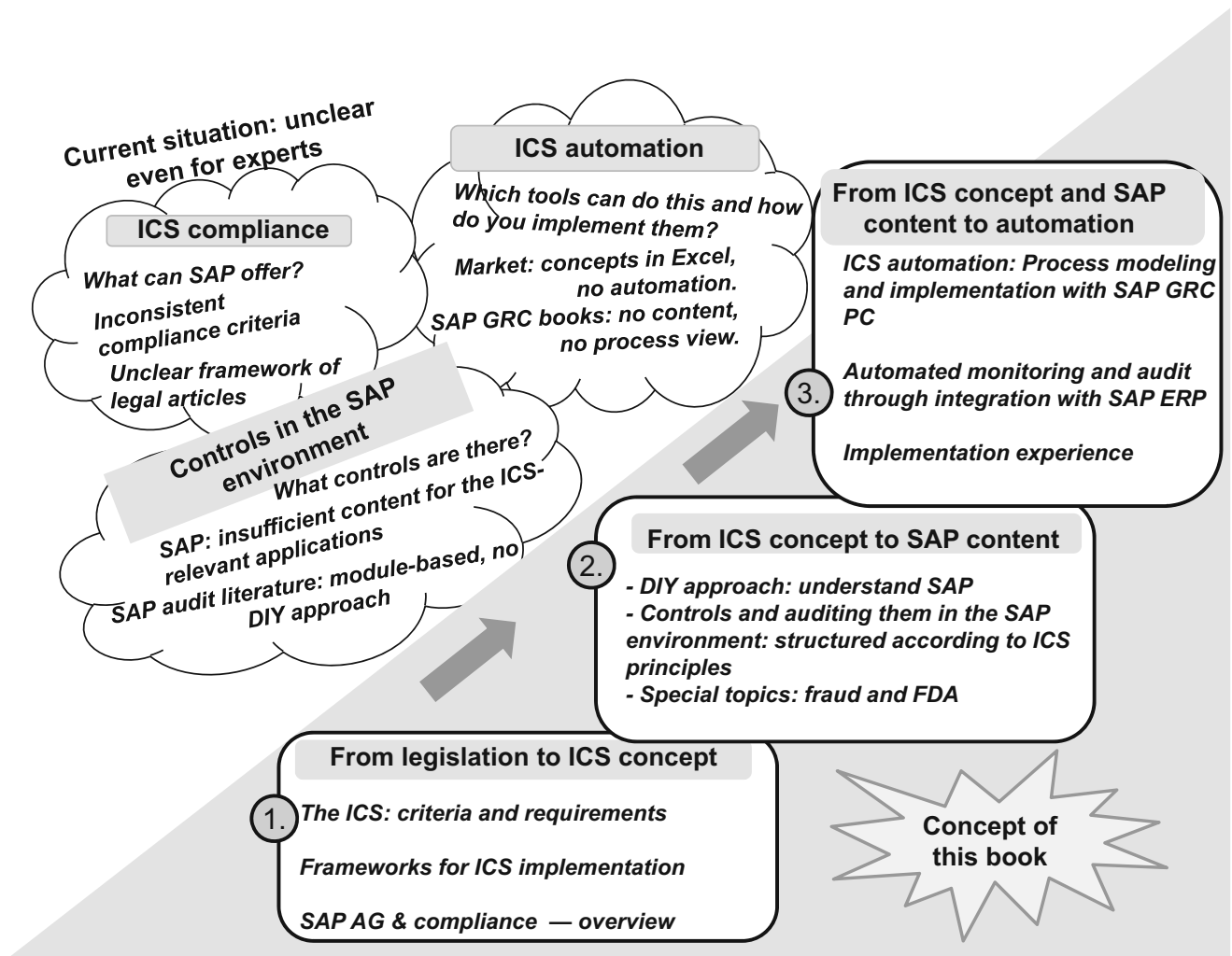
PART I – From Legislation to Concept: ICS and Compliance in the ERP Environment

ICS compliance in the SAP ERP environment – these words trigger many questions, even for experts: Which view of compliance is meant? Which legal and internal requirements are in focus? What does an integrated GRC approach based on SAP software look like? The first part of the book provides answers to these fundamental questions.

In **Chap. 1**, “Legal Requirements in ICS Compliance,” you will learn what is understood under the term ICS, and what the relevant legal compliance requirements are in an international and cross-industry comparison.

Chapter 2, “The Auditor Is Coming: When, Why, and How to Cope,” explains the special conditions that the audit in the IT environment is subject to and summarizes the most important facts and recommendations from audit practice.

In **Chap. 3**, “ICS Requirements and ERP Systems: Basic Principles, Frameworks, Structure,” we show you the basic principles for defining the content of an ICS in the SAP ERP environment and the internationally recognized studies and reference models that can help you to do this. The chapter highlights the importance of the continuous



■ **Figure 1** Concept of this book

monitoring approach. A new feature in this edition is the description of how to set up an efficiency-oriented and profitability-oriented ICS framework.

Chapter 4, “How Does SAP Deal with Risk- and Compliance-Related Topics?” summarizes the most important facts for making your compliance-relevant processes more efficient. These facts range from certification of SAP software solutions to sources of documentation for control mechanisms in SAP and an itemization of the software products. This chapter also describes the integrated GRC approach that is based on the components of the SAP solutions for GRC Release 10.0.

PART II – From Concept to Content: Audit Guide for SAP ERP

How do you translate the ICS compliance requirements into the language of SAP? What risks and controls are there in SAP ERP-supported processes? And how can you implement and monitor the efficiency of the SAP ERP-supported processes? You will find the answers to these questions in the second part of the book.

In **Chap. 5**, “Audit-Relevant SAP Basics,” we explain the basic connections in the SAP system and provide you with a tool for an independent search for control- and audit-relevant information in SAP ERP.

Chapter 6, “IT General Controls in SAP ERP,” looks at both general organizational controls and topics around change management, critical authorizations, and the basic system security.

In **Chap. 7**, “General Application Controls in SAP ERP,” you will learn how to ensure the general observance of the principles of traceability and completeness during processing in SAP ERP.

The titles of **Chap. 8**, “Controls in Financial Accounting,” **Chap. 9**, “Control Mechanisms in the SAP ERP-Supported Procure to Pay Process,” and **Chap. 10**, “Control Mechanisms in the SAP ERP-Supported Order to Cash Process” speak for themselves: these SAP-supported processes bear risks that directly endanger observance of compliance. The related control mechanisms are vital for survival and are described in the respective chapters.

In **Chap. 11**, “Data Protection Compliance in SAP ERP Human Capital Management,” you will learn which legal requirements regulate the treatment of personal data and how to implement these requirements in SAP ERP.

Chapter 12, “Fraud in an SAP System,” is dedicated to the topic of fraud. There is always a risk of fraudulent activities wherever material values and money are dealt with using SAP. In this chapter we use examples to show how you can handle this risk.

Chapter 13, “Excursion: FDA Compliance and Controls in SAP,” affects every reader of this book either directly or indirectly: the control mechanisms required by law in the pharmaceuticals and food industries, which focus primarily on the quality of the products manufactured, must be mapped in the SAP processes. We address the most important of these controls here.

Chapter 14, “Examples of Efficiency-Oriented and Profitability-Oriented Analysis Scenarios in SAP ERP,” gives detailed examples for each of the four elements of an efficiency-oriented ICS framework: process-oriented analyses, quality of master data, master data changes and user input, and supplementing reports. The aim of the high level of detail presented is to provide you with “do-it-yourself” instructions for setting up various analysis scenarios. It is also intended to give you an impression of the work involved in implementing continuous monitoring scenarios.

PART III – From Concept and Content to Implementation: Automation of an Internal Control System

Compliance at the push of a button is a realistic scenario. Software products that help you to automate an ICS are now available on the market. What is not widely available on the market, however, is a range of ICS processes and ICS content, together with their software-based implementation, from one source. On one hand, the Big Four auditing companies, as well as various compliance consultancy agencies, offer ICS content and concepts often based on Microsoft Excel; on the other hand, the conceptual compliance view is missing in both existing literature about ICS and GRC software and from consultants from software companies. The aim of this part of the book is to give you both conceptual and technical instructions for implementing ICS and compliance management processes (based on the SAP solutions for GRC Release 10.0).

In **Chap. 15**, “ICS Automation: How to Set the COSO Cube in Motion,” we address the conceptual importance of ICS automation and explain the individual building blocks that you can use to model the automation of ICS processes. You do this in the form of an ICS implementation matrix.

In **Chap. 16**, “ICS Automation Using SAP Process Control,” we show you how to implement the compliance and ICS management process using SAP GRC Process Control. You will also learn why, and using which integration scenarios, Process Control can be seen as part of an integrated GRC concept and strategy and performance management concept.

In **Chap. 17**, “Implementation of Automated Test and Monitoring Scenarios in the SAP ERP Environment,” we explain which options – including the integration of SAP Process Control with your SAP ERP systems – make the great vision of a “test at the push of a button” possible. We will take you step-by-step through the setup of the continuous monitoring approach in SAP GRC Process Control 10.0.

Chapter 18, “Experiences from Practice and Projects,” presents numerous project experiences that show how organizations from various industries have automated their compliance processes. The chapter summarizes the most important facts about project setup for implementing SAP GRC Process Control and gives some examples of implementation projects at SAP customers.

Target Audience for this Book

As a reader, what existing knowledge do you have? Although only healthy common sense and some basic business knowledge is required for Part I of this book, overall, and particularly for the remaining parts, SAP ERP experience would be an advantage. A compliance and ICS consultancy background is ideal for this book.

Who is the target audience for this book?

- **ICS owners, internal audit employees, external auditors, IT auditors, compliance experts**

This is the book for you – from the first to the last chapter!

- **Managers of SAP competence centers, project managers, data governance experts, business analysts, and consultants for SAP ERP implementations**

It is not easy to consider the compliance requirements when implementing SAP ERP. Therefore, Part I and Part II in particular provide you with important information for designing your implementation projects so that they are audit-compliant and ICS-compliant, and for daily operation of the SAP ERP applications.

- **SAP consultants for SAP GRC Products**

Part III should be mandatory reading for you. In your implementation projects, where the focus is on the process view of the ICS, you should never lose the reference to the ICS content: therefore, Part II is also important for you. And last but not least: it is essential that you understand the complex connections between legal requirements and the implementation of these requirements in the IT environment in order to find a common compliance language with customers. Therefore, Part I would also be relevant for you.

- **MBA, business, and information management students**

Part I and Part II of this book are particularly interesting for you: Part I looks in detail at the legal requirements in an international comparison, as well as the business

design of the ICS in the IT environment. The overview of internationally recognized GRC reference models could also be interesting for you. Part III explains what the automation of an ICS means from a concept perspective.

■ Senior management

Regardless of whether you are the CFO, CEO, or CIO in your organization, or are fulfilling your duties in the executive board or audit committee, you will not have been able to escape compliance issues. Even if you do not use SAP for processes in your organization, and a correct definition of the SAP-specific content of your ICS is irrelevant for you, you will certainly have thought about designing the ICS efficiently: the experiences of other organizations in handling ICS and compliance topics as described in Part II will provide you with good points of reference. Furthermore, the legal and other compliance requirements, recommendations for dealing with the external audit, and the overview of the GRC framework concepts from Part I of this book will be of interest to you. You should also not miss out on the visionary and conceptual explanations on the topic of “compliance at the push of a button” in Part III.

Notes for Reading this Book

This book contains various orientation aids that will help you to read it.

Gray information boxes provide information that is helpful and good to know, but that stands apart somewhat from the actual explanation text. To enable you to categorize the information in the boxes immediately, we have assigned symbols to the boxes:

Information boxes

Tip Start



- The *Tips* and *Notes* identified by this symbol provide recommendations that will make your work easier. These boxes also contain information on further topics or important content that you should note.

➤ Important Start

- The *Caution* symbol draws your attention to topics or areas where you should exercise particular caution.

Example Start

[e.g.]

- *Examples*, indicated by this symbol, indicate scenarios from practice and illustrate the functions presented.

Marginal notes enable you to search the book for topics you are particularly interested in or to find parts that you have already read. The marginal notes are adjacent to the respective section that contains the corresponding information.

Marginal notes

The audit procedures that are integrated in the presentation, for example, are indicated throughout the book with the marginal note “Check:” (followed in each case by key words reflecting the content).

Acknowledgments

Now it is time to thank everyone without whose support I would not have been able to complete this book project.

The English edition of the book, which you are currently holding, would not have been possible without the highly professional translation by Tracey Duffy (TSD Translations). In addition to, in my opinion, a very successful translation, Tracey Duffy also contributed to the quality of this book with her comments regarding content and with her great attention to detail. Many thanks also to Ralf Gerstner (Springer) for his expert advice and support in this project.

During the time in which I wrote this book, in addition to my main task as managing director and consultant at Riscomp GmbH, and parallel to many exciting projects, my friends and family often had to do without me. I would firstly like to thank them for their understanding and support.

Many people gave me comments, ideas, and information on various questions: many thanks to the SAP experts Jürgen Möller, Dominik Yow-Sin-Cheung, Daniel Welzbacher, Jan Gardiner, David Ramsay, and Atul Sudhalkar – for support in tricky questions surrounding the SAP GRC suite. Heartfelt thanks also to Dr. Karol Bliznak (SAP AG) for input regarding mapping the “risk-intelligent strategic execution” approach with SAP products. I would also like to thank Jürg Kasper (Canton Zürich) for his creative input regarding the automation of test and monitoring scenarios.

Esteemed colleagues have also written contributions to this book: with his highly competent and proven in practice description of the control mechanisms in the SAP ERP-supported Procure to Pay and Order to Cash processes, Gerhard Wasnick relieved me of a great deal of work. Günther Emmenegger (SAP Schweiz AG) wrote the chapter on mapping FDA-requirements in the SAP environment. Volker Lehnert wrote the majority of the chapter on data-protection relevant controls in SAP ERP HCM. Marc Michely (PricewaterhouseCoopers) contributed the section on fraud scenarios in SAP. The practical reports on mapping compliance requirements arose in close cooperation with Jan Laurisjen (Ericsson) and Michele Poffo (Tecan). Reto Bachmann provided input for the contribution on efficiency-oriented scenarios. Andreas Wiegenstein (Virtualforge) has contributed to the Sect. 6.4.2 describing key elements of the ABAP code security.

For various support, information, and help, I would also like to thank Dr. Michael Adam (SAP AG), Dr. Gero Mäder, Thomas Schmale (SAP AG), Evelyn Salie (SAP Schweiz AG), Arnold Babel (SAP Schweiz AG), Peter Heidkamp (KPMG), Florian Köller (SAP AG), Walter Harrer (SAP Schweiz AG), and Christian Brunner (SAP Schweiz AG).

Two, three, or four heads are better than one: Annett Nowatzki (DSJ Revision und Treuhand AG) and Patricia Sprenger at Galileo Press read first drafts, preliminary versions, and raw versions, as well as the finished text of the German edition of the book and improved it with their comments.

Despite the support that I have received from many quarters, I alone am responsible for any errors that remain.

I hope that this book will help you to solve your tasks concerning compliance, audit, and ICS automation with SAP, and wish you every success and enjoyment with your reading.

Maxim Chuprunov



<http://www.springer.com/978-3-642-35301-7>

Auditing and GRC Automation in SAP

Chuprunov, M.

2013, XXXII, 525 p., Hardcover

ISBN: 978-3-642-35301-7