

## ICS Requirements and ERP Systems: Basic Principles, Frameworks, Structure

Drinking tea and waiting or burying your head in the sand — these strategies are not particularly helpful in making your organization ready for an audit. You have to actively make sure that you establish an IT-capable ICS because these days, nothing works without IT.

The law prescribes and the auditor audits. And everything revolves around the internal control system. How can you make ICS requirements formulated in general terms more specific for IT-supported business processes? Where does the ICS content in the ERP environment come from? And how can you structure profitability and efficiency objectives in an ICS framework – above and beyond what is required by legislation? This chapter is dedicated to these questions. You will learn:

- How and which ERP-specific requirements are demanded of an ICS and how these requirements can be derived from generally accepted accounting principles
- Who defines the rules for compliance in the ERP environment
- How to find and structure the correct controls in the SAP environment
- Which internationally recognized studies, standards, and reference models are available for an ICS, particularly in the ERP environment

### 3.1 Defining ICS Content in the SAP ERP Environment

---

Who determines which risks are relevant in ERP-supported business processes and which controls cover these risks? How do we translate accounting-relevant compliance requirements into the language of the IT systems? The following explanations will help you to answer the most important questions regarding ICS content in the SAP ERP environment.

#### 3.1.1 ICS Basic Principles in the ERP Environment: From GAAP to GAPCAS

---

From Chap. 1, “Legal Requirements in ICS Compliance,” you already know which legal and internal requirements an ICS has to satisfy. There are further provisions that define how the requirements are to be understood with reference to the IT of an organization.

In this area, Germany has taken a leading role: almost no other country has compliance-based regulations that demonstrate ICS basic principles in the IT environment in any comparable form.

Requirements in Germany      In addition to the statements, standards, and guidelines specified in Chap. 1, in Germany the following IT-specific requirements are relevant. They are only recommendations, but have become firmly established in practice:

- The FAMA statement (FAMA = Technical Committee for Modern Accounting Systems at the Institut der Wirtschaftsprüfer Deutschland e.V. [Institute of Public Auditors in Germany, Incorporated Association] (IDW)) from 1987
- The IDW AcP FAIT 1 statement “Principles of Proper Accounting When Using Information Technology,” which partly replaces the FAMA statement
- The IDW AcP FAIT 2 statement “Principles of Proper Accounting for Electronic Commerce”
- The IDW AcP FAIT 3 statement “Principles of Proper Accounting using Electronic Archiving Procedures”
- The Generally Accepted Principles of Computer-assisted Accounting Systems (GAPCAS) from 11/7/1995 (letter from the German Federal Finance Ministry from 11/7/1995 – IVA8 – S0316 – 52/95, Federal Tax Gazette I p. 738)

If we consider the content of the statements and GAPCAS, the following overview of requirements for correctness that an accounting-relevant IT system has to fulfill stands out.

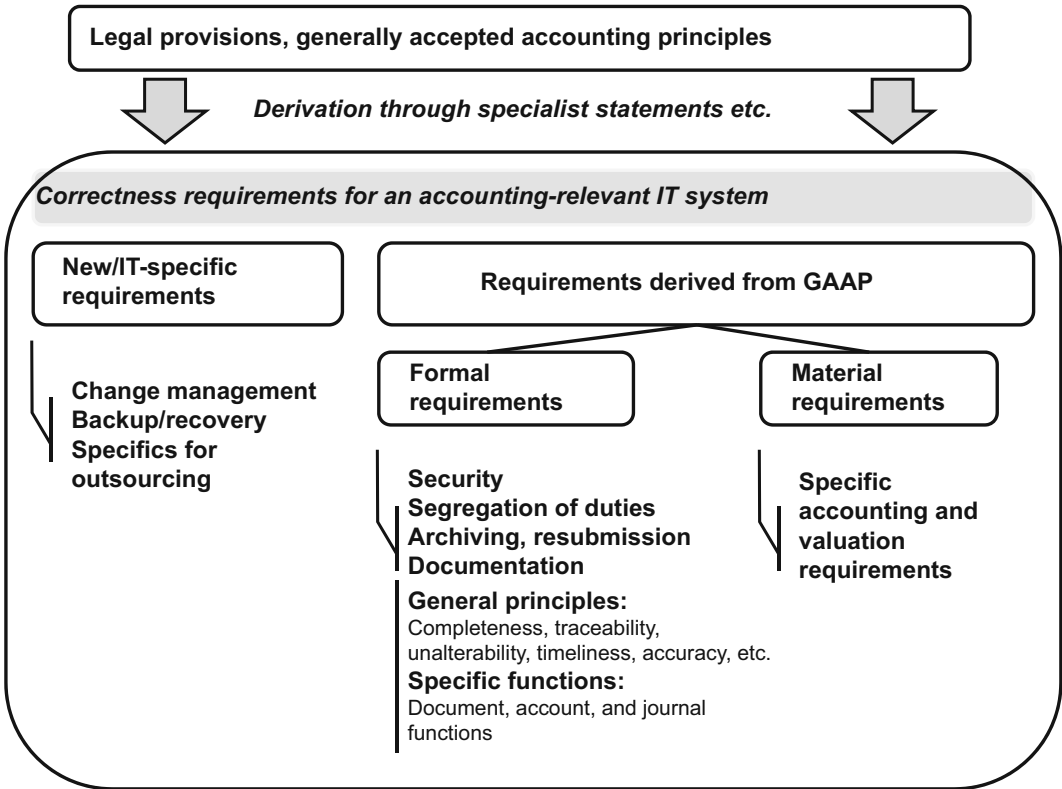
GAPCAS as basis for ICS      As you can see in Fig. 3.1, most requirements for correctness are derived directly from *Generally Accepted Accounting Principles* (GAAP). However, there are also requirements that are only relevant in an IT environment (IT-specific requirements). The fulfillment of these two groups of requirements can be seen as the primary task of control mechanisms established in (and around) IT systems relevant for accounting purposes.

Formal requirements      In Germany, most *formal* correctness requirements (for example, security, archiving, traceability, unalterability) are derived directly from Sections 238 and 239 of the German Commercial Code (HGB). Requirements such as the document function, the account function, or the journal function represent a “translation” of Sections 238 and 239 into IT language.

Material requirements      The *material correctness requirements* define the logic of the calculation, evaluation, and reporting of certain financial statement items within external reporting. The implementation of these requirements in the form of IT-supported processes requires various application controls that guarantee the fulfillment of specific audit-relevant criteria in the production of the figures.

In the professional world, these criteria have become established as *assertions* and are summarized under the abbreviation CEAVOP. The individual criteria are:

- Completeness
- Existence
- Accuracy
- Valuation
- Ownership
- Presentation



■ **Figure 3.1** Correctness criteria for an accounting-relevant IT system

### 3.1.2 Who Defines the Rules in the SAP Environment?

The formal and material GAAP-driven requirements that an ICS has to satisfy have to be “translated” into the language of an IT application that maps the accounting-relevant processes.

Unalterability of Documents in SAP ERP				[e.g.]
<p>The principle of unalterability of accounting documents can be negatively impacted if, in the SAP ERP system, authorizations that allow direct table changes are assigned for executing debugging activities. At this point, effective control mechanisms must be established, for example:</p> <ul style="list-style-type: none"> <li>— Preventive: restrictive authorization assignment</li> <li>— Preventive: emergency user concept</li> <li>— Detective: review of system log</li> </ul>				

No national application-specific provisions	In practice, who performs this “translation” task? The state as legislator and professional auditor associations have to maintain their independence as issuers of various standards and guidelines and must not influence free competition on the software provider market. For this reason, and because of the simple fact that there are numerous applications from various providers who are constantly improving or changing their products (which would make the effort required for updating documentation disproportionately high), official bodies cannot issue application-specific compliance requirements.
Organizations and auditors assume the role of translator	It is primarily organizations and companies themselves – as well as software manufacturers – who are interested in converting legal requirements into application-specific requirements. Various organizations, such as the <i>German-speaking SAP user group</i> (DSAG), represent these interests for the purposes of information exchange, networking, and the opportunity to exert influence. They publish guidelines that are helpful for implementing an ICS in the SAP environment. Amongst other things, these guidelines contain the experiences of many SAP users in dealing with <i>auditing companies</i> . As independent experts, auditors must be able to form their own opinion about the control mechanisms required in an ERP application. As the audit of legal compliance relevant to financial reporting is one of the primary tasks of the auditing companies, these companies predominate when it comes to defining application-specific ICS rules.

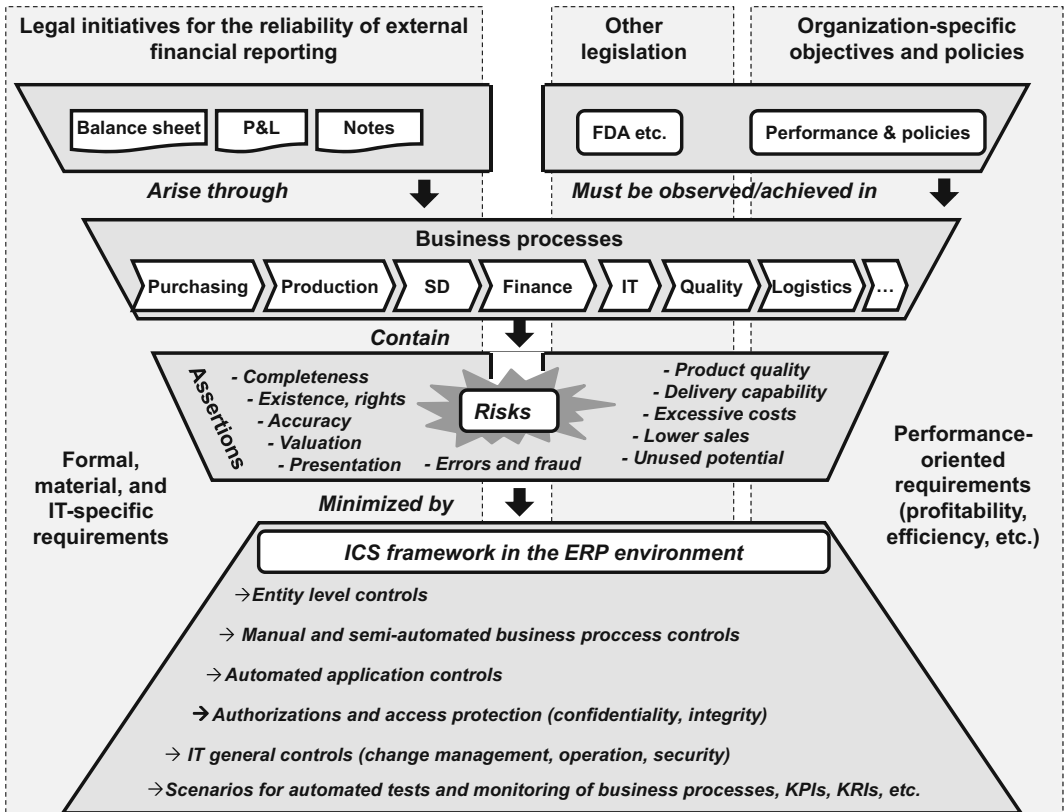
3.1.3 Control Identification Process

	An ICS is used to address compliance as well as effectiveness and profitability. Section 3.1.1, “ICS Basic Principles in the ERP Environment: From GAAP to GAPCAS,” describes the structure of financial reporting-driven compliance requirements in the IT environment. But how do we get from requirements or a conceptual ICS framework to the ICS content? This process for designing the ICS is presented below (see Fig. 3.2).
Finding risks	We also use the controls to minimize the relevant <i>risks</i> . This means that we first have to identify relevant risks. Figure 3.2 shows a simplified illustration of the three compliance areas as separate <i>ICS domains</i> . The domains are: financially-driven 1, industry-specific (for example, FDA) 2, and organization-specific 3. Even though in the example in Fig. 3.2 three domains are relevant (assuming the organization concerned manufactures medicinal products), the domains all refer to <i>business processes</i> . The question is how to find the relevant risks in these business processes. The decisive factor is the application of ICS domain-specific criteria to the relevant processes.

Domain 1: External Financial Reporting

The main criteria here are the *assertions* referred to in Sect. 3.1.1, “ICS Basic Principles in the ERP Environment: From GAAP to GAPCAS.”

[e.g.]	Main Criteria in Domain 1		
If we look at the SAP-supported sales process, in the subprocess billing, for example, we would recognize the following causal chain in the determination of controls:			



■ **Figure 3.2** Process for identifying controls in an organization

- **Process step:** Billing (invoicing)
- **Criteria:** Completeness and valuation of receivables and sales revenue
- **Risk:** Some documents with incorrect status get “stuck” in the interface between the SAP components SD and FI
- **Control:** Contents of the SAP table VBRK are regularly monitored for incorrect billing documents

## Domain 2: Requirements of Medicinal Products Manufacturers

You will learn about the main criteria for this domain in more detail in Chap. 13, “Excursion: FDA Compliance and Controls in SAP.”

[e.g.]	Main Criteria in Domain 2		
	Let us take the example of the recording of a purchase order for raw materials: <ul style="list-style-type: none"><li>■ <i>Process step</i>: Recording of a purchase order</li><li>■ <i>Criteria</i>: The appropriate quality of the raw materials procured</li><li>■ <i>Risk</i>: Health of the consumer</li><li>■ <i>Control</i>: Only qualified suppliers are used</li></ul>		

Domain 3: Organization-Specific Objectives

The objectives of an organization are very diverse. For the sake of simplicity, here we group them in one ICS domain.

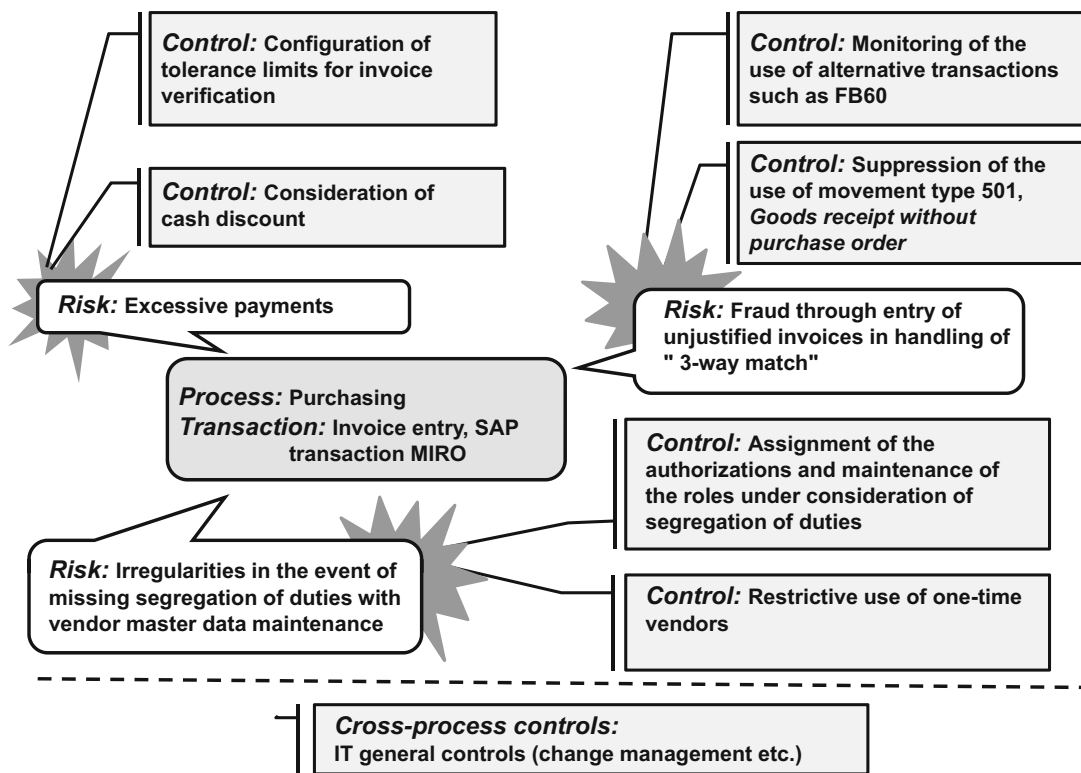
[e.g.]	Main Criteria in Domain 3		
	Let us assume the organization is very environmentally-aware, and as part of its own sustainability requirements, monitors the CO <sub>2</sub> emissions per employee: <ul style="list-style-type: none"><li>■ <i>Process step</i>: Monitoring of CO<sub>2</sub> emissions per USD 1 million sales</li><li>■ <i>Criteria</i>: Threshold value of a maximum of X tons per million USD</li><li>■ <i>Risk</i>: Environmental damage and increased expense for emissions certificates</li><li>■ <i>Control</i>: An automated control based on the interaction of SAP solutions (for example, the SAP products Sustainability Performance Management and Process Control). Information from all relevant IT systems comes together, including the systems for production and entry of travel expense data: if the threshold value exceeds a predefined limit, the control owners are informed automatically via workflow – using special dashboards, they can analyze the causes (proportion of flights and company cars for business trips)</li></ul>		

ICS framework      *ICS framework* is the term used for the set of derived control mechanisms as a whole. It is obvious that some controls can be relevant for more than one ICS domain simultaneously. The three ICS domains shown in Fig. 3.2 unfortunately often only form a single, standardized framework in theory; in practice, the ICS domains are primarily considered as self-contained silos.

For example, the control identified for domain 1 is also relevant for domain 3, as achieving higher sales is one of the fundamental interests of a company or organization. In the second part of this book, we will address the possibility of organizing individual ICS domains efficiently when automating the ICS in order to avoid the costly silo principle.

3.1.4 Structure of a Classic ICS Framework in the ERP Environment

What is the typical structure for an ICS framework in the ERP environment? To understand this structure, let us begin with a concrete example in SAP ERP. In the following explanation, we will focus on the “classic” consideration – compliance in the sense of



■ **Figure 3.3** Risks involved in invoice entry in SAP

legal compliance, thus, primarily the accuracy of the external financial reporting (see Sect. 1.1.1, "Compliance").

Let us take the SAP ERP-supported purchasing process (Procure to Pay) as an example. One of the process steps is invoice verification and entry. In SAP ERP, one of the ways to do this is using transaction MIRO. What risks does this transaction present and which controls are required? Figure 3.3 shows this example in a complete overview. The individual risks are as follows:

- Excessive payments  
This risk covers both compliance and profitability aspects: on one hand, excessive payments mean a direct loss and therefore economic damage, but no "violation" in the sense of compliance. On the other hand, the excessive payments affect the accuracy of the liabilities and therefore also affect compliance.
- Fraudulent activities through the bypassing of 3-way match controls
- Fraudulent activities due to missing segregation of duties between master data maintenance and posting authorizations
- General reliability, accuracy, and completeness of the relevant ERP processes

Example:  
purchasing process

Let us begin by looking at the "foundation" that in Fig. 3.3 consists of the IT general controls and the general application controls. Foundation

## IT General Controls

In order to be able to rely on the accuracy of the processing logic for transaction MIRO, you have to ensure that the underlying IT controls are effective. For example, changes in the system (modifications, developments, configuration changes) must be documented, agreed, tested, free of errors, and released before they can be adopted in the live environment of an SAP ERP application. You also have to ensure that the general security standards (application and network security, password protection, general settings that affect the treatment of SAP authorization roles) are observed. Every organization has its own special features. In practice, however, and under the influence of recognized ICS studies such as CobiT, a group of control mechanisms known as *IT General Controls* has become established.

- IT general controls:  
structure
- The usual structure of IT general controls is as follows:
  - Logical access to infrastructure, applications, and data
  - Controls related to the system development life cycle
  - Change management controls
  - Physical security of computer centers
  - Backup and recovery for systems and data
  - Controls related to system operation (SLAs, basis support, etc.)

## General Application Controls

In practice, it is not usual to consider the general application controls for covering some *formal requirements* separately, such as traceability, journal function, and account function, etc., unless the situation in question relates to a software certification. However, we do recommend this form of structure. With reference to transaction MIRO, for example, the general application controls would be part of the document number assignment that is supposed to satisfy the requirements for traceability.

These are controls for ensuring the following general basic principles:

- Traceability
- Unalterability
- Timeliness
- Document function

## Process Controls

- Based on business  
processes
- Now let us look at the *process controls*: as the name suggests, their structure is based on the structure of the business processes in the respective organization. The process of entering incoming invoices bears risks such as incorrect consideration of cash discount, excessive payments, but also fraud risks. As you can see in Fig. 3.3, if there is no segregation of duties, for example, between the authorization for transaction MIRO and maintenance of the vendor master data, and there are no alternative controls that could compensate for the segregation of duties deficiency, there is a risk of intentional fraudulent activities (such as payment to someone's personal account).

- Authorization roles  
according to  
segregation of  
duties
- You can prevent this risk by designing and assigning SAP authorization roles compliant with segregation of duties. In practice, there are differing opinions about the assignment of segregation of duties in the ICS framework: often, segregation of duties is considered as belonging to the corresponding controls, such as IT general controls, because the topic of authorizations sounds very “technical.” However, from the view of handling controls and as part of compliance management, as well as from a method-

ological perspective (for example, according to the CobiT study, see Sect. 3.2.2), segregation of duties is part of process controls.

Further process controls are:

Further process  
controls

#### ■ **Application controls**

Configurative settings for the tolerance limits for invoice verification ensure that, for example, an invoice is automatically blocked if the invoice amount exceeds the purchase order amount by a specific threshold value. If the use of *movement type 501* (see Sect. 9.2.1, “Goods Receipts: Critical Movement Types”) has been suppressed (for example, by the deletion of the accounts in account determination), no goods receipts can be entered without a purchase order reference.

#### ■ **Semi-automated controls**

The consideration of cash discount is a typical example of this type of control because it can require manual steps. Another example is the calculation of taxes during invoice entry: depending on the configuration in SAP ERP, a tax key can “force” the correct amount; alternatively, the correct amount can be entered manually as a deviation to the default value.

#### ■ **Automated monitoring**

These controls include steps that assume an auxiliary function and are not a direct part of the business processes; they are various evaluation options. For the MIRO-supported process of invoice verification presented, they are the following, for example:

- Reports for monitoring invoices with a suspicion of duplicate entry (based on the same reference number, amount, and due date)
- Reports for monitoring the other transactions (there are other transactions in addition to MIRO for entering an invoice without reference to a purchase order)

#### ■ **Manual controls**

The observance of administrative regulations concerning one-time vendors or manual scanning and filing of original invoices can be classified as a manual control.

Thus we can note the following composition of process controls in SAP ERP.

Process Controls			
Control mechanisms in business processes:			
■ Segregation of duties using authorizations			
■ Application controls (logic, configuration, master data)			
■ Semi-automated controls with a manual aspect			
■ Automated monitoring			
■ Manual controls			



The structure of the processes is specific for each organization and, by definition, based on the organization’s business processes. Where applicable, IT components are used. The following is a typical example of a division of processes in an industrial organization:

Division of  
processes

**Table 3.1** Structure of an ICS framework for ensuring the reliability of external financial reporting

Control area	Control contents	SAP ERP reference
IT general controls	Logical access to infrastructure, applications, and data	Direct
	Controls related to the system development life cycle	Indirect
	Change management controls	Direct
	Physical security of computer centers	Indirect
	Backup and recovery for systems and data	Indirect
	Controls related to system operation	Direct
General application controls	Controls for ensuring the traceability, unalterability, and completeness of processing	Direct
Process controls	Segregation of duties using authorizations	Direct
	Application controls (logic, configuration, master data)	Direct
	Automated monitoring	Direct
	Semi-automated controls with a manual aspect	Direct
	Manual or organizational controls	Indirect
Entity level controls	General controls outside a direct value-added chain	None

Financial accounting processes

Divided into accounts payable, accounts receivable, asset accounting, general ledger, period-end closing, and, where applicable, consolidation and consolidated financial statements

Procure to Pay (P2P)

Determination of requirements, ordering, vendor selection, invoice verification, payments, bank-related accounting, etc.

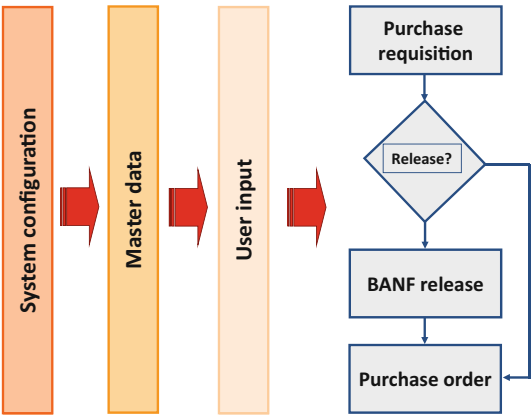
Order to Cash (O2C)

Order entry and verification, credit limit management, production, project management and valuation, warehouse management, material valuation, etc.

Entity level controls

*Entity level controls* (ELC) were named explicitly as such by *Auditing Standard No. 5* in the USA and cover that part of the ICS that is not directly part of the value-added chain. For example, these controls are the functions of the audit committee, internal audit, risk management, and the management of guidelines and regulations, etc. ELCs have no relevant reference to SAP and in this book, we consider them only marginally. Table 3.1 summarizes the structure of an ICS framework.

**Figure 3.4** Steps in a purchase order process



**3.1.5 Structure of Efficiency-Oriented and Profitability-Oriented Controls in the ERP Environment**

In Sect. 1.1.1, “Compliance,” we stated that an ICS can focus on profitability and efficiency. Whilst the control areas of IT general controls and general application controls, as described in Sect. 3.1.4, “Structure of a Classic ICS Framework in the ERP Environment,” form the standardized foundation for all ICS reference models, the main difference in the various ICS reference models lies in the contents of the process controls.

The objective of efficiency-oriented and profitability-oriented controls in the sense of this book is to address, at the deepest process or transaction level, risks that could endanger the economic success of an organization. In this book, we address primarily IT-supported or ERP-supported transactions. This means that the control mechanisms are data evaluations. The basic concept is to use the data present in an IT or ERP system to detect undesired changes in order to be able to introduce corrective measures.

Figure 3.4 shows a schematic illustration of a purchase order process.

Let us assume that the purchase order process is mapped in an ERP system. Which evaluations would help you to determine the optimization potential in this process?

Ensuring economic success

Useful analyses

**1. Analyses aimed at process efficiency**

Time is money – this applies for example to manufacturing process as well: in order to satisfy customer wishes on time and deliver specific goods, these goods must first be manufactured or procured. Procurement definitely takes place – regardless of whether it is manufacturing materials or finished goods that are procured. In our case, the delay between a purchase requisition, its potential release, and conversion into a purchase order would have a negative effect on the purchasing process. In order to determine the improvement potential here, you have to perform date-related mass evaluations of individual purchase order transactions. Section 14.1, “Process-Related Data Analyses,” contains further examples of analyses aimed at process efficiency.

**2. Quality of master data**

To avoid processes stalling, the quality of the master data must be correct. If, for example, certain fields in the vendor, customer, material, or other master data are

missing, incorrect, or inconsistent, in some circumstances in our example this can lead to the inability to enter a purchase order; in that case, you would have to create or correct certain data in an ERP system manually. Section 14.2 contains further examples of analyses concerning master data quality.

### 3. Manual data changes, user entries

Under some circumstances, uncontrolled data changes in a process (purchase requisitions, purchasing documents) can be the cause of process inefficiencies and also indicate poor data quality. Note that for some types of data, it is absolutely normal or part of daily operation that this data is changed. In any case, a mass analysis of the manual interventions, for example, in the purchase order process, can help to clarify the causes and, where applicable, introduce measures for reducing such interventions. Section 14.3, “Manual Data Changes,” contains examples for analyses in SAP that focus on manual data changes.

### 4. Enhancing reports

Standard reports available in an ERP system for monitoring specific processes (for example, in purchasing) are insufficient in some cases to cover the information requirements. In such cases, the results from data analyses whose results lists, for example, contain fields that standard reports do not have, can be used complementary to the standard reports. Section 14.4, “Supplementing SAP ERP Standard Reports,” contains further SAP-specific examples on the topic of reports.

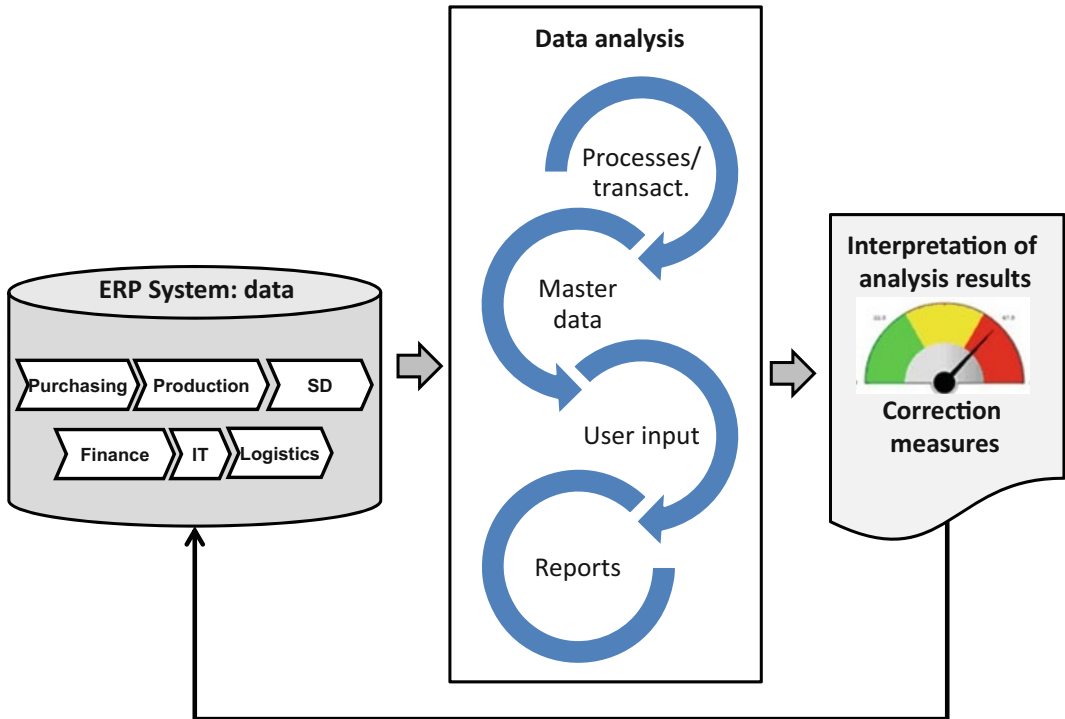
Figure 3.5 shows a simplified illustration of the process described that can help to increase the profitability and efficiency of the business processes.

Detective  
orientation

Finally, let us highlight a special feature of the efficiency-oriented and profitability-oriented approach in an ICS: whilst the “classic” compliance-oriented view differentiates between preventive and detective controls (primarily to reduce the audit effort by enabling reliance on preventive controls), in data analyses, mainly detective scenarios are used. Why is this so?

This is due to the nature of ERP systems: it is often extremely difficult or even impossible to design preventive controls in IT-supported processes so that they are watertight without simultaneously paying attention to IT general controls (particularly in change management) or general application controls (see Sect. 3.1.4). Preventive controls are based on the logic in the code or configuration settings. The controls can be performed on a key date, but do not provide information about whether the control has been active permanently or perhaps can still be circumvented. In practice, for example, it is not unusual in ERP implementation projects to use transaction data to check the accuracy of the business processes configured rather than simply inspecting configuration settings.

However, the main reason for the detective orientation of efficiency-oriented and profitability-oriented analyses is in the nature of such an orientation: in the same way that, when assessing the cholesterol level of a patient, a doctor will prefer to rely on the actual blood analyses rather than the contents of the patient’s refrigerator, the individual events and transactions executed and documented in an ERP system must be examined to obtain a reliable statement about the efficiency and profitability in the business process. Thus there is less scope here for assumptions or for assessing the hypothetical potential than with a pure compliance focus in an ICS.



■ **Figure 3.5** Schematic illustration of the process for optimizing the efficiency and profitability of business processes

## 3.2 ICS-Relevant Reference Models and Standards

There are numerous theoretical approaches to designing an ICS. The range extends from in-house developments that can be purchased from the large auditing companies, to globally recognized studies and frameworks that are freely available. The frameworks or reference models are explained below: they each contain a brief overview and notes on their practical use.

### 3.2.1 COSO

The COSO cube is often the first framework you will think of when discussing GRC or ICS frameworks. The acronym COSO is derived from *Committee of Sponsoring Organizations of the Treadway Commission*. James C. Treadway Jr., who gave COSO its name, was originally a member of the US Securities and Exchange Commission (SEC) and the first Chief Executive of this authority.

COSO has published studies that are ICS-relevant (including studies on the topic of fraud). The most well-known are:

- “Internal Control – An Integrated Framework” (1992, often referred to as a COSO classic)
- The Enterprise Risk Management study (COSO ERM 2004)

ICS classic

This second study is based on the original COSO framework and focuses more on risk management – a topic closely related to the ICS topic. The study describes approaches for achieving strategic and operative objectives as well as objectives in reporting and compliance. The COSO framework has eight main elements:

- Internal control environment
- Event identification
- Risk response
- Information and communication
- Objective setting
- Risk assessment
- Control activities
- Monitoring

With regard to governance, risk, and compliance, the COSO framework focuses more on the areas of risk and compliance.

**3.2.2 CobiT**

---

ICS in the IT environment	The CobiT framework (CobiT = Control Objectives for Information and Related Technologies, <a href="http://www.isaca.org/cobit">www.isaca.org/cobit</a> ) was developed by the IT Governance Institute (ITGI, <a href="http://www.itgi.org">www.itgi.org</a> ) and the Information Systems Audit and Control Association (ISACA, <a href="http://www.isaca.org">www.isaca.org</a> ) and is freely available. To some extent, CobiT can be seen as a more concrete form of COSO for IT concerns and it offers approaches for ICS and governance in the IT area.
Control objectives	<p>The CobiT framework groups control objectives in four categories:</p> <ul style="list-style-type: none"><li>■ Plan &amp; Organize</li><li>■ Acquire &amp; Implement</li><li>■ Deliver &amp; Support</li><li>■ Monitor &amp; Evaluate</li></ul>
ITGI document	<p>Each of these categories consists of 13 processes and these processes are designed to achieve a total of more than 200 illustrative control objectives (see Table 3.2). CobiT can be seen not only as an ICS, but also as an IT governance instrument.</p> <p>The IT Governance Institute has published a helpful document – “IT Control Objectives for Sarbanes-Oxley.” This document focuses on control mechanisms that have a direct reference to financial reporting and the associated compliance requirements. Illustrative business process-specific application controls in the appendix to this document represent a good basis for defining an ICS framework.</p>

**3.2.3 ITIL**

---

IT service management in five books	The <i>Information Technology Infrastructure Library</i> (ITIL, <a href="http://www.itil-officialsite.com">www.itil-officialsite.com</a> ), published for the first time in the 1980s by the British Office of Government Commerce, cannot be referred to as an ICS framework in the classic sense. Instead, concentrating on IT governance, ITIL covers the area of governance in the GRC concept. The ITIL framework is designed for IT service management and offers procedures for identi-
-------------------------------------	--

**Table 3.2** Overview of CobIT properties (source: ISACA online conference)

Strengths	Appropriate for
Broad use and acceptance Good for industry Good for SOX compliance Can be integrated with ISO 2700*	Any organization with a large IT department Formalized processes Any company subject to SOX
Weaknesses	Other notes
Requires substantial time and effort Poor coverage for security A lot of information about “what to do” but little information on “how” to do it	ISACA provides mappings to other frameworks Can be mapped to COSO

**Table 3.3** Overview of ITIL properties (source: ISACA online conference)

Strengths	Appropriate for
Good for service-related IT topics Provides for a certification process Good for the availability aspects of IT governance ITIL “small scale implementation” version for smaller organizations	Mid-sized to large companies with large IT departments Organizations with formalized IT processes Particularly useful where availability of IT services is critical (e.g., banks, healthcare, etc.)
Weaknesses	Other notes
Not an ICS framework in the sense of this book	Five books for approx. \$1,000 Training for approx. \$10,000 Additional costs for ITIL software

fying, planning, processing, and supporting IT services for organizations. The ITIL consists of five books:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Despite this, the ITIL structure can provide good points of reference for the structure of an ICS framework as it is designed for operative objectives (see Table 3.3).

### 3.2.4 GAIT

*The Guide to the Assessment of IT Risk*, published in 2007 by the US Institute of Internal Auditors, is one of the latest frameworks to address IT audit directly. Instead of a list of IT-specific control objectives, GAIT offers a risk-based method for prioritizing these controls.

IT general controls:  
checks

■ **Table 3.4** Overview of GAIT properties (source: ISACA online conference)

Strengths	Appropriate for
Good for IT general controls IT not as a “science itself” but as a business service provider	Auditing Scoping
Weaknesses	Other notes
The IIA and ISACA approaches are sometimes different	Freely available

■ **Table 3.5** Overview of ITAF properties (source: ISACA online conference)

Strengths	Appropriate for
Conveys an understanding of the IT audit process	IT auditors and their customers
Weaknesses	Other notes
The IIA and ISACA approaches are sometimes different No input for ICS content	Freely available

The first version of GAIT was intended to support the scoping process in SOX audits. The latest edition of GAIT extends this focus by enabling the general interaction of business and IT risks. In addition to compliance aspects, GAIT addresses efficiency and effectiveness topics. GAIT is based on the belief that not all IT risks can be monitored successfully within IT and that requirements from the main business processes of an organization should play a central role. This is a great plus point for GAIT because during the SOX wave, the impression arose that IT general controls are a science in themselves and that business is driven by IT and not vice versa.

Table 3.4 shows an overview of the GAIT properties.

3.2.5 ITAF

Reference model for IT audits      As already stated, ISACA offers reference models that follow a similar objective to GAIT. These reference models are ITAF and Risk IT.

The acronym ITAF stands for *Information Technology Assurance Framework*. This reference model is aimed at users who deal with topics in the area of IT applications, systems, and infrastructure, presented simply for IT auditors. The standards, guidelines, and audit procedures that ITAF contains can be useful not only for auditors, but also for the “consumers” of the audit results or reports. In detail, ITAF does the following:

- It offers good practice models for design, implementation, and reporting as part of IT audits
- It explains IT audit-specific concepts and standard roles for people involved in an IT audit
- It describes requirements for the expertise, experience, and code of conduct of an auditor, as well as typical processes for reporting

■ **Table 3.6** Overview of Risk IT properties (source: ISACA online conference)

Strengths	Appropriate for
Link between IT and business Content and concrete examples for risk management	Risk management in the IT domain
Weaknesses	Other notes
Little input for ICS content	Link to CobiT and Val IT

### 3.2.6 Risk IT

The Risk IT reference model from ISACA deals with risks in the IT field and supplements CobiT: whilst CobiT gives examples of controls that minimize IT risks, Risk IT provides a framework concept for identifying and managing IT-related risks.

Risk IT claims to link business risks with IT risks by establishing a connection to the business objectives in all areas (including in an example list of typical risk scenarios) and viewing the management of IT risks as part of the overall risk management process in an organization. It also considers a cost/benefit ratio in risk management.

IT risks as part of  
business risks

The overall model is divided into three large domains, and each of these domains consists of three processes:

■ **Risk governance**

Development of the risk content, integration of this content in the Enterprise Risk Management process, risk-conscious decisions in business processes

■ **Risk evaluation**

Information procurement, risk analysis, maintenance of the risk profile

■ **Risk response**

Communication of risks, task plans, reaction to events

The document “Risk IT Practitioner Guide” supports the Risk IT reference model with examples of the IT-specific key risk indicators (KRI), impact criteria for business, description of links to CobiT and Val IT, etc.

Risk IT fills the gap between *generic* reference models such as COSO ERM and *detailed* (primarily security-related) IT risk management reference models.

Table 3.6 shows an overview of the Risk IT properties.

### 3.2.7 Val IT

Val IT is a reference model for the management of investments in the IT domain. It consists of several documents. The objective of this reference model is to measure and control the benefits of IT investments from the view of the main business of an organization and to support organizations in achieving an optimal value contribution from their IT investments. Val IT consists of a series of principles and processes. In Version 2.0 (available since 2008), Val IT is based to a large extent on the structure and setup of CobiT. Val IT consists of three domains, and the following three processes are assigned to each of the domains:

■ **Table 3.7** Overview of Val IT properties (source: ISACA online conference)

Strength	Appropriate for
Supplements CobiT Optimization of the value contribution from IT investments	Offers approaches for value engineering in IT
Weakness	Other notes
Provides more detailed reference models than Val IT	From a structural perspective, is oriented on CobiT Three domains, each with three processes

- Value governance
- Portfolio management
- Investment management

Relationship to CobiT      The description of the processes follows the approach in CobiT. The following are defined for each process:

- Key management practices
- Management guidelines
- RACI chart
- Goals and metrics

Val IT is intended to supplement or complete CobiT in the financial management domains in particular and to give information to those persons hoping for information on the value contribution of their IT. CobiT also contains governance elements from these domains, which means that certain overlaps are possible. However, Val IT also contains new perspectives that are missing in CobiT.

Relationship to VMM      From a content perspective, Val IT is related to a further reference model, Value Measuring Methodology (VMM). This reference model offers more detailed instructions than Val IT on the different types of added value. In particular, VMM differentiates between a tangible and measurable added value and an intangible added value. VMM also offers comparison models and examples for calculating the added value for various projects.

Table 3.7 shows an overview of the Val IT properties.

We can assume that the topic of “sustainability/success of IT investments” will continue to grow in importance. In this regard, Val IT makes a good contribution to the topic of “value management.”

3.2.8 CMMI

Five degrees of maturity in software development      *Capability Maturity Model Integration* (CMMI) is a collection of reference models for various application areas. It is primarily a model for assessing the quality (“degree of maturity model”) of the software process (development, maintenance, configuration, etc.) of organizations as well as for determining improvement measures for the process. At the end of 2003, CMMI replaced the older CM model in order to consolidate various CM models available at the time (every development discipline had a separate model)

■ **Table 3.8** Overview of CMMI properties (source: ISACA online conference)

Strengths	Appropriate for
Optimization of the processes for software development in an organization Could be used as a source for ICS content in software development processes	Improving the organization in the area of software development Certification or assessment recognized in practice
Weaknesses	Other notes
Focus on software development, but not enough detail for large software companies	Official check of the degree of maturity is offered Parallels to ITIL with regard to determination of the degree of maturity

■ **Table 3.9** Overview of MOF properties (source: ISACA online conference)

Strengths	Appropriate for
Available free of charge Logical and clear structure	Smaller companies that choose not to implement a larger framework
Weaknesses	Other notes
Not detailed enough for complex organizations Focuses on Microsoft Windows customers Does not address risk assessment	Closely related to ITIL V3 Attempts to be an IT governance framework, may have good prospects in future versions

and to create a new, standardized model. A CMMI model is a systematic representation of tested practices to support organizational improvement. At the center of CMMI are five levels between different degrees of maturity of the software development processes. For example, a CMMI model can be used for the following:

- To get an overview of the most common procedures (for example, in project planning)
- To analyze the strengths and weaknesses of an organization
- To determine improvement measures and bring them into a useful sequence

ITIL can be seen as partially related to CMMI as both models offer assessments based on degrees of maturity. However, the focus of the assessment in ITIL is on the IT infrastructure and on services. Table 3.8 shows an overview of the CMMI properties.

ITIL and CMMI

### 3.2.9 MOF

*Microsoft Operations Framework* (MOF) is a reference model from the software manufacturer Microsoft. It is not very well known in Europe, but is closely related to ITIL V3 and focuses on IT services. For the details of this model, see <http://technet.microsoft.com/en-us/library/cc506049.aspx>. From a content perspective, MOF represents an attempt to offer an integrated reference model between the areas of governance, risk, and compliance across the entire IT life cycle.

Table 3.9 shows the properties of Microsoft Operations Framework.

**Table 3.10** Overview of the properties of ISO 27k (source: ISACA online conference)

Strengths	Appropriate for
Focus on security policy Risk-based approach Strong standard with good data protection strategies	Generally for all organizations that use IT Used by IT auditors as a benchmark for security topics
Weaknesses	Other notes
Very technology-centric, requires a larger governance framework Addition of availability and integrity but these elements are part of data governance, which belongs to the security topic	Standards, not a framework Approx. \$200 for ISO 27002 and \$300 for ISO 27001 and 27002 Self-assessment and certification are possible (extra charge)

**3.2.10 ISO 27k**

Standards for security      ISO 27k (<http://webstore.ansi.org>) groups standards – therefore it is not a reference model. These standards arose in 2000 (British Standard BS 7799, subsequently ISO 17799) and were updated in 2005 and 2007. Basically, ISO 27k represents a checklist for controls in the field of information security. From a content perspective, ISO 27k is structured in three pillars:

- Confidentiality
- Availability
- Integrity

Table 3.10 shows the properties of ISO 27k.

**3.2.11 PCI-DSS**

Data security for plastic money      In connection with the scandals surrounding stolen credit card data, the PCI-DSS standard (PCI-DSS = Payment Card Industry Data Security Standard, [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) is very interesting. Just like the ISO standards, PCI-DSS is a standard and not a reference model. It has been developed to supplement other standards, providing specific details in the field of “plastic money.” From a content perspective, this standard could be projected onto another security environment that focuses on the protection of data (see Table 3.11).

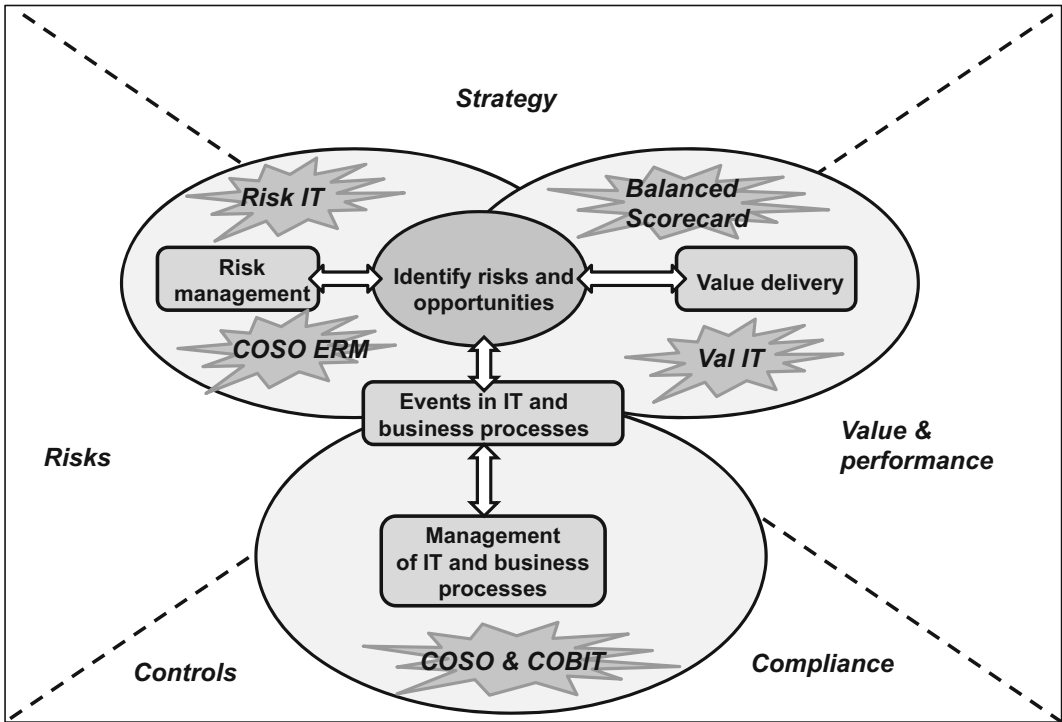
**3.2.12 Summary View of Reference Models**

Four dimensions      As you can see, existing frameworks and reference models have content orientations and objects that are settled across four main dimensions with different degrees of cover:

- Strategy
- Performance
- Risk
- Compliance

■ **Table 3.11** Overview of the properties of PCI-DSS (source: ISACA online conference)

Strengths	Appropriate for
Available free of charge Good data protection strategies Provides a self-assessment, although this is very generic	All organizations that produce, collect, store, or transfer cardholder data
Weaknesses	Other notes
Not a governance-based concept Very high-level, little specific information	Checklist approach rather than an established governance model



■ **Figure 3.6** Classification of reference models in GRC and enterprise performance topics (source: Risk IT Overview)

Figure 3.6 shows the classification of some reference models into these four dimensions.

Whilst GRC, strategy, and business performance management concepts independent of one another is nothing new, their coming together is a trend that is still quite new (see Sect. 16.6.4, “Merging GRC, Strategy, and Performance Topics”). Of the four dimensions mentioned, in which C-level management is active (C = Chief, as in CFO, CEO, CIO), two are relevant in this book: *risk* and *compliance*. Therefore, in the following chapters, we will consider COSO and CobiT as reference models, particularly for the topic of ICS content and automation in the SAP environment.

### 3.3 Summary

---

In this chapter we have created a bridge between the legal requirements of an ICS and the practical structure of an ICS in the IT environment. We have classified and described ICS basic principles in the IT environment and presented the process for identifying the ICS content schematically. We have also provided a good overview of internationally recognized studies, reference models, and standards that can provide a lot of useful information with regard to the process and content in the design of an ICS.

From this chapter you also know that for IT-supported business processes, some control mechanisms can target the efficiency and profitability of the transactions.

Chapter 4, “How Does SAP Deal with Risk- and Compliance-Related Topics?” offers further help with designing your ICS, particularly in the SAP environment.



<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