

# Contents

---

<b>List of Abbreviations</b> .....	xxix
------------------------------------	------

## **I From Legislation to Concept: ICS and Compliance in the ERP Environment**

<b>1 Legal Requirements in ICS Compliance</b> .....	3
1.1 <b>Definition of Terms and Differentiation</b> .....	3
1.1.1 Compliance .....	3
1.1.2 Internal Control System (ICS) .....	4
1.2 <b>Legal ICS Requirements Around the World – the Many Faces of SOX</b> .....	5
1.2.1 SOX in the USA .....	5
1.2.2 SOX in Canada (NI 52-109) .....	7
1.2.3 SOX in Japan .....	7
1.2.4 SOX in China .....	8
1.3 <b>ICS Requirements in Europe</b> .....	8
1.3.1 Eighth EU Directive .....	8
1.3.2 Germany .....	9
1.3.3 Switzerland .....	10
1.3.4 Austria .....	11
1.3.5 United Kingdom of Great Britain and Northern Ireland .....	11
1.3.6 France .....	12
1.3.7 Denmark .....	12
1.3.8 Italy .....	12
1.3.9 Spain .....	13
1.4 <b>ICS Requirements in the Financial Sector</b> .....	13
1.4.1 Solvency II in the Insurance Industry .....	14
1.4.2 Basel II and III in Banking .....	15
1.5 <b>ICS as Contributing Factor to Business Success?</b> .....	16
1.6 <b>Summary</b> .....	17
<b>2 The Auditor Is Coming: When, Why, and How to Cope</b> .....	19
2.1 <b>ICS in the IT Environment from the View of Auditing</b> .....	19
2.1.1 The Challenge Presented by Information Technology .....	20
2.1.2 Transaction Audit as Audit Approach in the IT Environment .....	21

2.1.3	Approaches for a Transaction Audit: Focus on ICS .....	22
2.1.4	ICS and Mandatory Transaction Audit .....	23
2.2	<b>ICS Assurance in Practice</b> .....	26
2.2.1	The Auditor's Focus .....	26
2.2.2	Selected Auditing Principles .....	27
2.2.3	Types of External Audit in the ERP Environment .....	29
2.2.4	Recommendations for Working with the Auditor .....	31
2.3	<b>Summary</b> .....	34
3	<b>ICS Requirements and ERP Systems: Basic Principles, Frameworks, Structure</b> .....	35
3.1	<b>Defining ICS Content in the SAP ERP Environment</b> .....	35
3.1.1	ICS Basic Principles in the ERP Environment: From GAAP to GAPCAS .....	35
3.1.2	Who Defines the Rules in the SAP Environment? .....	37
3.1.3	Control Identification Process .....	38
3.1.4	Structure of a Classic ICS Framework in the ERP Environment .....	40
3.1.5	Structure of Efficiency-Oriented and Profitability-Oriented Controls in the ERP Environment .....	45
3.2	<b>ICS-Relevant Reference Models and Standards</b> .....	47
3.2.1	COSO .....	47
3.2.2	CobiT .....	48
3.2.3	ITIL .....	48
3.2.4	GAIT .....	49
3.2.5	ITAF .....	50
3.2.6	Risk IT .....	51
3.2.7	Val IT .....	51
3.2.8	CMMI .....	52
3.2.9	MOF .....	53
3.2.10	ISO 27k .....	54
3.2.11	PCI-DSS .....	54
3.2.12	Summary View of Reference Models .....	54
3.3	<b>Summary</b> .....	56
4	<b>How Does SAP Deal with Risk- and Compliance-Related Topics?</b> .....	57
4.1	<b>Software Certification</b> .....	57
4.1.1	SAP Note 671016 .....	58
4.1.2	Certification Reports .....	58
4.2	<b>Compliance-Relevant Guides</b> .....	61
4.2.1	SAP Online Resources .....	61

4.2.2	Security Guides .....	63
4.2.3	DSAG Guides: Audit Guides, Data Protection Guides .....	68
4.3	<b>Integrated Approach in SAP GRC 10.0 and Further Compliance-Relevant Solutions</b> .....	68
4.3.1	SAP Governance, Risk, and Compliance Suite 10.0 .....	69
4.3.2	SAP Process Control 10.0 .....	70
4.3.3	SAP Access Control 10.0 .....	72
4.3.4	Policy Management .....	77
4.3.5	SAP Risk Management 10.0 .....	77
4.3.6	Summary Overview of Integration Scenarios in SAP GRC 10.0 .....	79
4.3.7	SAP Audit Management .....	79
4.3.8	SAP Audit Information System .....	81
4.3.9	SAP Security Optimization Service .....	82
4.3.10	RSECNOTE Tool .....	82
4.4	<b>Compliance-Relevant Content</b> .....	82
4.4.1	Direct ICS Content: What Controls Are Available in SAP? .....	83
4.4.2	Content with ICS Relevance: Standard Business Processes and Controls in SAP .....	89
4.5	<b>Summary</b> .....	92

## II From Concept to Content: Audit Guide for SAP ERP

5	<b>Audit-Relevant SAP Basics</b> .....	95
5.1	<b>In the Beginning Was the Table: SAP as Table-Controlled Application</b> .....	96
5.1.1	Data in an SAP System .....	97
5.1.2	Controls in the SAP System .....	102
5.1.3	Table-Specific Search .....	103
5.1.4	Transaction-Specific Search .....	109
5.1.5	Program-Specific Search .....	111
5.1.6	The Relationship Between Programs and Transactions .....	111
5.1.7	The Relationship Between Programs and Tables .....	113
5.1.8	Summary of the Search Options in SAP .....	116
5.1.9	Organizational Structures in the SAP System .....	117
5.2	<b>Authorizations</b> .....	118
5.2.1	Flow and Hierarchy of Authorization Controls .....	119
5.2.2	Authorization Objects .....	119
5.2.3	Determining Authorization Objects .....	122
5.2.4	Roles in the SAP System .....	125
5.2.5	Users in the SAP System .....	127
5.2.6	User Types in SAP .....	128

5.2.7	Example of an Authorization Analysis .....	129
5.3	<b>Summary</b> .....	130
6	<b>IT General Controls in SAP ERP</b> .....	131
6.1	<b>Organizational Controls</b> .....	131
6.1.1	IT Organization .....	131
6.1.2	IT Outsourcing: Who Is Responsible for the Controls? .....	132
6.1.3	Guidelines and Documentation .....	135
6.2	<b>Controls in the Area of Change Management and Development</b> .....	136
6.2.1	SAP System Landscape .....	136
6.2.2	Change and Transport Management .....	137
6.2.3	Client Control .....	140
6.2.4	Maintenance and Updates .....	142
6.2.5	SAP Solution Manager .....	143
6.3	<b>Security Controls for Access to the SAP System and for Authentication</b> .....	145
6.3.1	Identity and Life Cycle of the User .....	145
6.3.2	Password Protection .....	146
6.3.3	Handling Standard Users .....	148
6.3.4	Emergency User Concept .....	150
6.4	<b>Security and Authorization Controls within SAP ERP</b> .....	150
6.4.1	Protecting Programs and Transactions – Basic Level .....	151
6.4.2	Protecting Programs and Transactions – Advanced Level .....	154
6.4.3	Protecting Tables .....	158
6.4.4	Controlling Authorization Checks .....	159
6.4.5	Critical Administration Transactions .....	161
6.4.6	Consideration of the Principle of Segregation of Duties .....	161
6.5	<b>Summary</b> .....	163
7	<b>General Application Controls in SAP ERP</b> .....	165
7.1	<b>The Principle of Unalterability</b> .....	165
7.1.1	Protecting Data in Tables .....	166
7.1.2	Debugging .....	166
7.1.3	Modifiability of Documents .....	168
7.2	<b>Controls for Data-Related Traceability</b> .....	169
7.2.1	Change Documents in SAP .....	169
7.2.2	Table Logging .....	171
7.2.3	Document Number Assignment .....	173
7.3	<b>Traceability of User Activities in SAP</b> .....	174
7.3.1	System Log .....	174

7.3.2	Security Audit Log .....	176
7.3.3	History of Transaction Calls .....	177
7.3.4	Traceability of System Changes in the Change and Transport Management System (CTS) .....	178
7.4	<b>Cross-Process Processing Controls</b> .....	179
7.4.1	Monitoring Update Terminations .....	180
7.4.2	Completeness of the ALE Interface Processing .....	182
7.4.3	Remote Function Call Connections .....	184
7.4.4	Completeness of Batch Input Processing .....	185
7.5	<b>Summary</b> .....	187
8	<b>Controls in Financial Accounting</b> .....	189
8.1	<b>Underlying Control Mechanisms in General Ledger Accounting (FI-GL)</b> .....	189
8.1.1	Principle: Real-Time Postings .....	190
8.1.2	Financial Statements .....	192
8.1.3	G/L Account Master Data .....	193
8.1.4	Checking that Transaction Figures Are Consistent with the Accounting Reconciliation .....	195
8.1.5	Selected Controls for Closing Operations .....	195
8.1.6	Reconciliation Work in FI-GL .....	197
8.2	<b>Controls over the Accuracy and Quality of Data in General Ledger Accounting</b> .....	198
8.2.1	Accurate Account Determination .....	198
8.2.2	Field Status Groups .....	199
8.2.3	Calculating Taxes for Manual Postings .....	200
8.2.4	Validations in SAP .....	202
8.2.5	Foreign Currencies .....	203
8.3	<b>Completeness of Processing in General Ledger Accounting</b> .....	205
8.3.1	Document Parking .....	205
8.3.2	Recurring Entries .....	207
8.3.3	Reconciliation Ledger .....	208
8.4	<b>Data Security and Protection in General Ledger Accounting</b> .....	209
8.4.1	Protecting Company Codes .....	209
8.4.2	Tolerance Groups .....	212
8.4.3	Protecting Master Data .....	212
8.4.4	Critical Transactions .....	215
8.4.5	Segregation of Duties in General Ledger Accounting .....	217
8.5	<b>Controls in Asset Accounting (FI-AA)</b> .....	218
8.5.1	Basics of Asset Accounting in SAP .....	218

8.5.2	Default Values for Asset Classes .....	219
8.5.3	Account Determination in Asset Accounting .....	220
8.5.4	Consistency Check for Account Determination and Configuration .....	221
8.5.5	Depreciation .....	221
8.5.6	Asset History Sheet .....	225
8.5.7	Low Value Assets .....	226
8.5.8	Authorization Control in Asset Accounting .....	227
8.5.9	Critical Authorizations in Asset Accounting .....	228
8.6	<b>Controls in Accounts Payable (FI-AP) and Accounts Receivable (FI-AR)</b> .....	229
8.6.1	Accuracy of the Reconciliation Accounts .....	229
8.6.2	Payment Functions .....	230
8.6.3	One-Time Customers and Vendors – Caution! .....	232
8.6.4	Ageing Structure and Value Adjustments .....	234
8.6.5	Segregation of Duties for Master Data Maintenance .....	234
8.7	<b>Summary</b> .....	235
9	<b>Control Mechanisms in the SAP ERP-Supported Procure to Pay Process</b> .....	237
9.1	<b>Ordering</b> .....	238
9.1.1	Maintenance of the Organizational Structures Consistent with Authorizations .....	238
9.1.2	Segregation of Duties in Ordering .....	239
9.2	<b>Goods Receipts and Invoice Verification</b> .....	242
9.2.1	Goods Receipts: Critical Movement Types .....	242
9.2.2	3-Way Match and Payment Blocks in Logistics Invoice Verification .....	243
9.2.3	Check for Duplicate Invoice Entry .....	245
9.3	<b>GR/IR Account</b> .....	245
9.3.1	Clearing the GR/IR Account .....	245
9.3.2	Closing Operations and Reporting of the GR/IR Account in the Balance Sheet .....	247
9.4	<b>Controls for Stocks</b> .....	249
9.4.1	Maintenance of Material Master Data .....	249
9.4.2	Non-Valuated Stock Value and Split Valuation .....	250
9.4.3	Account Determination for Material Movements .....	251
9.4.4	Correction of Stock Values: Inventory and Material Devaluations .....	253
9.4.5	Release of Scrapping .....	254
9.4.6	Product Cost Accounting .....	255
9.4.7	Goods Issues from Non-Valuated Stock .....	257
9.5	<b>Corporate Governance</b> .....	257
9.6	<b>Summary</b> .....	258

10	<b>Control Mechanisms in the SAP ERP-Supported Order to Cash Process</b> .....	259
10.1	<b>Controls in the Preparatory Sales and Distribution Phase</b> .....	260
10.1.1	Controls during Order Entry .....	260
10.1.2	Quality of Customer Master Data .....	261
10.1.3	Segregation of Duties for Master Data Maintenance .....	262
10.1.4	Credit Limit Assignment and Control .....	263
10.2	<b>Controls in Order Fulfillment and Revenue Recognition</b> .....	264
10.2.1	Controls for Delivery of Goods .....	265
10.2.2	Pricing and Determination of Sales Tax .....	266
10.2.3	Return Deliveries and Credit Memos .....	269
10.2.4	Billing Due List .....	269
10.2.5	Completeness of Accounting Entry of Billing Documents .....	270
10.2.6	Dunning .....	271
10.3	<b>Summary</b> .....	274
11	<b>Data Protection Compliance in SAP ERP Human Capital Management</b> .....	275
11.1	<b>Legal Data Protection Requirements</b> .....	275
11.1.1	Data Protection .....	276
11.1.2	Basic Principles: European Union Directive .....	277
11.1.3	Co-Determination and Employee Data Protection .....	283
11.1.4	Excursion: Protection of Patient Data .....	285
11.2	<b>General Data Protection-Relevant Control Mechanisms in SAP</b> .....	286
11.2.1	Tracing Changes to Personal Data .....	287
11.2.2	Logging Report Calls in SAP ERP HCM .....	288
11.2.3	Deleting Data and Making it Unrecognizable .....	288
11.2.4	Personal Data Outside SAP ERP HCM .....	289
11.3	<b>Special Requirements of SAP ERP HCM</b> .....	290
11.4	<b>Authorizations and Roles in SAP ERP HCM</b> .....	290
11.4.1	Differentiating Attributes in SAP ERP HCM .....	291
11.4.2	Personnel Events .....	293
11.4.3	Structural Authorizations .....	296
11.4.4	Authorization Main Switches .....	299
11.5	<b>Summary</b> .....	301
12	<b>Fraud in an SAP System</b> .....	303
12.1	<b>Introduction to "Fraud"</b> .....	303
12.1.1	Types of Fraud .....	303
12.1.2	Fraud and the SAP System .....	305

12.2	<b>Fraud Scenarios in SAP Basis</b> .....	306
12.2.1	“Write-Debugging” Authorizations .....	306
12.2.2	Processing a Batch Input Session under a Different User ID .....	307
12.3	<b>Fraud Scenarios in the General Ledger</b> .....	308
12.3.1	Fraudulent Manual Document Postings in the General Ledger .....	308
12.3.2	Identification and Analysis of Manual Journal Entries .....	309
12.4	<b>Fraud Scenarios in the Sales Area</b> .....	311
12.4.1	Issuing Fictitious Invoices to Fictitious Customers .....	311
12.4.2	Granting Improper Credit Memos or Discounts .....	312
12.4.3	Excessive Use of Free Goods .....	313
12.4.4	Improper Write-Off of Open Customer Receivables .....	314
12.5	<b>Fraud Scenarios in Personnel Accounting</b> .....	315
12.5.1	Fictitious Employees .....	315
12.5.2	Limited Access to Own HR Data .....	316
12.5.3	Segregation of Duties for Confidential Data .....	316
12.6	<b>Summary</b> .....	317
13	<b>Excursion: FDA Compliance and Controls in SAP</b> .....	319
13.1	<b>Legal Requirements in the Manufacture of Food and Medicinal Products</b> ....	319
13.1.1	FDA-Relevant Legal Requirements in an International Comparison .....	320
13.1.2	GxP – The FDA Basic Principles .....	321
13.1.3	IT from the View of FDA Compliance .....	322
13.2	<b>Validation of IT Systems</b> .....	322
13.2.1	Validation Procedure .....	323
13.2.2	Controls in Implementation Processes .....	324
13.3	<b>FDA Compliance in IT-Supported Business Processes</b> .....	325
13.3.1	Examples: Controls in Procurement .....	325
13.3.2	Examples: Controls in Production Management .....	325
13.3.3	Examples: Controls in Quality Management .....	326
13.3.4	Examples: Controls in Asset Maintenance .....	326
13.3.5	Examples: Controls for Batch Traceability .....	327
13.3.6	Examples: Controls in Warehouse Management Processes .....	327
13.4	<b>Observing FDA Compliance for System Maintenance, System Updates, and System Changes</b> .....	328
13.5	<b>Summary</b> .....	329
14	<b>Examples of Efficiency-Oriented and Profitability-Oriented Analysis Scenarios in SAP ERP</b> .....	331
14.1	<b>Process-Related Data Analyses</b> .....	331



14.1.1	Comparison of the Purchase Order Date with the Goods Receipt Date .....	332
14.1.2	Timely Release or Creation of Purchase Requisitions and Purchase Orders .....	336
14.1.3	Time between Incoming Purchase Order and Confirmation of the Customer Order ..	343
14.1.4	Ten Further Examples of Possible Data-Based Process Analyses .....	344
14.2	<b>Analysis of Master Data Quality</b> .....	344
14.2.1	Quality of Customer Master Data .....	345
14.2.2	Produced Materials with No Bill of Materials .....	346
14.2.3	Reconciliation of Material Costs within a Company Code .....	347
14.2.4	Ten Further Examples of Possible Master Data Analyses .....	349
14.3	<b>Manual Data Changes</b> .....	349
14.3.1	Changes to Purchase Requisitions .....	350
14.3.2	Changes to Purchasing Documents .....	351
14.3.3	Changes to Sales Documents .....	355
14.3.4	Manual Data Changes – Ten Further Examples .....	357
14.4	<b>Supplementing SAP ERP Standard Reports</b> .....	358
14.4.1	Planning Parameters Added to Stock Analyses .....	358
14.4.2	Customer Master Data Added to Credit Management Analysis .....	359
14.5	<b>Summary</b> .....	360

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

15	<b>ICS Automation: How to Set the COSO Cube in Motion</b> .....	363
15.1	<b>Basic Concept of ICS Automation</b> .....	363
15.1.1	COSO Cube in Action .....	364
15.1.2	Concept of ICS Automation .....	365
15.2	<b>ICS-Relevant Objects and Documentation</b> .....	367
15.2.1	Organizational Units .....	367
15.2.2	Processes .....	368
15.2.3	Controls .....	369
15.2.4	Control Objectives .....	370
15.2.5	Risks .....	371
15.2.6	Account Groups .....	371
15.2.7	Example of an ICS Data Model .....	372
15.3	<b>Basic Scenarios of ICS Activities</b> .....	373
15.3.1	Documentation .....	374
15.3.2	Selection and Prioritization of Control Activities .....	374
15.3.3	Control Execution .....	375
15.3.4	Design Test .....	376

15.3.5	Effectiveness Test .....	376
15.3.6	Survey .....	377
15.3.7	Risk Assessment .....	377
15.3.8	Remediation .....	378
15.3.9	Sign-Off .....	378
15.3.10	Report Evaluation .....	379
15.3.11	Persons as Links Between ICS Objects and Activities .....	379
15.4	<b>Summary</b> .....	380
16	<b>ICS Automation Using SAP Process Control</b> .....	381
16.1	<b>Introduction: ICS Implementation with SAP Process Control</b> .....	381
16.2	<b>Technical Implementation</b> .....	383
16.2.1	Technical Architecture and Installation .....	383
16.2.2	Initial Configuration of the Standard Functions .....	385
16.2.3	Information Sources on Implementing, Operating, and Upgrading SAP Process Control .....	386
16.3	<b>Data Model</b> .....	388
16.3.1	ICS Master Data in SAP Process Control .....	388
16.3.2	ICS Data Model in SAP Process Control .....	391
16.3.3	Central vs. Local ICS Master Data .....	392
16.3.4	Time Dependency of ICS Master Data .....	393
16.3.5	Traceability of Changes .....	395
16.3.6	Concept of Object-Related Security .....	395
16.3.7	Customer-Specific Fields .....	396
16.3.8	Multiple Compliance Framework Concept .....	399
16.4	<b>Implementation of the ICS Process</b> .....	400
16.4.1	ICS Documentation Process .....	401
16.4.2	Scoping Process .....	405
16.4.3	Planning Process, Tests, and Assessments .....	409
16.4.4	Issue Remediation Process .....	416
16.4.5	Reporting .....	424
16.5	<b>ICS and Compliance Implementation: Roles</b> .....	427
16.5.1	Authorization Model in SAP Process Control .....	427
16.5.2	Object-Related Security in Action .....	428
16.5.3	First Level vs. Second Level Authorizations .....	429
16.5.4	Predefined Best Practice Role Concept in SAP .....	431
16.5.5	Adjusting the Roles .....	431
16.6	<b>SAP Process Control as GRC Component – New Features and Developments</b> ..	433
16.6.1	Policy Management and Other New Features in Release 10.0 .....	433

16.6.2	Integration with SAP Access Control .....	434
16.6.3	Integration with SAP Risk Management .....	435
16.6.4	Merging GRC, Strategy, and Performance Topics .....	437
16.7	<b>Summary</b> .....	439
17	<b>Implementation of Automated Test and Monitoring Scenarios in the SAP ERP Environment</b> .....	441
17.1	<b>Automated Test and Monitoring Scenarios in the SAP Environment</b> .....	441
17.1.1	Offline CAAT Tools .....	442
17.1.2	Online CAAT Reports and Evaluations .....	445
17.1.3	Compliance Management Software .....	446
17.2	<b>Automated Tests and Monitoring in SAP Solutions for GRC Release 10.0 – Introduction</b> .....	448
17.2.1	Continuous Monitoring Framework .....	448
17.2.2	Continuous Monitoring Framework – Potential and Expectations .....	450
17.3	<b>Setting up CMF Scenarios in SAP Process Control</b> .....	453
17.3.1	Connecting SAP Solutions for GRC with Business Applications .....	453
17.3.2	Data Sources in SAP Process Control .....	456
17.3.3	Creating Business Rules in CMF .....	460
17.3.4	Monitoring Data Changes in CMF .....	462
17.3.5	Automation Using Predefined Best Practice Scenarios .....	465
17.3.6	Connecting Controls with Rules .....	467
17.3.7	And off You Go! .....	468
17.4	<b>Potential of CMF Scenarios in SAP Process Control</b> .....	469
17.4.1	Use of SAP NetWeaver Business Warehouse for Continuous Monitoring .....	470
17.4.2	Thoughts About SAP BusinessObjects .....	471
17.5	<b>Summary</b> .....	472
18	<b>Experiences from Practice and Projects</b> .....	473
18.1	<b>Practical Experiences: Projects for ICS and Compliance Automation</b> .....	473
18.1.1	Tools for Implementation .....	473
18.1.2	Best Practice Project Structure for ICS Implementation .....	475
18.1.3	Business Blueprint .....	475
18.1.4	ICS Content .....	477
18.1.5	Factors that Influence the Project Expense .....	479
18.1.6	Success Factors .....	480
18.2	<b>Project Examples for ICS and Compliance Automation</b> .....	482
18.2.1	Coverage of Swiss Compliance Requirements at KUONI .....	482
18.2.2	Integrated GRC Approach at Tecan .....	485

18.3	<b>SOX at Ericsson</b> .....	488
18.3.1	ICS Framework at Ericsson .....	489
18.3.2	SOX Compliance Process at Ericsson .....	491
18.3.3	Experiences from Previous Projects .....	494
18.3.4	Optimization Potential .....	495
18.3.5	Steps Towards Optimization .....	495
18.4	<b>Review of the Stages of Evolution of the ICS and Conclusion</b> .....	496
	<b>References</b> .....	501
	<b>The Author of this Book</b> .....	503
	<b>Contributors to this Book</b> .....	505
	<b>Index</b> .....	509



<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