

Table of Contents

- Part 1: Foundation 1
 - 1 Subject (from pain to pleasure) 3
 - 1.1 Challenges 3
 - 1.2 Areas of activity beyond „Protection, Detection, Reaction“ 6
 - 1.2.1 Transparency 9
 - 1.2.2 Interfaces and interaction 14
 - 1.2.3 Standardization 18
 - 1.3 Solutions 21
 - 2 Environment 25
 - 2.1 Frameworks for ESARIS 26
 - 2.2 Perspectives: corporate versus product security 30
 - 3 Main building blocks and general set-up 33
 - 3.1 ESARIS Dimensions 33
 - 3.2 ESARIS Work Areas 35
 - 3.3 ESARIS Collaboration Model 37
 - 3.4 Hierarchy of Security Standards 42
 - 3.4.1 Overview 42
 - 3.4.2 Level 1: Corporate Security Policy 44
 - 3.4.3 Level 2: Corporate Security Rules 44
 - 3.4.4 Level 3: ICT Security Principles 45
 - 3.4.5 Level 4: ICT Security Standards 46
 - 3.4.6 Level 5: ICT Security Baselines 46
 - 3.5 ESARIS Concept of Double Direction Standards 47
 - 4 ESARIS Security Taxonomy 51
 - 4.1 Design criteria for the ESARIS Security Taxonomy 51
 - 4.2 Structure of the ESARIS Security Taxonomy 55
 - 4.3 Areas and the ICT Security Standards at a glance 61
 - 4.3.1 Networks 62
 - 4.3.2 Data center 63
 - 4.3.3 Customer and users 66
 - 4.3.4 Evidence and Customer Relation 67
 - 4.3.5 Service Management 69
 - 4.3.6 Risk Management and Certification 71
 - 4.4 Summary of standards and taxonomy 72
 - 4.5 Provider Scope of Control 74

5	Secured by definition – integration with core business (ITSM)	81
5.1	ITSM processes and why security must be integrated into them	81
5.2	Division of labor between IT and IT security	88
5.3	How the integration looks like and actually works	91
Part 2: Core activities		97
6	Standardization – ensuring quality and efficiency	99
6.1	Understanding standardization, its necessity and benefits	99
6.2	ESARIS Industrialization Concept	103
6.2.1	Dealing with requirements	103
6.2.2	Composition of services	105
6.3	ESARIS Security Specification Concept	106
6.4	Obstacles towards standardization and solutions	113
7	Attainment – achieving compliance with ESARIS standards	121
7.1	Foundation	121
7.2	Requirements engineering and elaboration and application of ESARIS standards	123
7.3	ESARIS Attainment Levels and verification of compliance	128
7.4	Service offering portfolio integration	134
8	Fulfillment – meeting customer demands	139
8.1	Foundation	139
8.2	IT outsourcing	142
8.3	Assurance for customers	148
8.3.1	Contractual evidence	148
8.3.2	Operational evidence	153
8.3.3	Contractual and other changes	155
9	Flexibility – managing the supplier network	159
9.1	Roles and types of suppliers	159
9.2	Third party integration model	162
Part 3: Implementation		171
10	Maintenance – requirements, documents, improvements	173
10.1	Document IDs and more	173
10.2	Virtual organization, roles and processes	179
10.3	Library, versions and consistency	182
10.4	Protecting intellectual property	186
11	Transformation – implementing ESARIS sustainably	189
11.1	Mission: induce a massive change	189
11.2	Approach: ESARIS Maturity Level and master plan	192
11.3	Enablement: training and communication	200
11.4	Voyage of ICT services	205

12 Implementation – IT production and its protection in practice209

12.1 Evidence and Customer Relation 209

12.1.1 Match – (Im)Prove – Correct 210

12.1.2 Accomplishing security 214

12.2 Service Management 220

12.2.1 Plan – Build – Change 222

12.2.2 Accomplishing security 229

12.2.3 Stocktake – Assemble – Preserve 236

12.2.4 Accomplishing security 241

12.3 ICT Service Access 246

12.3.1 Transportation..... 247

12.3.2 Customer side and endpoints 249

12.3.3 Connectivity 253

12.3.4 Securing transportation 256

12.3.5 Securing workplaces 258

12.3.6 Securing connectivity 265

12.4 IT Service Production 267

12.4.1 The lower IT stack 268

12.4.2 IT management and data center premises 274

12.4.3 Applications 279

12.4.4 Securing the lower IT stack 282

12.4.5 Securing IT management and data center premises 286

12.4.6 Securing applications 290

12.5 Risk Management and Certification..... 297

13 Routine – day-to-day security management using ESARIS 303

13.1 Fourteen tasks for managing security using ESARIS 303

13.2 Three ways of verifying compliance with security standards 309

13.3 A number of tips to deal with trouble and confusion..... 313

13.4 Buyers and providers: joint security management 316

14 Conclusion 325

Annexes..... 331

A Authors and acknowledgement..... 331

B Glossary (terms and definitions)..... 336

B.1 Fundamental terms..... 336

B.2 Terms relating to security organization..... 338

B.3 Terms relating to difficulties and restoration..... 342

B.4 Major concepts and models at a glance 343

C Literature..... 359

D Abbreviations 363

E Index 364

Overview: Fig. 1 below provides a quick point of reference.

Front matter

Foreword	Preface	About this book	Contents
----------	---------	-----------------	----------

Part 1: Foundation

1. Introduction: from pain to pleasure Challenges Beyond „Protection, Detection, Reaction“ Solutions	2. Scope and environment Perspectives; governance, frameworks <i>Enforcement Framework for ESARIS</i> <i>Endorsement Framework for ESARIS</i>	3. Building blocks and general set-up <i>ESARIS Dimensions and Work Areas</i> <i>ESARIS Collaboration Model</i> <i>Hierarchy of Security Standards</i> <i>Concept of Double Direction Standards</i>	4. ESARIS Security Taxonomy Design criteria Structure Areas and <i>ICT Security Standards</i> <i>Provider Scope of Control</i>	5. Integration with core business (ITSM) Secure by definition IT business units versus IT security Hands-on integrations
--	---	--	---	--

Part 2: Core activities

6. Standardization: quality and efficiency Necessity and benefits <i>ESARIS Industrialization Concept</i> <i>ESARIS Specification Concept</i> Obstacles and solutions	7. Attainment: comply with standards Foundation and overview From requirements all the way to... <i>ESARIS Attainment Levels</i> Service catalog integration	8. Fulfillment: meet customer demands IT-outsourcing: phases and actions Assurance: contractual evidence Assurance: operational evidence Contractual and other changes	9. Flexibility: manage supplier networks IT industry: roles and deliverables <i>ESARIS Third Party Integration Model</i> Summary
--	---	---	--

Part 3: Implementation

10. Maintenance: documents and more Naming conventions and assignments Document management Library, versions, consistency etc. Protecting intellectual property	11. Transformation: sustainable roll-out Subject: induce massive changes Approach: levels, master plans etc. Enablement: Training and communication Voyage of ICT services	12. Implementation: secure ICT in practice Evidence and customer relation Service Management ICT Service Access ICT Service Production Certification and Risk Management	13. Routine: security management Central activities due to the use of ESARIS Three ways of verifying compliance Dealing with trouble and confusion Joint security management	14. Conclusion Development of IT, IT security and ESARIS
--	---	--	---	--

Annexes

Authors and acknowledgement	Literature	Glossary	Index
-----------------------------	------------	----------	-------

Fig. 1: Structure of this book

Secure ICT Service Provisioning for Cloud, Mobile and
Beyond

ESARIS: The Answer to the Demands of Industrialized IT
Production Balancing Between Buyers and Providers

von Faber, E.; Behnsen, W.

2017, XIV, 369 p. 159 illus. in color., Hardcover

ISBN: 978-3-658-16481-2