

Table of Contents

1	Introduction.....	1
1.1	Why read this book?.....	1
1.2	How should this book be read?	3
1.3	What is the content of this book?.....	5
1.4	Relation to other programs.....	10
2	Security, assurance and the division of labor	25
2.1	Motivation for using third-party services	25
2.2	The problem: Economies versus a priori assurance.....	30
2.3	Perceived security and business risk.....	33
2.4	Balanced security profile and economies of scale	34
2.5	Risk management for third-party ICT services.....	37
3	Approach and framework	43
3.1	Setting goals.....	43
3.2	Perspectives	46
3.3	Framework for ESARIS.....	49
3.3.1	General	49
3.3.2	Enablement Framework for ESARIS.....	52
3.3.3	Enforcement Framework for ESARIS	53
3.4	ESARIS Industrialization Concept	56
3.4.1	Dealing with requirements.....	56
3.4.2	Composition of services.....	58
3.5	ESARIS Dimensions.....	59
4	Main building blocks.....	61
4.1	ESARIS Work Areas	61
4.2	ESARIS Collaboration Model.....	64
4.3	Hierarchy of Security Standards.....	68
4.3.1	Overview	69
4.3.2	Level 1: Corporate Security Policy	70
4.3.3	Level 2: Corporate Security Rule Base	71
4.3.4	Level 3: ICT Security Principles.....	73
4.3.5	Level 4: ICT Security Standards.....	74
4.3.6	Level 5: ICT Security Baselines	74
4.4	ESARIS Concept of Double Direction Standards	75

5	ESARIS Security Taxonomy	81
5.1	Criteria for the ESARIS Security Taxonomy	81
5.2	Understanding the ESARIS Security Taxonomy	87
5.3	The ICT Security Standards at a glance	93
5.3.1	Networks	94
5.3.2	Data center.....	96
5.3.3	Customer and users	99
5.3.4	Evidence and Customer Relation	100
5.3.5	Service Management.....	102
5.3.6	Certification and Risk Management	105
5.4	ESARIS Security Specification Concept.....	106
5.5	Summary of standards and taxonomy	113
6	ICT production and protecting it in practice	115
6.1	Evidence and Customer Relation	115
6.1.1	Match – (Im)Prove – Correct.....	116
6.1.2	Secure Accomplishment	121
6.2	Service Management	127
6.2.1	Plan – Build – Change.....	128
6.2.2	Secure Accomplishment	136
6.2.3	Stock – Assemble – Preserve	143
6.2.4	Secure Accomplishment	149
6.3	ICT Service Access.....	153
6.3.1	Transportation	155
6.3.2	Customer side and end-points.....	157
6.3.3	Connectivity	162
6.3.4	Securing transportation	165
6.3.5	Securing workplaces	167
6.3.6	Securing connectivity.....	174
6.4	IT Service Production.....	176
6.4.1	The lower ICT stack	177
6.4.2	ICT management and data center premises	184
6.4.3	Applications	189
6.4.4	Securing the lower ICT stack	192
6.4.5	Securing ICT management and data center premises.....	197
6.4.6	Securing applications.....	201
6.5	Certification and Risk Management	209
7	Usage of the ICT Security Standards	215
7.1	ESARIS Scope of Control	215
7.2	ESARIS Customer Fulfillment Model	220

7.3	ESARIS Compliance Attainment Model.....	222
7.3.1	Verification process	223
7.3.2	Who provides for compliance?	227
7.4	Conclusion	229
8	Rollout process	231
8.1	Organization and timing.....	231
8.2	Handling documentation.....	235
8.3	Protecting intellectual property	241
8.4	Making it a standard offering	243
A	Authors and acknowledgement.....	247
A.1	Acknowledgement.....	247
A.2	Curriculum vitae of Eberhard von Faber	249
A.3	Curriculum vitae of Wolfgang Behnsen	250
B	Terms and definitions	252
B.1	Fundamental terms.....	252
B.2	Terms relating to security organization.....	255
B.3	Terms relating to difficulties and restoration.....	259
B.4	Major concepts and models at a glance	262
C	Literature.....	274
D	Abbreviations	278
E	Index	280