

Contents

1	Introduction	1
1.1	Motivation	1
1.2	Research Questions	5
1.3	Overview	7
	References	8
2	Background	11
2.1	Overview	11
2.2	Security Standards	11
2.2.1	The ISO 27000 Series of Standards	12
2.2.2	ISO 27001	14
2.2.3	ISO 27001:2013	15
2.2.4	Common Criteria	16
2.3	Safety Standard ISO 26262	17
2.4	A Conceptual Framework for Security Requirements Engineering	18
2.5	Security Requirements Engineering Methods	20
2.5.1	Si*	20
2.5.2	CORAS	23
2.5.3	Problem Frame-Based Methods	29
2.6	The Agenda Concept	33
	References	33
3	The PEERESS Framework	37
3.1	Introduction	37
3.2	Coverage of Knowledge Areas	38
3.3	An Overview of the PEERESS Framework	40
3.4	Application of Our PEERESS Framework	45
3.5	Summary	47
	References	48

4	The CAST Method for Comparing Security Standards.	51
4.1	Introduction	51
4.2	A Method for Comparing Security Standards	52
4.3	CAST Step 1: Define a Common Terminology.	53
4.4	CAST Step 2: Analyze Existing Work.	54
4.4.1	The HatSec Method.	55
4.4.2	NIST SP 800-30 Standard	56
4.5	CAST Step 3: Define a Conceptual Model.	57
4.6	CAST Step 4: Instantiate Template with Standards	62
4.6.1	ISO 27001	62
4.6.2	ISO 27001:2013	63
4.6.3	IT Grundschutz.	64
4.6.4	The Common Criteria	69
4.7	CAST Step 5: Compare Standards.	73
4.8	Discussion	81
4.9	Summary	81
	References.	82
5	Relating ISO 27001 to the Conceptual Framework for Security Requirements Engineering Methods	85
5.1	Introduction	85
5.2	Relating ISO 27001 to Security Requirements Engineering Methods.	87
5.3	Insights	98
5.4	Practical Application of Our Results	104
5.5	Related Work	106
5.6	Summary	106
	References.	107
6	Supporting ISO 27001 Compliant ISMS Establishment with Si*	109
6.1	Introduction	109
6.2	A Method for Goal-Based ISMS Establishment.	110
6.3	Application of Our Method to a Smart Grid Scenario	115
6.4	Discussion	132
6.5	Related Work	133
6.5.1	Techniques that support ISO 27001 compliant ISMS Establishment	133
6.5.2	Goal-based Requirements Engineering for Security Analysis	134
6.6	Summary	135
	References.	135

7	Supporting ISO 27001 Establishment with CORAS	139
7.1	Introduction	139
7.2	The ISMS-CORAS Method	141
7.3	Application of Our Method	149
7.4	Related Work	188
7.5	Summary	191
	References.	192
8	Supporting Common Criteria Security Analysis with Problem Frames	195
8.1	Introduction	195
8.2	Supporting Common Criteria Using Problem Frames.	196
8.3	UML Profile for Problem-Based and Common Criteria-Compliant Security Analysis	197
8.4	A Method for a Systematic Security Analysis and Documentation	200
8.5	Application of Our Method	206
8.6	Tool Support	218
8.7	Discussion of Our Results with Practicioners	220
8.8	Related Work	222
8.9	Summary	225
	References.	226
9	Supporting ISO 26262 Hazard Analysis with Problem Frames	229
9.1	Introduction	229
9.2	Challenges in an ISO 26262 Hazard Analysis.	230
9.3	A Hazard Analysis and Risk Assessment Method	231
9.4	Tool Support	237
9.5	Application	239
9.6	Related Work	243
9.7	Summary	244
	References.	245
10	A Catalog of Context-Patterns.	247
10.1	Introduction	247
10.2	Definition.	248
10.3	Related Work	249
10.4	Cloud System Analysis Pattern	251
10.4.1	Graphical Pattern.	252
10.4.2	Templates.	253
10.4.3	Method	254
10.4.4	Example.	257
10.4.5	Tool Support	259

10.5	Peer-to-Peer System Analysis Pattern.	262
10.5.1	Graphical Pattern.	263
10.5.2	Templates.	264
10.5.3	Method	264
10.6	Service-Oriented Architecture Pattern.	266
10.6.1	Graphical Patterns	266
10.6.2	Templates.	269
10.6.3	Method	269
10.7	Law Pattern	272
10.7.1	Graphical Patterns	272
10.7.2	Templates.	273
10.7.3	Method	273
10.8	Summary	277
	References.	278
11	Initiating a Pattern Language for Context-Patterns	281
11.1	Motivation	281
11.2	A Template for Pattern Languages	282
11.2.1	Viewpoints of Pattern Languages	282
11.2.2	A Template for Describing a Pattern Language	284
11.2.3	Software Engineering Definitions of a Pattern Language	285
11.2.4	A Pattern Language for Context-Patterns	288
11.3	A Meta-Model for Context-Pattern	290
11.4	Relations Between Existing Context-Patterns	292
11.5	Summary	297
	References.	297
12	Supporting the Establishment of a Cloud-Specific ISMS According to ISO 27001 Using the Cloud System Analysis Pattern	299
12.1	Introduction	299
12.2	Governance, Risk, and Compliance for Clouds	300
12.3	Motivation for a Cloud-Specific ISMS Establishment Method	303
12.4	Overview of Our PACTS Method	306
12.5	PACTS Step 1: Get Management Commitment.	309
12.6	PACTS Step 2: Define ISMS Scope	313
12.6.1	The Extended Cloud Pattern	313
12.6.2	Instantiate the Extended Cloud Pattern with Our Running Example	318
12.7	PACTS Step 3: Identify Assets	322

12.8	PACTS Step 4: Analyze Threats	330
12.8.1	Cloud Security Alliance—Top Threats to Cloud Computing	331
12.8.2	Gartner’s Cloud Security Risks Assessment	332
12.8.3	Relations Between Threats and the Cloud Pattern	334
12.8.4	Cloud Threat Patterns	336
12.8.5	A Method for Pattern-Based Threat Analysis for Clouds	340
12.9	PACTS Step 5: Conduct Risk Assessment	344
12.10	PACTS Step 6: Create Security Policies and Reason About Controls	347
12.10.1	Controls in the ISO 27001 Standard	349
12.10.2	A Method for Establishing ISO 27001 Policies	349
12.10.3	Cloud Security Alliance: Cloud Controls Matrix	352
12.10.4	Application of Our ISO 27001 Policy Method to Our Running Example	355
12.10.5	Consistency Checks	357
12.10.6	Policy Change Pattern	359
12.11	PACTS Step 7: Design ISMS Specification	361
12.12	Considering Legal Compliance in the PACTS Method	362
12.12.1	Overview on Compliance Issues of Clouds	364
12.12.2	PACTS Step 8: Identify Relevant Laws and Regulations	366
12.12.3	Example	368
12.12.4	PACTS Step 9: Define Compliance Controls	371
12.12.5	Example	373
12.13	Considering Privacy in the PACTS Method	375
12.13.1	A Method for Considering Privacy in an ISMS	376
12.13.2	Pacts Step 10: Instantiate Privacy Patterns	376
12.13.3	Pacts Step 11: Analyze Privacy Threats	381
12.13.4	Example of Our Privacy Method	381
12.14	Related Work	385
12.15	Summary	388
	References	389
13	Validation and Extension of Our Context-Pattern Approach	393
13.1	Introduction	393
13.2	The ClouDAT Framework	395
13.3	A Catalog for Cloud Security Requirements Patterns	396
13.4	Representing Cloud Security Requirements Patterns	398
13.5	Discussion and Analysis	404
13.6	Tool Support	405

13.7	Discussions with Practitioners	409
13.8	Summary	411
	References.	412
14	Conclusion	415
14.1	Overview	415
14.2	Key Findings	415
14.2.1	Security-Requirements-Engineering-Based Establishment of Security Standards.	416
14.2.2	Knowledge Transfer of Our Results to the Establishment of Safety Standards	418
14.2.3	Structured Elicitation of the Environment with Context Patterns.	419
14.3	Answers to Our Research Questions	420
14.4	Directions for Future Research	422
14.4.1	Ontology-Based Support for Identifying Knowledge Objects to Support Security Standard Establishment	422
14.4.2	Investigating the Relations Between SRE and Security Testing	423
14.4.3	Empirical Studies	424
14.5	Summary	424
	References.	424
Appendix A: OCL-Expressions for Validation and Security Reasoning.		427
Appendix B: Comparing ISO 27001 and ISO 31000		457
Appendix C: Comparing Annex A of ISO 27001 and ISO 27001:2013		465
Appendix D: Template for Security Standards		473

<http://www.springer.com/978-3-319-16663-6>

Pattern and Security Requirements
Engineering-Based Establishment of Security Standards
Beckers, K.
2015, XXV, 474 p. 186 illus., Hardcover
ISBN: 978-3-319-16663-6