

# Contents

## Part I    Introductory Overview

<b>1</b>	<b>Introduction</b> . . . . .	3
1.1	The Importance of Risk Analysis . . . . .	3
1.2	Asset Identification . . . . .	4
1.3	Risk Modelling . . . . .	5
1.4	The CORAS Approach . . . . .	5
1.4.1	The CORAS Language . . . . .	6
1.4.2	The CORAS Tool . . . . .	6
1.4.3	The CORAS Method . . . . .	6
1.5	The Generality of CORAS . . . . .	7
1.6	Overall Aim and Emphasis . . . . .	8
1.7	Organisation . . . . .	8
1.7.1	Part I: Introductory Overview . . . . .	9
1.7.2	Part II: Core Approach . . . . .	9
1.7.3	Part III: Selected Issues . . . . .	11
1.7.4	Appendices . . . . .	12
1.8	Colours in CORAS and in this Book . . . . .	13
<b>2</b>	<b>Background and Related Approaches</b> . . . . .	15
2.1	Basic Terminology . . . . .	15
2.2	Related Approaches . . . . .	17
2.2.1	Risk Analysis Methods . . . . .	17
2.2.2	Table-based Risk Analysis Techniques . . . . .	18
2.2.3	Tree-based Risk Analysis Techniques . . . . .	18
2.2.4	Graph-based Risk Analysis Techniques . . . . .	19
2.2.5	Situating CORAS Within this Picture . . . . .	20
<b>3</b>	<b>A Guided Tour of the CORAS Method</b> . . . . .	23
3.1	Preparations for the Analysis . . . . .	23
3.2	Customer Presentation of the Target . . . . .	25
3.3	Refining the Target Description Using Asset Diagrams . . . . .	26

- 3.4 Approval of the Target Description . . . . . 31
- 3.5 Risk Identification Using Threat Diagrams . . . . . 33
- 3.6 Risk Estimation Using Threat Diagrams . . . . . 37
- 3.7 Risk Evaluation Using Risk Diagrams . . . . . 39
- 3.8 Risk Treatment Using Treatment Diagrams . . . . . 41

**Part II Core Approach**

- 4 The CORAS Risk Modelling Language . . . . . 47**
  - 4.1 Central Concepts . . . . . 48
    - 4.1.1 What is a Threat? . . . . . 48
    - 4.1.2 What is a Threat Scenario? . . . . . 49
    - 4.1.3 What is a Vulnerability? . . . . . 51
    - 4.1.4 What is an Unwanted Incident? . . . . . 53
    - 4.1.5 What is an Asset? . . . . . 55
  - 4.2 The Diagrams of the CORAS language . . . . . 56
    - 4.2.1 Asset Diagrams . . . . . 56
    - 4.2.2 Threat Diagrams . . . . . 58
    - 4.2.3 Risk Diagrams . . . . . 60
    - 4.2.4 Treatment Diagrams . . . . . 62
    - 4.2.5 Treatment Overview Diagrams . . . . . 64
  - 4.3 How to Schematically Translate CORAS Diagrams into English  
Prose . . . . . 65
    - 4.3.1 How to Translate Asset Diagrams . . . . . 65
    - 4.3.2 How to Translate Threat Diagrams . . . . . 67
    - 4.3.3 How to Translate Risk Diagrams . . . . . 69
    - 4.3.4 How to Translate Treatment Diagrams . . . . . 69
    - 4.3.5 How to Translate Treatment Overview Diagrams . . . . . 70
  - 4.4 Summary . . . . . 71
- 5 Preparations for the Analysis . . . . . 73**
  - 5.1 Overview of Step 1 . . . . . 73
  - 5.2 Conducting the Tasks of Step 1 . . . . . 76
  - 5.3 Summary of Step 1 . . . . . 78
- 6 Customer Presentation of the Target . . . . . 81**
  - 6.1 Overview of Step 2 . . . . . 81
  - 6.2 Conducting the Tasks of Step 2 . . . . . 83
    - 6.2.1 Presentation of the CORAS Terminology and Method . . . . . 83
    - 6.2.2 Presentation of the Goals and Target of the Analysis . . . . . 86
    - 6.2.3 Setting the Focus and Scope of the Analysis . . . . . 89
    - 6.2.4 Determining the Meeting Plan . . . . . 91
  - 6.3 Summary of Step 2 . . . . . 94
- 7 Refining the Target Description Using Asset Diagrams . . . . . 95**
  - 7.1 Overview of Step 3 . . . . . 95

- 7.2 Conducting the Tasks of Step 3 . . . . . 97
  - 7.2.1 Presentation of the Target by the Analysis Team . . . . . 97
  - 7.2.2 Asset Identification . . . . . 101
  - 7.2.3 High-level Analysis . . . . . 106
- 7.3 Summary of Step 3 . . . . . 109
  
- 8 Approval of the Target Description . . . . . 111**
  - 8.1 Overview of Step 4 . . . . . 111
  - 8.2 Conducting the Tasks of Step 4 . . . . . 113
    - 8.2.1 Approval of the Target Description . . . . . 114
    - 8.2.2 Ranking of Assets . . . . . 115
    - 8.2.3 Setting the Consequence Scales . . . . . 116
    - 8.2.4 Setting the Likelihood Scale . . . . . 118
    - 8.2.5 Defining the Risk Function . . . . . 120
    - 8.2.6 Deciding the Risk Evaluation Criteria . . . . . 122
  - 8.3 Summary of Step 4 . . . . . 124
  
- 9 Risk Identification Using Threat Diagrams . . . . . 125**
  - 9.1 Overview of Step 5 . . . . . 125
  - 9.2 Conducting the Tasks of Step 5 . . . . . 128
    - 9.2.1 Categorising Threat Diagrams . . . . . 128
    - 9.2.2 Identification of Threats and Unwanted Incidents . . . . . 129
    - 9.2.3 Identification of Threat Scenarios . . . . . 133
    - 9.2.4 Identification of Vulnerabilities . . . . . 137
  - 9.3 Summary of Step 5 . . . . . 144
  
- 10 Risk Estimation Using Threat Diagrams . . . . . 147**
  - 10.1 Overview of Step 6 . . . . . 147
  - 10.2 Conducting the Tasks of Step 6 . . . . . 149
    - 10.2.1 Likelihood Estimation . . . . . 150
    - 10.2.2 Consequence Estimation . . . . . 154
    - 10.2.3 Risk Estimation . . . . . 157
  - 10.3 Summary of Step 6 . . . . . 163
  
- 11 Risk Evaluation Using Risk Diagrams . . . . . 165**
  - 11.1 Overview of Step 7 . . . . . 165
  - 11.2 Conducting the Tasks of Step 7 . . . . . 167
    - 11.2.1 Confirming the Risk Estimates . . . . . 167
    - 11.2.2 Confirming the Risk Evaluation Criteria . . . . . 168
    - 11.2.3 Providing a Risk Overview . . . . . 169
    - 11.2.4 Accumulating Risks . . . . . 170
    - 11.2.5 Estimating Risks with Respect to Indirect Assets . . . . . 173
    - 11.2.6 Evaluating the Risks . . . . . 182
  - 11.3 Summary of Step 7 . . . . . 185

- 12 Risk Treatment Using Treatment Diagrams . . . . . 187**
  - 12.1 Overview of Step 8 . . . . . 187
  - 12.2 Conducting the Risk Treatment . . . . . 188
    - 12.2.1 Grouping of Risks . . . . . 189
    - 12.2.2 Treatment Identification . . . . . 191
    - 12.2.3 Treatment Evaluation . . . . . 196
  - 12.3 Summary of Step 8 . . . . . 203

**Part III Selected Issues**

- 13 Analysing Likelihood Using CORAS Diagrams . . . . . 207**
  - 13.1 Using CORAS Diagrams to Calculate Likelihood . . . . . 208
    - 13.1.1 Specifying Likelihood Using CORAS Diagrams . . . . . 208
    - 13.1.2 Rules for Calculating Probability in CORAS Diagrams . . . 210
    - 13.1.3 Rules for Calculating Frequency in CORAS Diagrams . . . 222
    - 13.1.4 Likelihood as Probability or Frequency . . . . . 226
    - 13.1.5 Generalisation to Intervals and Distributions . . . . . 227
  - 13.2 Using CORAS Diagrams to Check Consistency . . . . . 229
  - 13.3 Using CORAS to Analyse Scenarios with Logical Connectives . . 233
    - 13.3.1 Using CORAS to Analyse Scenarios with Logical  
Conjunction . . . . . 233
    - 13.3.2 Using CORAS to Analyse Scenarios with Logical  
Disjunction . . . . . 236
  - 13.4 How to Structure a Threat Diagram to Exploit the Potential for  
Likelihood Analysis . . . . . 237
    - 13.4.1 Enabling Application of Rules by Composition . . . . . 237
    - 13.4.2 Enabling Application of Rules by Decomposition . . . . . 239
  - 13.5 Summary . . . . . 243
- 14 The High-level CORAS Language . . . . . 245**
  - 14.1 Referring Elements and Referenced Diagrams . . . . . 246
    - 14.1.1 Threat Scenarios . . . . . 247
    - 14.1.2 Unwanted Incidents . . . . . 250
    - 14.1.3 Risks . . . . . 251
    - 14.1.4 Treatment Scenarios . . . . . 253
  - 14.2 Likelihoods in High-level CORAS . . . . . 257
    - 14.2.1 Reasoning About the Likelihoods in a High-level Diagram . 260
    - 14.2.2 Reasoning About the Likelihoods in a Referenced Diagram 261
    - 14.2.3 Analysing the Relation Between the Likelihoods of a  
Referring Element and the Likelihoods in the Referenced  
Diagrams . . . . . 263
  - 14.3 Consequences in High-level CORAS . . . . . 264
  - 14.4 Risk Levels in High-level CORAS . . . . . 266
  - 14.5 How to Schematically Translate High-level CORAS Diagrams  
into English Prose . . . . . 267

- 14.5.1 Referring Elements . . . . . 267
- 14.5.2 Referenced Diagrams . . . . . 270
- 14.6 Example Case in High-level CORAS . . . . . 271
  - 14.6.1 Threat Diagram . . . . . 272
  - 14.6.2 Risk Diagram . . . . . 275
  - 14.6.3 Treatment Diagram . . . . . 277
- 14.7 Summary . . . . . 279
- 15 Using CORAS to Support Change Management . . . . . 283**
  - 15.1 Classification of Changes . . . . . 283
    - 15.1.1 Target of Analysis . . . . . 284
    - 15.1.2 Scope and Focus . . . . . 285
    - 15.1.3 Environment . . . . . 285
    - 15.1.4 Assumptions . . . . . 285
    - 15.1.5 Parties and Assets . . . . . 286
    - 15.1.6 Context . . . . . 286
    - 15.1.7 Changes in our Knowledge . . . . . 287
  - 15.2 Managing Change . . . . . 287
    - 15.2.1 Maintenance Perspective . . . . . 288
    - 15.2.2 Before-after Perspective . . . . . 290
    - 15.2.3 Continuous Evolution Perspective . . . . . 294
  - 15.3 Summary . . . . . 296
- 16 The Dependent CORAS Language . . . . . 297**
  - 16.1 Modelling Dependencies Using the CORAS Language . . . . . 298
    - 16.1.1 Dependent CORAS Diagrams . . . . . 299
    - 16.1.2 Representing Assumptions Using Dependent CORAS  
Diagrams . . . . . 300
    - 16.1.3 How to Schematically Translate Dependent CORAS  
Diagrams into English Prose . . . . . 303
  - 16.2 Reasoning and Analysis Using Dependent CORAS Diagrams . . . 305
    - 16.2.1 Assumption Independence . . . . . 307
    - 16.2.2 Assumption Simplification . . . . . 308
    - 16.2.3 Target Simplification . . . . . 309
    - 16.2.4 Assumption Consequence . . . . . 310
  - 16.3 Example Case in Dependent CORAS . . . . . 311
    - 16.3.1 Creating Dependent Threat Diagrams . . . . . 311
    - 16.3.2 Combining Dependent Threat Diagrams . . . . . 313
  - 16.4 Summary . . . . . 316
- 17 Using CORAS to Analyse Legal Aspects . . . . . 319**
  - 17.1 Legal Risk . . . . . 319
  - 17.2 Uncertainty of Legal Aspects . . . . . 321
    - 17.2.1 Legal Uncertainty . . . . . 322
    - 17.2.2 Factual Uncertainty . . . . . 323
    - 17.2.3 Combining Legal and Factual Uncertainty . . . . . 324

- 17.3 Modelling Legal Aspects Using the CORAS Language . . . . . 326
  - 17.3.1 Legal CORAS Diagrams . . . . . 326
  - 17.3.2 How to Schematically Translate Legal CORAS Diagrams  
into English Prose . . . . . 328
- 17.4 Analysing Legal Aspects through the Eight Steps of CORAS . . . 330
- 17.5 Summary . . . . . 337
- 18 The CORAS Tool . . . . . 339**
  - 18.1 Main Functionality of the CORAS Tool . . . . . 339
  - 18.2 How to Use the CORAS Tool During Risk Analysis . . . . . 341
    - 18.2.1 Initial Modelling Before a Meeting . . . . . 341
    - 18.2.2 On-the-fly Modelling During a Meeting . . . . . 342
    - 18.2.3 Revising and Analysing Diagrams After a Meeting . . . . . 344
  - 18.3 Integration with Other Tools . . . . . 344
  - 18.4 Summary . . . . . 345
- 19 Relating CORAS to the State of the Art . . . . . 347**
  - 19.1 Risk Modelling . . . . . 347
  - 19.2 Risk Analysis Methods . . . . . 350
  - 19.3 Likelihood Analysis . . . . . 351
  - 19.4 High-level Risk Modelling . . . . . 353
  - 19.5 Change Management . . . . . 354
  - 19.6 Dependency Analysis . . . . . 355
  - 19.7 Legal Risk Management . . . . . 356
- Appendix A The CORAS Language Grammar . . . . . 359**
  - A.1 Basic CORAS . . . . . 359
    - A.1.1 Meta-model . . . . . 359
    - A.1.2 EBNF Grammar . . . . . 364
    - A.1.3 Examples . . . . . 366
  - A.2 High-level CORAS . . . . . 370
    - A.2.1 Meta-model . . . . . 370
    - A.2.2 EBNF Grammar . . . . . 374
    - A.2.3 Examples . . . . . 377
  - A.3 Dependent CORAS . . . . . 383
    - A.3.1 Meta-model . . . . . 383
    - A.3.2 EBNF Grammar . . . . . 385
    - A.3.3 Example . . . . . 386
  - A.4 Legal CORAS . . . . . 387
    - A.4.1 Meta-model . . . . . 387
    - A.4.2 EBNF Grammar . . . . . 388
    - A.4.3 Example . . . . . 389
- Appendix B The CORAS Language Semantics . . . . . 391**
  - B.1 Basic CORAS . . . . . 391
    - B.1.1 Elements . . . . . 392

- B.1.2 Relations . . . . . 392
- B.1.3 Diagrams . . . . . 393
- B.1.4 Examples . . . . . 394
- B.2 High-level CORAS . . . . . 398
  - B.2.1 Referring Elements . . . . . 398
  - B.2.2 Relations . . . . . 399
  - B.2.3 Referenced Diagrams . . . . . 402
  - B.2.4 Examples . . . . . 403
- B.3 Dependent CORAS . . . . . 410
  - B.3.1 Border . . . . . 410
  - B.3.2 Dependent Diagrams . . . . . 411
  - B.3.3 Example . . . . . 411
- B.4 Legal CORAS . . . . . 412
  - B.4.1 Elements . . . . . 412
  - B.4.2 Relations . . . . . 412
  - B.4.3 Example . . . . . 415
- Appendix C The CORAS Guidelines . . . . . 417**
  - C.1 Step 1: Preparations for the Analysis . . . . . 418
  - C.2 Step 2: Customer Presentation of the Target . . . . . 418
    - C.2.1 Step 2a: Presentation of the CORAS Terminology and Method . . . . . 419
    - C.2.2 Step 2b: Presentation of the Goals and Target of the Analysis . . . . . 419
    - C.2.3 Step 2c: Setting the Focus and Scope of the Analysis . . . . . 420
    - C.2.4 Step 2d: Determining the Meeting Plan . . . . . 420
  - C.3 Step 3: Refining the Target Description Using Asset Diagrams . . . . . 421
    - C.3.1 Step 3a: Presentation of the Target by the Analysis Team . . . . . 422
    - C.3.2 Step 3b: Asset Identification . . . . . 422
    - C.3.3 Step 3c: High-level Analysis . . . . . 422
  - C.4 Step 4: Approval of the Target Description . . . . . 423
    - C.4.1 Step 4a: Approval of the Target Description . . . . . 423
    - C.4.2 Step 4b: Ranking of Assets . . . . . 424
    - C.4.3 Step 4c: Setting the Consequence Scales . . . . . 424
    - C.4.4 Step 4d: Setting the Likelihood Scale . . . . . 424
    - C.4.5 Step 4e: Defining the Risk Function . . . . . 424
    - C.4.6 Step 4f: Deciding the Risk Evaluation Criteria . . . . . 425
  - C.5 Step 5: Risk Identification Using Threat Diagrams . . . . . 425
    - C.5.1 Step 5a: Categorising Threat Diagrams . . . . . 426
    - C.5.2 Step 5b: Identification of Threats and Unwanted Incidents . . . . . 427
    - C.5.3 Step 5c: Identification of Threat Scenarios . . . . . 427
    - C.5.4 Step 5d: Identification of Vulnerabilities . . . . . 428
  - C.6 Step 6: Risk Estimation Using Threat Diagrams . . . . . 428
    - C.6.1 Step 6a: Likelihood Estimation . . . . . 429
    - C.6.2 Step 6b: Consequence Estimation . . . . . 429

- C.6.3 Step 6c: Risk Estimation . . . . . 430
- C.7 Step 7: Risk Evaluation Using Risk Diagrams . . . . . 430
  - C.7.1 Step 7a: Confirming the Risk Estimates . . . . . 431
  - C.7.2 Step 7b: Confirming the Risk Evaluation Criteria . . . . . 431
  - C.7.3 Step 7c: Providing a Risk Overview . . . . . 432
  - C.7.4 Step 7d: Accumulating Risks . . . . . 432
  - C.7.5 Step 7e: Estimating Risks with Respect to Indirect Assets . 432
  - C.7.6 Step 7f: Evaluating the Risks . . . . . 433
- C.8 Step 8: Risk Treatment Using Treatment Diagrams . . . . . 433
  - C.8.1 Step 8a: Grouping of Risks . . . . . 434
  - C.8.2 Step 8b: Treatment Identification . . . . . 434
  - C.8.3 Step 8c: Treatment Evaluation . . . . . 435
- Appendix D The CORAS Terminology . . . . . 437**
- Appendix E Glossary of Terms . . . . . 445**
  - E.1 Logic . . . . . 445
  - E.2 Sets . . . . . 445
  - E.3 Likelihoods . . . . . 445
  - E.4 Likelihood Intervals . . . . . 446
  - E.5 Deductions . . . . . 447
  - E.6 Extended Backus-Naur Form . . . . . 447
  - E.7 Semantics . . . . . 448
  - E.8 Miscellaneous . . . . . 448
- Acronyms . . . . . 449**
- References . . . . . 451**
- Index . . . . . 455**





<http://www.springer.com/978-3-642-12322-1>

Model-Driven Risk Analysis

The CORAS Approach

Lund, M.S.; Solhaug, B.; Stolen, K.

2011, XVI, 460 p., Hardcover

ISBN: 978-3-642-12322-1