Preface

Exposure to risk is inescapable in most domains. People and families, enterprises, governments, private and public organisations, infrastructure providers, service providers, and so forth all encounter risks on an ongoing and frequent basis. The kinds of risks however vary from domain to domain, be it safety, economy, information and ICT security, politics, civil protection, emergency planning, defence, law, health, and so on. The need for understanding and managing risk is self-evident. Risk management is moreover in many cases imposed as a prerequisite, be it by law and legal regulations or from the public opinion, in particular within critical areas that may affect privacy and welfare, or even health and human life. In other cases, the lack of good routines, cultures and processes for managing risk may be a decisive factor for risks to emerge that should or could have been avoided.

In this book, we present CORAS, which is a model-driven approach to risk analysis. Risk analysis is a core part of the overall process of risk management. In order to conduct risk analysis in practice, there is clearly a need for well-defined methods, techniques and guidelines for how to do this, and this is precisely what CORAS offers. Risk analysts, or for that matter anyone with a need for identifying and understanding risks, will in this book find guidance on how to conduct a stepwise, structured and systematic analysis and documentation of risks.

The book also serves as an introduction to risk analysis in general, and as an introduction to the central and well-established underlying concepts and terminology. Practitioners, as well as graduate or undergraduate students, particularly within the IT domain, are therefore main target groups of this book. CORAS is strongly related to international standards on risk management, and this book therefore serves as an introduction to many of the issues that are addressed in these standards.

An important objective of this book is to accompany standardised risk management guidelines and terminology with comprehensive pragmatic support. International standards generally focus on the *what*, but say little or nothing about the *how*. This book is a self-contained contribution not only to understand what risk management, risk analysis and risk related concepts are, but also to learn how to do risk analysis in practice. Extensive use of practical and illustrative examples furthermore facilitates a deep understanding of both the pragmatics and the conceptual aspects.

The comprehensiveness of CORAS is manifested by the three complementary parts of the approach. CORAS consists of a customised language for risk modelling, a tool supporting the language, and a risk analysis method into which the tool-supported risk modelling language is tightly interwoven. It is particularly the specialised support for risk modelling that distinguishes CORAS from other approaches to risk analysis. The CORAS language provides explicit support for the risk analysis steps and tasks, and is furthermore closely related to the underlying risk analysis concepts.

The CORAS approach as presented in this book is the result of work that was initiated in 2001, and that draws upon academic research, empirical studies, thorough experience, as well as close interaction and cooperation with actors from several industrial domains. Along the way, we have benefited greatly from fruitful cooperation with many colleagues, and much work on different aspects of CORAS has already been published in articles, papers, reports and doctoral theses. Several colleagues have also contributed to this book by coauthoring some of the chapters, or by giving valuable criticism, suggestions and feedback, and for this we owe them great thanks.

We are deeply grateful to Ida Hogganvik Grøndahl for her influential doctoral work. Many aspects of the CORAS approach as presented in this book are strongly inspired by her work, in particular the basic CORAS language.

We owe our great thanks to Gyrd Brændeland, Atle Refsdal and Fredrik Seehusen for each coauthoring a chapter in this book, and for their valuable suggestions and comments. Fredrik Seehusen has moreover contributed by being the main developer of the current version of the CORAS tool. Many thanks also to Folker den Braber, Heidi Dahl and Fredrik Vraalsen for their contributions over the past years, and to Olav Ligaarden for helping us with the index and for making valuable suggestions.

Many thanks to Tobias Mahler for his many comments and fruitful criticism, in particular on the chapter on legal aspects. His doctoral work on legal risk management served as a valuable source of inspiration, and we acknowledge the synergies between his work and the work that has led to this book.

We are thankful to Jan Øyvind Aagedal, Iselin Engan, Bjørn Axel Gran, Jan Heim, Siv Hilde Houmb, Tormod Håvaldsrud, Tom Lysemose, Aida Omerovic, Eva Skipnes and Jan Håvard Skjetne, each of which has contributed by valuable suggestions or via fruitful cooperation in CORAS related work.

We are thankful to our colleagues at SINTEF ICT, including our Head of Department Bjørn Skjellaug. Many thanks also to the colleagues that we have worked with in several national and international projects that have been related to CORAS. These people include Demissie Aredo, Gustav Dahll, Theo Dimitrakos, Ivan Djordjevic, Rune Fredriksen, Chingwoei Gan, Eva Henriksen, Erik Mork Knutsen, Monica Kristiansen, Simon Lambert, Katerina Papadaki, Xavier Parent, Athanasios Poulakidas, Dimitris Raptis, Brian Ritchie, Yannis Stamatiou, Nikos Stathiakis, Atoosa Thunem, Erik Wisløff and Bjarte Østvold.

We also recognise the valuable feedback and knowledge acquired from many industrial field trials and commercial risk analyses based on CORAS. In relation to this, we would like to thank Tor Aalborg, Semming Austin, Nils Inge Bruberg, Petter Christensen, Sten Vidar Eikrem, Håvard Fridheim, Are Torstein Gimnes, David

Goldby, Janne Hagen, Rune Hagen, Tor-Gaute Indstøy, Hege Jacobsen, Ole Jarl Kvammen, Arne Bjørn Mildal, Per Myrseth, Mikkel Skou, Petter Taugbøl, Anne Karin Wahlfjord, Hermann Steen Wiencke and Jon Ølnes.

We are also in debt to the many students who have followed our course INF5150 at the University of Oslo since it was started up in 2001, as well as the to the MSc students who have addressed various aspects of CORAS in their thesis work. In particular, we would like to thank Emese L. Bogya, Jenny Beate Haugen, Vikash Katta, Igor Kodrik, Mihail Korabelnikov, Stig Torsbakken, and Shahbaz Chaudhary Yaqub.

Our work on developing the CORAS approach has benefited from research in joint projects with a number of good partners. The initial CORAS approach was developed within the CORAS project funded by the European Commission that ran from 2001 until 2003. We are thankful to the project coordinator Yves Paindaveine, as well as the project leaders Tom Arthur Opperud and Tony Price, for providing a good environment for fruitful research. We are also grateful to Habtamu Abie who together with Eva Skipnes in 1999 invited us to join the consortium that later started the CORAS project.

Some of the research results that is reported in this book has partly been funded by the Research Council of Norway through the projects COBRA, COMA, DIGIT, EMERGENCY, ENFORCE and SECURIS. The research has also partly been funded by the European Commission through the projects iTrust, MASTER, MODELWARE, SecureChange, S3MS and TrustCoM.

Oslo, Norway   Mass Soldal Lund
                                                                                    Bjørnar Solhaug
                                                                                      Ketil Stølen