

Review of the book
"Information Security Evaluation A holistic Approach"
by Igli Tashi, Solange Ghernaouti Helie
EPFL Press, 2011

ISBN: 978-2-940222-53-7

Nishant Doshi
MEFGI, Gauridad Campus, India

1 Summary of the review

In today's e-world, everything is available as single click. Indeed, this also requires the security of the messages and also the proper authentication of it too. Thus in the corporate world, it becomes necessary to develop information security assessment model to evaluate own security parameters. This book is of its first kind to propose the Information Security Assurance Assessment Model (ISAAM) to visualize the various dimension of security. The framework approach in this book is in general applicable to any organization.

For the researchers, this book gives the fundamentals understanding of the information security, and to develop information security assurance assessment model from scratch. I will recommend this book to the UG students to strengthen their fundamentals on information security. For the PG student (and researchers too) to get the well depth understanding with further scope of improvements in the information security assessment model and analysis using various tools.

2 Summary of the book

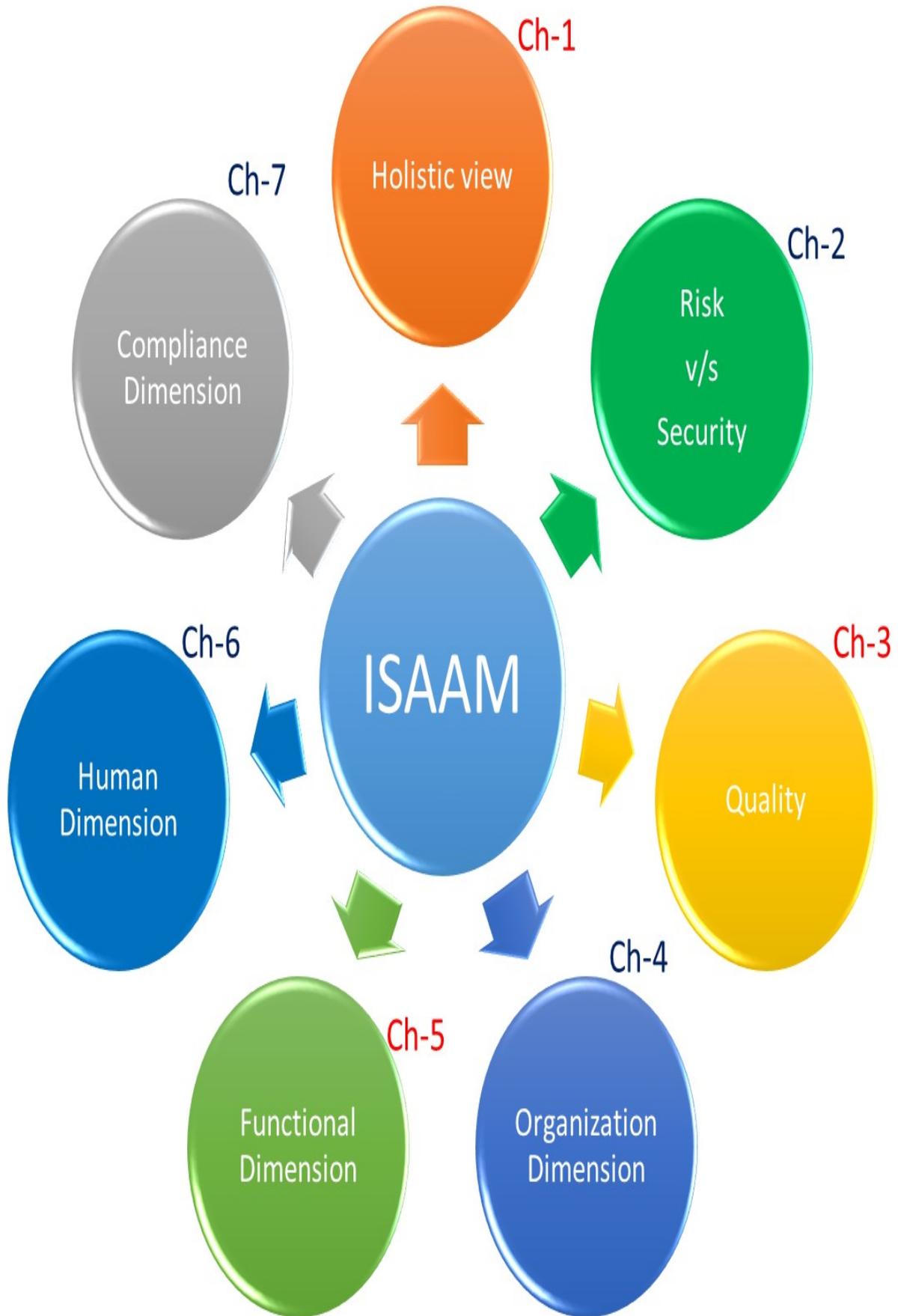
Chapter 1 This chapter starts with current stakes and challenges for information security and afterward deep drive in governance perspective of it. The different actors of system and relationship among them is diagrammatically defined. In the holistic view, various parameters like government, employee, investor, criminals, etc. are shown with its influence to information security. Thus, I can say that this chapter server its purpose as introduction.

Chapter 2 After getting introduction to information security. This chapter lead the reader to to important aspects of it i.e. risk and security management. It begins with what is risk management, ISO standard of it. It shows the analysis and assessment process of risk. After this, it explains the difference between risk and security assessment very nicely.

Chapter 3 The aim of this chapter is to familiarize the readership with authors proposed Information Security Assurance Assessment Model (ISAAM) model with its different layers and components within it. It starts with multidimensional view of information security and explains the various domains and dimensions of it. Authors have taken the nice use of diagrams to explain the each concepts of it.

Chapter 4-7 The ISAAM model is put to test in four of information security dimension i.e. organizational, functional, human and compliance. Thus ch.4 to 7 deals with each of the dimension with respect to ISAAM model. Authors have taken the two layer approach to deal with each dimension as follows.

- The first layer deals with the basics required to understand the respective domains. These includes the elements, focus area, etc. of the dimension.



- The second layer is built upon the first layer and authors have nicely put the ISAAM model to identify the risks, process, procedures, etc. of the respective dimension. Finally, for each of the dimension, authors have suggest the generic maturity model which helps for each organization to define its own security assessment.

Chapter 8 This chapter not only gives the concluding remarks but also gives scope of ISAAM and requirements of new paradigm.

3 Comments and Recommendations

One thing that I like about this book is *how* it proves its title in each chapter. First is to give introduction to various information security measures and second it to model the same using the ISAAM model. In addition, the footnote in every page really helps the reader to get quick reference for each topic. One thing, that I suggest to incorporate in future editions is discussion about various tools for readers to implement it. Also some real time scenario with case studies can be helpful to novice readers too. Finally, some future scopes can be mentioned to help researchers to work on it.

On an average, this book gives the undergraduate students (of pre-final year), postgraduate students, researchers, scientists and so on to motivate and also to study further in the information security assurance assessment model and how to do the analysis of them. Surely, I will suggest this book as first hand book in information security model for UG, PG and the researchers.

The reviewer is a faculty at Department of Computer Engineering, MEFGI, India.