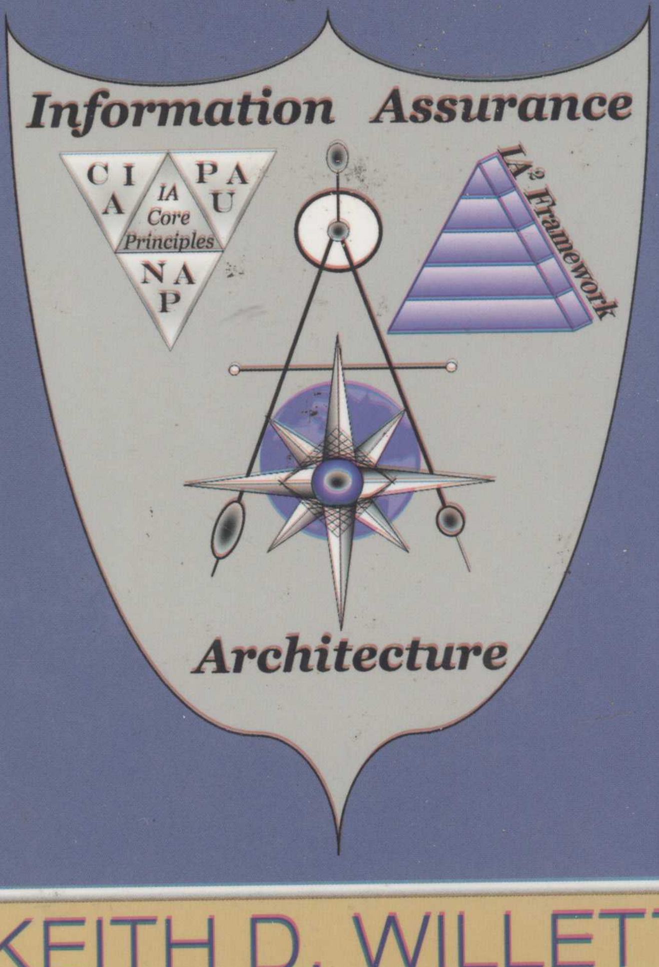
INFORMATION ASSURANCE ARCHITECTURE



KEITH D. WILLETT

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

INFORMATION ASSURANCE ARCHITECTURE

KEITH D. WILLETT

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-0-8493-8067-9 (Hardcover)

This book contains information obtained from authentic and highly regarded sources Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The Authors and Publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Willett, Keith D.
Information assurance architecture / author, Keith D. WIllett.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-8493-8067-9 (hardback : alk. paper) 1. Computer security.
2. Computer networks--Security measures. 3. Information resources
management. 4. Information technology--Management. 5. Business
enterprises--Communication systems--Management. 6. Data protection. I.
Title.

QA76.9.A25W5487 2008
005.8--dc22 2008010630

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the Auerbach Web site at
http://www.auerbach-publications.com

INFORMATION ASSURANCE ARCHITECTURE

802.1X Port-Based Authentication
Edwin Lyle Brown
ISBN: 1-4200-4464-8

Building an Effective Information Security Policy Architecture
Sandy Bacik
ISBN: 1-4200-5905-X

CISO Soft Skills: Securing Organizations Impaired by Employee Politics, Apathy, and Intolerant Perspectives
Michael Gentile, Ron Collette and
Skye Gentile
ISBN: 1-4200-8910-2

Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI
Debra S. Herrmann
ISBN: 0-8493-5402-1

Computer Forensics: Evidence Collection and Management
Robert C. Newman
ISBN: 0-8493-0561-6

Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition
Albert Marcella, Jr. and Doug Menendez
ISBN: 0-8493-8328-5

Digital Privacy: Theory, Technologies, and Practices
Alessandro Acquisti, Stefanos Gritzalis,
Costos Lambrinoudakis and
Sabrina di Vimercati
ISBN: 1-4200-5217-9

How to Achieve 27001 Certification: An Example of Applied Compliance Management
Sigurjon Thor Arnason and Keith D. Willett
ISBN: 0-8493-3648-1

Information Assurance Architecture
Keith D. Willett
ISBN: 0-8493-8067-7

Information Security Management Handbook, Sixth Edition
Harold F. Tipton and Micki Krause
ISBN: 0-8493-7495-2

Information Security Management Handbook, Sixth Edition, Volume 2
Harold F. Tipton and Micki Krause
ISBN: 1-4200-6708-7

Information Security Management Handbook, 2008 CD-ROM Edition
Harold F. Tipton and Micki Krause
ISBN: 1-4200-6698-6

Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks
Kenneth Brancik
ISBN 1-4200-4659-4

Mechanics of User Identification and Authentication: Fundamentals of Identity Management
Dobromir Todorov
ISBN: 1-4200-5219-5

Official (ISC)2 Guide to the SSCP CBK
Diana-Lynn Contesti, Douglas Andre, Eric
Waxvik, Paul A. Henry and Bonnie A. Goins
ISBN: 0-8493-2774-1

Oracle Identity Management: Governance, Risk, and Compliance Architecture, Third Edition
Marlin B. Pohlman
ISBN: 1-4200-7247-1

Software Deployment, Updating, and Patching
Bill Stackpole and Patrick Hanrion
ISBN: 0-8493-5800-0

Testing Code Security
Maura A. van der Linden
ISBN: 0-8493-9251-9

Wireless Crime and Forensic Investigation
Gregory Kipper
ISBN: 0-8493-3188-9

AUERBACH PUBLICATIONS
www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

Dedication

To opportunity! *Luck* is preparation meeting opportunity. I dedicate this book to those who provided me with the opportunity to put into practice many, many years of preparation:

- My father, Louis Willett, for teaching me what discipline is as he learned from his grandfather Henry Cochran, and for living the example that education and success are never further away than a commitment to hard work.
- My mother, Mary Elizabeth Willett, for always being there in every situation.
- My wife, Terri Meyer Willett, for her unwavering encouragement and patience during the writing of this book, and for being a shining example of perseverance and showing me a strong spirit gets you through the challenges.
- My teacher, Joyce Currie Little, for inspiration in forward thinking and turning thoughts into action; I never told her this in person and I am only sorry it took me 20 years to express my appreciation.
- My first technical manager, Doris Fell, for her ability to express complex issues in understandable terms and her patience in repeating many examples many times.
- My first commercial hiring manager, John Parkent—thanks for the opportunity; it was a first step on a long and winding career path.
- Mich Kabay for an example of truest professionalism and energy. Mich sets a new standard for vision, execution, and results. Mich's hard work in developing the Norwich University Master of Information Assurance (MSIA) program provided the forum to develop the initial version of this work as a master's thesis.
- Peter Stephenson for introducing me to the excellent people at Auerbach Publications who afforded me the opportunity to write this book.

Author's Note

If I have seen further it is by standing on ye shoulders of Giants.

—Isaac Newton

This work is a continuation on a long path of knowledge, and my greatest hope is to take another step forward in the professions of information assurance and enterprise architecture.

Information assurance architecture (IA^2) will evolve into an ever-more refined discipline that promotes practical and efficient information assurance (IA) solutions to effectively address business risk. Please feel free and encouraged to supply any comments or input to kwillett@ia2.info. Also, look for IA^2 updates, clarification, and supplemental tools on www.ia2.info. You may need a copy of this book handy to find the passwords that grant access to the extras for those of you kind enough to have purchased this book.

This book may make reference to vendors, products, and services. These are for examples only and do not constitute an endorsement of any particular vendor, product, or service for any particular purpose.

Scope and Objective

Information Assurance Architecture introduces a new way to think about IA. The IA services and IA mechanisms herein are not new; however, IA^2 provides a method to identify, select, and arrange IA services and mechanisms that find root in business needs and provide for the effective management of business risks. This work provides the security industry with a formal *information assurance architecture* (IA^2) that complements enterprise architecture, systems engineering, and enterprise life-cycle management (ELCM). For many readers, this book will be an introduction to the disciplines of enterprise architecture (EA) and systems engineering (SE). There are many excellent books on these subjects (see Appendix L, "Reading List") and the details regarding EA and SE herein are merely an introduction to give context to IA^2.

IA^2 itself consists of an IA^2 Framework, IA^2 Process, and many supporting tools, templates, and methodologies. The IA^2 Framework provides a reference model for the consideration of security in many contexts and from many various perspectives. The IA^2 Process provides direction on how to apply the IA^2 Framework. There are many tools that may be used individually or together to address IA issues. IA^2 provides you with the tools for a disciplined approach to think about, plan for, implement, and operate IA solutions that integrate with the enterprise.

Security for its own sake, like technology for its own sake, is not good business practice. If security or technology is a hobby, then by all means pursue them to the delight of your intellectual satisfaction. However, when introducing IA services or IA mechanisms into a business environment, there must be sound business reasons to do so. Therefore, this book conveys many non-IA aspects with the understanding that a discussion about a business process, business service, technical infrastructure, or technical application is incomplete until there are discussions about risk and how to address that risk. Therefore, it is critical to integrate IA into the processes, planning, and implementation of business governance, management, and operations.

The objectives of *Information Assurance Architecture* include:

- Introduce the disciplines of enterprise architecture and systems engineering
- Introduce the concept of IA architecture
- Introduce the IA^2 constructs: the IA^2 Framework and the IA^2 Process
- Provide a business context for IA^2
- Align IA^2 with the discipline of EA
- Explain how to use IA^2 Framework and IA^2 Process as tools for business risk management
- Introduce a series of frameworks to provide the IA architect with an effective approach to manage the complexity of enterprisewide IA

Target Audience

This book is primarily for security engineers, security architects (information assurance architects), security management, and other security personnel with interest in identifying and addressing business risk in a disciplined, repeatable, and comprehensive manner. The book is also useful for enterprise architects and systems architects who desire to integrate information assurance in their solutions. Business managers, project managers, program managers, and many others will find this book useful to understand information assurance in context of the enterprise, including business need, business fit, and business justification for IA.

The book is written to address the information assurance architect. You may take this term to imply any individual who desires a disciplined, repeatable approach to identify, enumerate, articulate, understand, and address business risk, or in other words, understand the enterprise context of IA.

This work covers many information assurance (IA) subjects, like disaster recovery, firewalls, etc. However, the goal is *not* to instruct in the mechanics of these areas; rather, the objective is to present security services and security mechanisms in context of IA^2, architectural considerations, and in an enterprise context of managing business risk. The reader should have at least intermediate knowledge of information technology and information assurance to derive the most benefit from this book.

Goals for the Reader

We all start out life not knowing that we do not know. As we go along, most of us learn *about* many things; that is, we become aware of them. There is a big difference between *knowing about* something and *knowing* that something. We decide what subjects to pursue in more depth according to our personal interest, economic need, and many other motivations. We then discover varying degrees of aptitude and fluency with what we pursue. The learning progression is from awareness to understanding, understanding to use, and varying degrees of use, including *appropriate* use, *effective* use, and even *secure* use (Figure 1).

As an IA architect, you need the right tools to accomplish your mission of generating an IA architecture and integrating IA with enterprise architecture. *Information Assurance Architecture* is an IA architecture toolkit. A toolkit is a collection of tools, a tool is a device for a specific purpose; a hammer drives in nails, or the other end of the hammer can pull out nails. Moreover, there is an appropriate use for each tool; a hammer can insert a screw, but a screwdriver is a better choice so the threads grip the wood more effectively. Experience and skill provide for appropriate tool selection and effective tool application.

At the end of studying this material, you should have an understanding of IA^2, the IA^2 Framework, and the IA^2 Process, and how to apply them in an enterprise

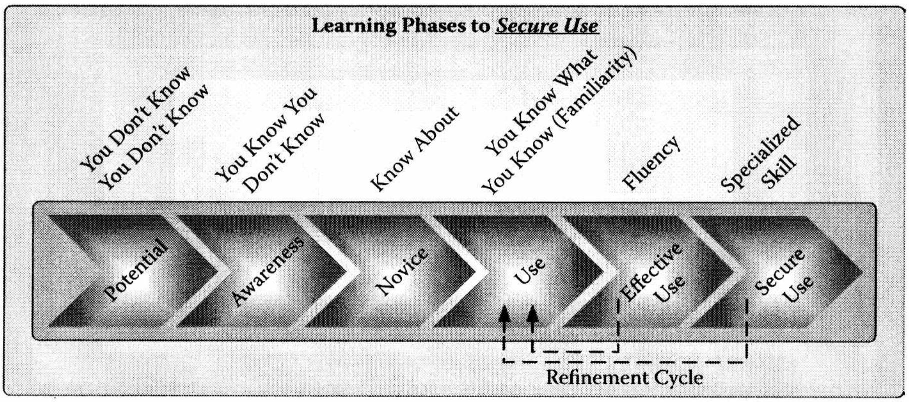


Figure 1 Learning phases to secure use.

context. You should have an awareness of what EA is and the need to integrate information assurance with EA. Moreover, you should understand how to use IA^2 to determine IA requirements and align those IA requirements with business drivers. You should understand an approach to develop an IA quantification scheme.

This book provides you with a disciplined approach to learn the variety of contexts and perspectives for IA, and how to view and think about IA in various contexts and from various perspectives. Fluency in IA^2 only comes from study, application, and hard work. IA architecture is not easy, but is critical for cost-effective risk management.

Preface

When teaching at Towson University in 1984, a student asked, "What is the purpose of college?" My answer was that college should teach you two things: how to think, and if you do not know the answer, where to find it. A subsequent question was, "How do you teach someone to think?" My answer was, "Hmmm...well, I don't know." More than 20 years later, I still do not know, but I have some ideas. Many of those ideas are herein.

Information Assurance Architecture does not provide answers to conventional questions regarding security. You will not learn how to perform a risk assessment, design a secure network, or configure a firewall. You will learn *how to think about* these and many other aspects of information assurance. *Information Assurance Architecture* is more a philosophy of IA than a how-to for IA—a philosophy that provides insight on how to think about IA in context of the entire organization (the enterprise). This IA thought process will help you discern and define the problem (the risks), identify and enumerate options on how to address the problem, identify constraints on determining the best solution, and how to select the best solution and move forward to design, implement, test, deploy, and operate that solution.

Will this book teach you how to think? Well, if you do not know how to think, it may point you in the right direction. If you already know how to think, *Information Assurance Architecture* will help you think better.

Acknowledgments

I wish to gratefully acknowledge Elizabeth Templeton, the administrative director of the MSIA program at Norwich University in Vermont. Elizabeth provided invaluable support as an editor for this book. Elizabeth's technical and editing experience enabled her to provide thoughtful input with challenges as necessary and encouragement when needed. Thank you!

Contents

SECTION II APPLIED IA^2