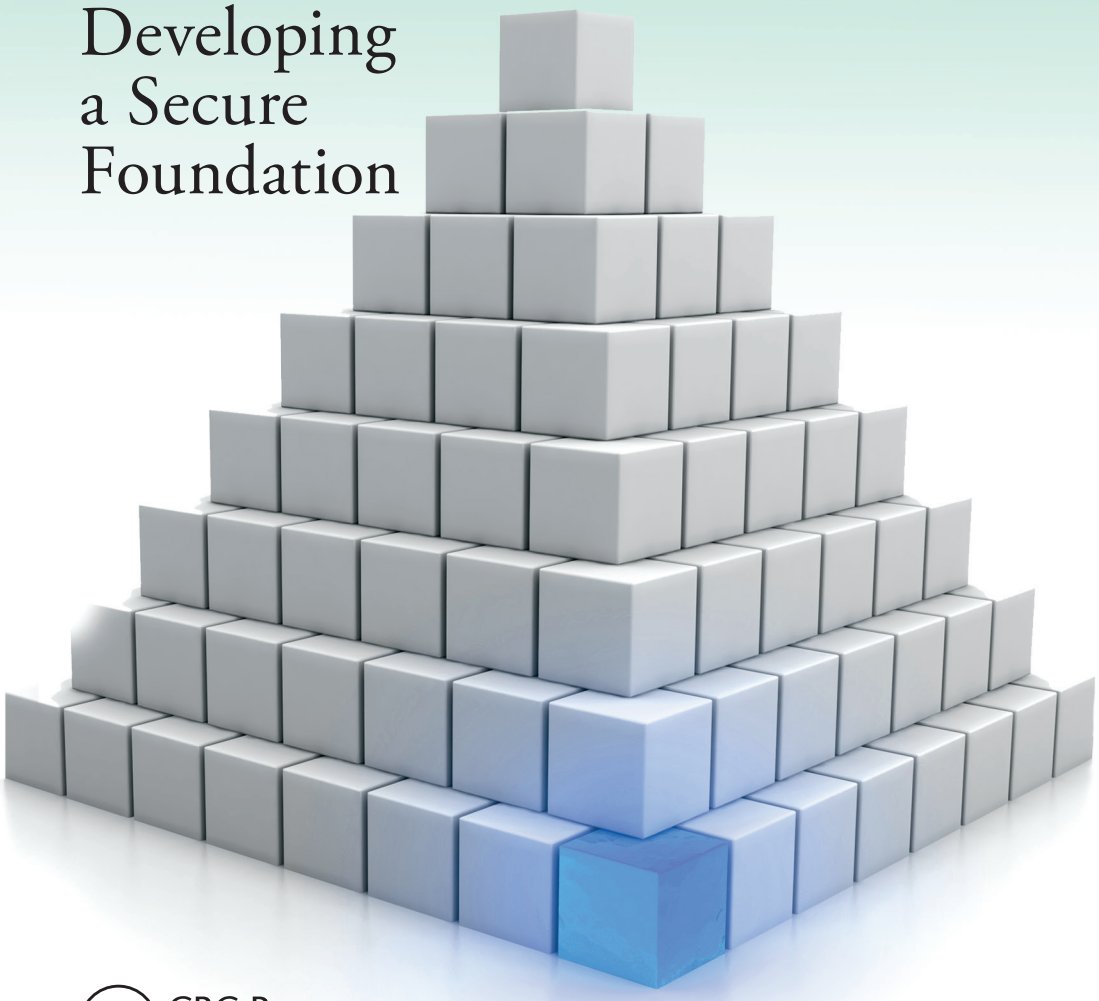
Enterprise Architecture and Information Assurance

Developing a Secure Foundation



CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

James A. Scholz

Enterprise Architecture and Information Assurance

Developing a Secure Foundation

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

Asset Protection through Security Awareness
Tyler Justin Speed
ISBN 978-1-4398-0982-2

Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks
Mohssen Mohammed and Al-Sakib Khan Pathan
ISBN 978-1-4665-5727-7

The Complete Book of Data Anonymization: From Planning to Implementation
Balaji Raghunathan
ISBN 978-1-4398-7730-2

The Complete Guide to Physical Security
Paul R. Baker and Daniel J. Benny
ISBN 978-1-4200-9963-8

Conflict and Cooperation in Cyberspace: The Challenge to National Security
Panayotis A Yannakogeorgos and Adam B Lowther (Editors)
ISBN 978-1-4665-9201-8

Cybersecurity: Public Sector Threats and Responses
Kim J. Andreasson
ISBN 978-1-4398-4663-6

The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules
John J. Trinckes, Jr.
ISBN 978-1-4665-0767-8

Digital Forensics Explained
Greg Gogolin
ISBN 978-1-4398-7495-0

Digital Forensics for Handheld Devices
Eamon P. Doherty
ISBN 978-1-4398-9877-2

Effective Surveillance for Homeland Security: Balancing Technology and Social Issues
Francesco Flammini, Roberto Setola, and Giorgio Franceschetti (Editors)
ISBN 978-1-4398-8324-2

Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval
David R. Matthews
ISBN 978-1-4398-7726-5

Enterprise Architecture and Information Assurance: Developing a Secure Foundation
James A. Scholz
ISBN 978-1-4398-4159-4

Guide to the De-Identification of Personal Health Information
Khaled El Emam
ISBN 978-1-4665-7906-4

Information Security Governance Simplified: From the Boardroom to the Keyboard
Todd Fitzgerald
ISBN 978-1-4398-1163-4

Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0
Barry L. Williams
ISBN 978-1-4665-8058-9

Information Technology Control and Audit, Fourth Edition
Sandra Senft, Frederick Gallegos, and Aleksandra Davis
ISBN 978-1-4398-9320-3

Iris Biometric Model for Secured Network Access
Franjieh El Khoury
ISBN 978-1-4665-0213-0

Managing the Insider Threat: No Dark Corners
Nick Catrantzos
ISBN 978-1-4398-7292-5

Network Attacks and Defenses: A Hands-on Approach
Zouheir Trabelsi, Kadhim Hayawi, Arwa Al Braiki, and Sujith Samuel Mathew
ISBN 978-1-4665-1794-3

Noiseless Steganography: The Key to Covert Communications
Abdelrahman Desoky
ISBN 978-1-4398-4621-6

PRAGMATIC Security Metrics: Applying Metametrics to Information Security
W. Krag Brotby and Gary Hinson
ISBN 978-1-4398-8152-1

Securing Cloud and Mobility: A Practitioner's Guide
Ian Lim, E. Coleen Coolidge, and Paul Hourani
ISBN 978-1-4398-5055-8

Security and Privacy in Smart Grids
Yang Xiao (Editor)
ISBN 978-1-4398-7783-8

Security for Wireless Sensor Networks using Identity-Based Cryptography
Harsh Kupwade Patil and Stephen A. Szygenda
ISBN 978-1-4398-6901-7

The 7 Qualities of Highly Secure Software
Mano Paul
ISBN 978-1-4398-1446-8

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

Enterprise Architecture and Information Assurance

Developing a Secure Foundation

James A. Scholz

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

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

Version Date: 20130617

International Standard Book Number-13: 978-1-4398-4160-0 (eBook - PDF)

This book is dedicated to all those hardworking system administrators who do not get enough recognition for the thankless job of keeping data safe, systems running, and development life cycles moving.
This book is dedicated to the members of the American public who would like to understand what our government does to secure our data and where our taxpaying dollars go in support of the countless undisclosed amounts of data.
And of course, many thanks to my lovely wife for the hours spent proofreading the many lines of this book to ensure that I say what I mean, as translated from geek to lay terminology! Sue, I love you.

Contents

Preface

Within the "industry" most know, or have heard, that the requirements of the federal government and enforcement of information assurance have heightened in the past years. With the incorporation of the Gramm–Leach–Bliley Act (GLBA), the Sarbanes–Oxley Act (SOX), and the Clinger–Cohen Act, it seems that we have multiple requirements with a mixture of standards. To add to the confusion (as some may see it), we have Control Objectives for Information and related Technology (CoBit), Information Technology Infrastructure Library (ITIL), Microsoft Operations Framework (MOF), International Organization for Standardization (ISO), and other frameworks that our clients wish to incorporate into their infrastructures.

Business service management (BSM) holds many challenges; approaches to BSM, using each of the different platforms, are a little different than most organizations think and should remain that way by identifying the lowest common denominator, a piece of hardware or software, and applying that piece of equipment to the business model and its functions within the business. Asset management involves budgetary requirements under the ITIL, and it coexists with change, release, and configuration management, all of which require input into the management of an information technology (IT) system and cohesion with the configuration management database (CMDB) so the organization can get on track and meet the requirements of its governing headquarters.

The three operations required for effective IT management are as follows:

1. Portfolio management (PM)
2. Enterprise architecture (EA)
3. Capital planning and investment control (CPIC)

Each of these operations is an essential factor in relation to the total cost of ownership (TCO) and the management of investments within the infrastructure. Although some of these management functions are called something else, still they equate to an ITIL, MOF, CoBit, or ISO requirement or process. Regardless, following a secure model will save the organization millions of dollars in losses, damages, and the cost of rebuilding your data system infrastructure.

For those of you not aware of the requirements, they have all been part of the federal government and can be referenced at http://csrc.nist.gov. Pick your subject area, and you will discover expert levels of knowledge at your fingertips. The federal government has been doing this since the inception of the computer. Some who have been around for a while may remember the "Rainbow Series," "Common Criteria," and "Earned Value Management System"; these are all federal standards that date back to 1960 (I know, before some of you were born!). When in doubt about incorporation of someone's way of doing things in Enterprise Architecture (EA), Portfolio Management (PM), Capital Planning and Investment Control (CPIC), or Information Assurance (IA), reference the National Institute of Standards and Technology (NIST) and your level of understanding will be raised 100%.

Additional information is available from the CRC Press website: http://www.crcpress.com/product/isbn/9781439841594. This includes templates that will help document what you are doing and help management understand the importance of what "managing" is all about for the security of the enterprise. Security is more than just defining a few controls; these policies and procedures will assist you in becoming compliant with its many requirements, regardless of the industry. These templates are provided as an enhancement to the verbiage of the chapters and are just some of the many examples that you have full right to manipulate and adjust to meet your requirements. The templates

provided cover each chapter and if you follow along with the templates after or before reading a chapter, you will receive the full benefit of your reading experience.

Each process is just a means of management, operation, or some level of technical control, and with a sound foundation of security you cannot go wrong in building your infrastructure.

Acknowledgments

Thanks go to Dr. Ron Ross, Arnold Johnson, Marianne Swanson, Peggy Hines, and the rest of the great, hardworking enthusiasts at the National Institute of Standards and Technology (NIST). NIST is a part of the Department of Commerce and under executive order defines the security standards for the federal government. These standards are free, as are many of the publications I encourage you to read and to heed the requirements as best as possible. NIST develops its documents in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347. I am a miser and do not like throwing money at a problem that can be solved with some common sense, education, and a little hard work. Don't waste your stakeholder's money; you can save thousands by educating yourself and reading some of these great manuals.

Introduction

Where or when did information security become an issue? If you look at the various ages our world has evolved through, we are now in what we call the Information Age, a period in time during which we have more data that are related to almost nothing and for which we try to account. The types of data issues we are faced with include the following:

- Classifying (not in the security sense but as in filing or archiving)
- Storing
- Setting destruction standards
- Setting sensitivity standards (personally identifiable information (PII))
- Protecting
- Moving (media bandwidth)
- Controlling—who can access it
- Needless other tasks that produce nothing

And then we have the metadata and the components that accompany it.

Reading this book will not give you just a few reasons why security is foremost, but reading it and following the procedures will give you an understanding of your infrastructure and what requires further attention.

In the Information Age we have created requirements and standards that for some are hard to understand and follow—or perhaps people are just plain lazy in doing their jobs. With the recent crash of the economy, loss of jobs, fleecing of America, and corporations' continuance to destroy America by outsourcing jobs, job security does not exist. Information assurance is and will remain the future for all the "data" created. Now you have to create a new wheel on how to meet the standards and requirements for infrastructure security. A mere review of the confidentiality, integrity, and availability is not and will never be acceptable in a world that demands privacy.

Throughout this book, I will interject my opinion about various areas and my experience in dealing with customers as a consultant and how they can manipulate you to produce more than you should or expect you to overlook what is not completed or planned for the infrastructure, or is just not happening.

Studies have shown that the enactment of the Paperwork Reduction Act (44 U.S.C. 3501 et seq.) has placed more of a burden and paper requirement on the people it was designed to protect than during any other time in history, and we produce more paper documents than ever before.

After reading this book you will have the knowledge to better understand how to evaluate your network, evaluate the business model of your company, and learn how they fit together in the selection of the correct systems to support your infrastructure. You will understand how to perform a business impact analysis and a risk assessment to further develop your data security needs. Furthermore, your knowledge of the different processes of the Information Technology Infrastructure Library (ITIL), Microsoft Operations Framework (MOF), and business service management will come to light. You will understand how they are truly derivatives of a security function that is or is not in place, and you will see how you can implement the correct level of controls for the specific process. You will also have the seed to start developing your skills to better understand the 17 families of management, how they are applied, and at what level they are applied; you will know what management, operational, and technical control is and how each are implemented within your infrastructure (Figure I.1). As a final benefit of this book, you will have the tools to

IDENTIFIER	FAMILY	CLASS
CA	Security assessment and authorization	Management
PL	Planning	Management
RA	Risk assessment	Management
SA	System and services acquisition	Management
PM	**Program management**	**Management**
AT	Awareness and training	Operational
CM	Configuration management	Operational
CP	Contingency planning	Operational
IR	Incident response	Operational
MA	Maintenance	Operational
MP	Media protection	Operational
PE	Physical and environmental protection	Operational
PS	Personnel security	Operational
SI	System and information integrity	Operational
AC	Access control	Technical
AU	Audit and accountability	Technical
IA	Identification and authentication	Technical
SC	System and communications protection	Technical

Figure I.1 Eighteen security families.

document your infrastructure to feed into the continuity of operations and disaster recovery.

Although there are 18 controls listed, the PM controls information security programs (NIST SP 800-53r3, Appendix G, "Program Management (PM) Family"). This family provides security controls at the organization rather than information system level.

Okay, you want to learn about securing the network. Hopefully you can understand the requirements as well as the process of such a tedious task.

Where do I start? I recommend you begin when the company is first decided upon and the company name has been selected. You've gone to the Secretary of State and are now registered. This is a place we all want to start from, and if you are fortunate, you were given the chance to begin your tasks here. Unfortunately, most of us start in the middle and work our way to one end or the other.

There are five basic areas to think about when designing a foundation for your security program and building your infrastructure. You really don't have to start at the beginning; it just helps the downriver processes

when you know where you are. When looking at the five basic areas, you need to take into consideration each of the families of controls. As laid out previously, the controls are placed in class order and relate to the five basic areas. When you start building the foundation of your infrastructure, you need policies for everything that is done; if in doubt, write a policy. Information technology (IT) people forget about the policy and just jump right into the implementation process, building procedures as they go. This will come back to bite you when you have a compliance audit (Statement on Auditing Standards [SAS] no. 7, HIPAA, GLBA, NIST) or a restructuring phase of your infrastructure—count on it. This is especially true when dealing with database structures and software development projects. When you look at your infrastructure and what has already been accomplished, take a look at the five requirements in order and see where and how you stack up, and to what level of detail your compliance levels are. The six levels of compliance are

1. **Policy:** Applies to management buy-in and is expressed to the users.
2. **Procedure:** Pertains to the true meaning of how and why things are done this way.
3. **Implementation:** How and what plan is in place, and what documents are written.
4. **Testing:** How it works; "works fine" does not meet the criteria.
5. **Acceptance:** Does it really do what you (or they) say it should do, and does it do it efficiently and proficiently?
6. **Maintenance:** Although the maintenance phase should always be considered, I do not feel that it should be part of the compliance process, but rather a management-driven requirement to keep them involved in the security of data.

Regardless of how you lay out your project(s), have some form of logical order of events that defines each of the steps and your level of compliance with the steps. These six examples are common logical steps that take more than just the "system" into account. Enterprise architecture (EA) of all types needs to follow some template process to get from A to Z in the structure of design, management, and business services. When in doubt, improvise, adapt, and overcome!

The National Institute of Standards and Technology (NIST) is an organization within the U.S. government, under the Department of

Commerce, that has many "think tank" operators with years of experience in the enterprise architecture and security arena. The documents and processes are free and exceed those of all the other frameworks, so why develop a new wheel? I have used ITIL, Microsoft, and NIST. I always go back to NIST, not because I know it, but because it makes sense and gives you the information to design, develop, and implement a foundation that is commensurate to some of the best infrastructures in the world—you just need to stay with it and stay proactive!

Understand that the NIST "framework" is not a model but more of a practice of common sense and management by control groups and the level of responsibility for the infrastructure:

- **Management** belongs to the policy and procedures in place that dictate the way we perform functions within the architecture.
- **Operational** belongs to the way the policy and procedures are incorporated into the infrastructure and what measures are taken to ensure they work.
- **Technical** belongs to the system in which the control is implemented at the hardware or software level, a process of the hardware or the results of a software command and functions.

The certification and accreditation (C&A) process is the practical application and verification that a particular entity (government agency) has performed and met the requirements of the Federal Information Security Management Act (FISMA) by accounting for information systems, applying specific security controls, and maintaining some level of a system development life cycle (SDLC). As guides, Public Law (P.L.) 107-347 appointed NIST as a source for developing the "rules of the road" for the C&A process. Within those guidelines NIST has developed the Special Publications and Federal Information Processing Standards (FIPS) shown in Table I.1 to define and clarify the conduct of the C&A process.

Table I.1 NIST Special Publications

NIST SP 800-18	NIST SP 800-53A
NIST SP 800-30	NIST SP 800-53r3
NIST SP 800-34	NIST SP 800-60
NIST SP 800-37	NIST SP 800-128
FIPS 199/200	FIPS 140-2

There are three major factors that impact the outcome and extent of time when performing the C&A process:

1. Level of experience the provider has
2. Level of infrastructure knowledge
3. Level of cooperation provided by the client

Other factors also apply, but these three factors impart the majority of the outcomes and durations. When you look at the best practices, one must first look at the maturity level of the organization. An organization's maturity level is determined by the following five factors that are in place at the time of the evaluation:

1. Depth of policies written (what level of management buy-in is in place)
2. Level of procedures in place (determined by policy)
3. Implementation of the procedures and follow-through
4. The level of testing that has taken place to validate the procedures implemented and whether they follow policy
5. How well each of the steps is integrated into the infrastructure

Once it is determined what and how things are accomplished, a provider must look at the business model. NIST SP 800-34 defines the process of completing a business impact analysis (BIA), and this can be accomplished mentally or formally. The mental process is just a cursory review of the organization, and the provider imparts its knowledge of the organization and the NIST guidelines. For example, the Federal Bureau of Investigation (FBI) is part of the Department of Justice (DOJ), and therefore part of the executive branch of the government, which is directly governed by specific executive orders in addition to the Office of Management and Budget (OMB) and DOJ regulations and guidelines. Having background knowledge of the requirements will assist in evaluating the full business model.

Once a mental or full BIA is performed the provider can further tier the infrastructure into business units and start to draw mental boundaries of the systems. Each business unit will have certain responsibilities, and with those responsibilities the business unit is likely to have IT assets that support the unit's business model. In evaluating the business unit and adjoining IT assets, the provider should

develop boundaries. NIST SP 800-37 identifies the development of boundaries and what factors need to be considered.

In the process of what has taken place so far, a provider has worked with the client and also determined the system development life cycle (SDLC) process the client is using, if any. A mature SDLC has defined security controls (SCs) for each business system and has or is in the process of applying the controls. Additionally, the client has already determined what level of confidentiality, integrity, and availability (CIA) the system must meet, and those levels are defined as high, moderate, or low. Each level is determined through a process of evaluation using FIPS 199/200 and NIST SP 800-60.

Security controls are determined first by deciding what level of CIA the systems require and second by determining what controls are applicable to the system as prescribed in NIST SP 800-53r3.

With all the data collected, the provider must now start to evaluate the level of the facility, the security controls, and the environmental controls. Once each of the areas is reviewed and defined, the provider can start to develop the system security plan (SSP), risk assessment (RA), plan of action and milestones (POA&M), and other documents as needed for compliance with FISMA.

Most providers have or are given templates to use for the evaluation process. NIST SP 800-18 has minimum requirements for the SSP, NIST SP 800-30 and 800-39 have examples and specifics for the risk assessment, and an organization will generally have a POA&M template that is used. According to the U.S. military strategy on cyberspace (formerly secret document):

> Through the process of risk management, leaders must consider risk to U.S. interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations.
>
> Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain.

Security is a process, something that you must practice, test, implement, and audit to learn and know what results are driven from its actions. Good luck and get certified—certification is a way to express your desire and motivation of becoming a better professional. Besides, you need to be a member of the club!