EDPACS: The EDP Audit, Control, and Security Newsletter

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uedp20

Information Security Governance: A Practical Development and Implementation Approach

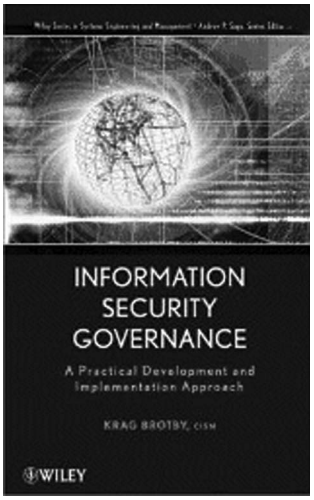
Gary Hinson

Published online: 09 Mar 2011.

To cite this article: Gary Hinson (2011) Information Security Governance: A Practical Development and Implementation Approach, EDPACS: The EDP Audit, Control, and Security Newsletter, 43:2, 15-17, DOI: 10.1080/07366981.2011.560055

To link to this article: http://dx.doi.org/10.1080/07366981.2011.560055

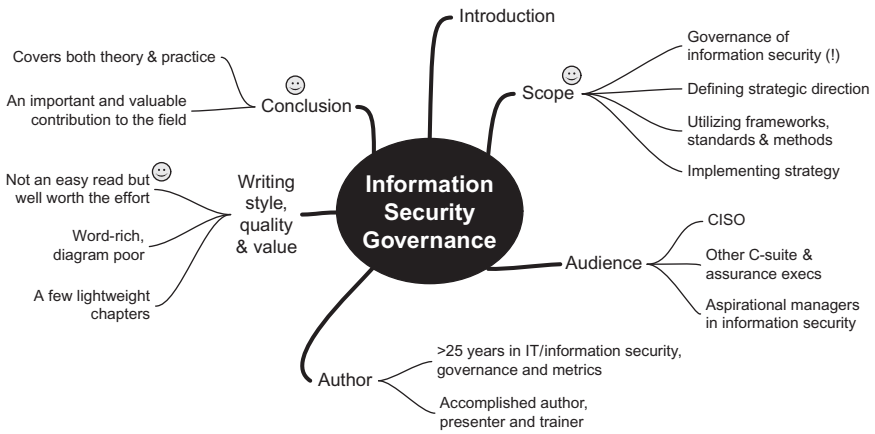
Book Review



INFORMATION SECURITY GOVERNANCE: A PRACTICAL DEVELOPMENT AND IMPLEMENTATION APPROACH

Author: Krag Brotby
ISBN: 978-0-470-13118-3
Publisher: Wiley (2010)
189 pages
Reviewed by Gary Hinson

SUMMARY



INTRODUCTION

The author introduces his book with this eloquent paragraph:

[F]or most organizations, failure to implement effective information security governance will result in the continued chaotic, increasingly expensive, and marginally effective firefighting mode of operation typical of most security departments today. Tactical point solutions will continue to be deployed, and effective administration of assurance functions will have no impetus and remain merely a concept in the typically fragmented multitude of "assurance-" and security-related stovepipes. Allocation of security resources is likely to remain haphazard and unrelated to risks and impacts as well as to cost-effectiveness. Breaches and losses will continue to grow and regulatory compliance will be more costly to address. It is clear that senior management will increasingly be seen as responsible and legally liable for failing the requirements of

due care and diligence. Customers will demand greater care and, failing to get it, will vote with their feet, and the correlation between security, customer satisfaction, and business success will become increasingly obvious and reflected in share value.

If that litany of issues does not ring lots of bells and is not enough to persuade you that information security governance is an important topic for senior managers, then frankly you are part of the very problem this book addresses.

SCOPE, STRUCTURE, AND COVERAGE

While inevitably introducing related aspects such as general/corporate governance and management, information, risk and information security management, and IT security operations, the book's prime focus is firmly on the governance of information security. A rational process for determining the strategy and defining desirable outcomes and strategic objectives for information security runs like a center-line from start to finish. The "practical implementation" element of the title is exemplified by fairly detailed coverage of information security metrics.

The first six to eight chapters of the book provide the context and introduction, with the remainder offering more practical guidance.

ABOUT THE AUTHOR

Krag Brotby, CISM, CGEIT, is a knowledgeable information security consultant with more than two decades' information security management experience in big-name companies. This gives real depth to the content. Krag has written and maintained the CISM review manual since 2005, and teaches workshop courses on CISM, governance, metrics, and related topics.

AUDIENCE

This is an advanced management topic of direct concern to senior information security, risk management, and related assurance professionals. Although unfortunately only chief information security officer (CISOs) and chief information officers (CIOs) may be prepared to set aside the time needed to really study a book of this depth, it is equally valuable for all C-suite executive managers and board members with a genuine interest in aligning information security with other business objectives. Junior managers may also benefit from this book in terms of their personal and career development: truly appreciating the difference between tactical and strategic levels, for example, is helpful when attempting to draw senior management's attention to information security issues.

WRITING STYLE, QUALITY, UTILITY, AND VALUE

Krag writes clearly and well but, as noted earlier, this is an advanced topic that requires effort to read, comprehend, and consider the subject matter. It helps if the reader is already familiar with standards frameworks or approaches such as Sherwood Applied Business Security Architecture (SABSA), ISO/IEC 27000 family of

standards (ISO27k), Cabability Maturity Model (CMM), and Control OBjectives for Information and related Technology (COBIT) but these are introduced and explained in enough detail to be meaningful in any case.

There are a few duplicated paragraphs and lists, but thankfully not many spelling/grammatical errors or annoying turns of phrase to distract the reader. I personally would have preferred more diagrams, particularly to help explain the broad conceptual aspects, contexts, and linkages.

The depth of coverage is inconsistent with a couple of the chapters, including the conclusion, being surprisingly short. Chapter three on legal and regulatory requirements, for instance, is just over three pages long, although compliance is undoubtedly an important governance issue and, unfortunately, a major strategic driver in this field. To be fair, most of the laws, regulations, and standards are self-explanatory and there are hundreds, maybe thousands, of them across the globe so there would be little point in going through them in detail here. However, I feel three pages does not do justice to the amount of effort the CISO is likely to expend in practice, both directly in fulfilling information security compliance obligations, and indirectly in supporting the compliance burden on other parts of the organization through information security controls.

CONCLUSION

As with Krag's complementary book on security metrics, *Information Security Governance* confidently covers challenging material on a subject that many find hard even to describe, let alone understand. The effort needed to read and learn from this book pays off through a better appreciation of both the theoretical background and the practical steps needed to design, develop, implement, and manage— or govern—information security at the strategic level.

If you are tasked with preparing, reviewing, or approving information security strategies and policies, or if you have governance or management responsibilities in this area, this book will help you make practical sense of the confusing morass of advice regarding governance. It's the kind of book that grows on you, becoming more valuable over time as you pick up experience and find yourself in ever more challenging situations.

Dr. Gary Hinson, Ph.D., MBA, CISSP, is an information security specialist with a particular interest in the human aspects. Gary's career stretches back to the mid-1980s as a practitioner, manager, and consultant in the fields of IT system administration, information security, and IT auditing. Gary runs the information security awareness service NoticeBored and spends his days writing creative security awareness materials for subscribers. By night, Gary is a passionate supporter of the ISO/IEC 27000-series "ISO27k" information security management standards. Visit his website ISO27001security.com for ISO27k information, guidance, and tools.