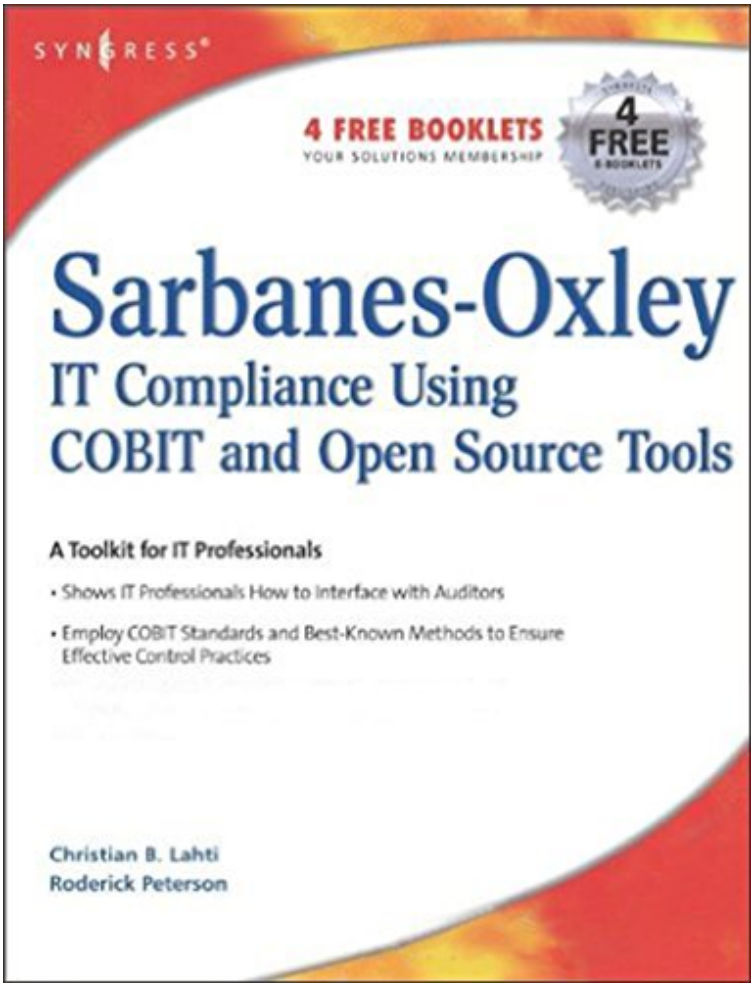
Sarbanes-Oxley Compliance Using COBIT and Open Source Tools

Christian B Lahti, Roderick Peterson
*ePub | *DOC | audiobook | ebooks | Download PDF*



#3134152 in eBooks 2005-10-07 2005-10-07File Name: B00CLC3U3E | File size: 26.Mb

Christian B Lahti, Roderick Peterson : Sarbanes-Oxley Compliance Using COBIT and Open Source Tools before purchasing it in order to gage whether or not it would be worth my time, and all praised Sarbanes-Oxley Compliance Using COBIT and Open Source Tools:

8 of 8 people found the following review helpful. Very helpful introduction to SOX compliance through COBITBy Richard BejtlichI read Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools (SOICUCAOST) to learn more about compliance issues. I am a security engineer who thankfully has not had to suffer through a SOX audit. I am glad I read SOICUCAOST, however. The book is clear, well-written, and makes innovative use of a live CD. While the book is not the answer to SOX compliance (no book is), small-to-medium-sized businesses will find SOICUCAOST a valuable guide.I found SOICUCAOST's advice to be surprisingly candid. This is no "SOX is awesome" book. On p 276 we read "one could conclude that not only is there no realistic way to calculate ROI for SOX compliance, but if there were, there would be no positive ROI for SOX. The value of SOX compliance is qualitative and not quantitative. If there is no way to justify SOX compliance, how do I answer questions about how

my company's compliance activities affect the bottom line? By shifting the ROI from SOX and the cost savings to open source and cost avoidance... a decision point of whether to comply with SOX or not does not exist." That is only one dose of brutal honesty -- there are many others in this book.I thought the XFLD-based live CD was an innovative touch. Assuming one can get it to work (I had no trouble), it is a slick way to use a portal for two fictitious companies created to demonstrate ways to achieve IT-related SOX compliance. Not every component works, but using the live CD gets the reader to think he or she may be doing SOX activities instead of reading a book about it.As far as specific open source tools goes, I don't think it's realistic to be able to use tools based on the information in this book. Syngress published an entire book on Nagios, an entire book on host-based integrity monitoring, an entire book on Snort, and so on. I would have preferred to see SOICUCAOST spend more time on presenting options with advantages and disadvantages for each. I also though the idea of running Snort from a live CD as a production sensor (Ch 6) to be very ill-conceived.Regarding the reviews -- I am surprised to see they are all over the map. I think Christopher Byrne makes a few good points, but his criticism doesn't warrant a one-star review. Author Roderick Peterson should not have written a five-star "rebuttal". Authors write books, not reviews of their own books. That's poor form and it manipulates 's star ratings.Overall, I think SOICUCAOST is helpful for any SMB staring at SOX compliance. It certainly provides plenty of sound guidance, solid frameworks, and examples (on the live CD). The book is well-written and organized. I think some of the material could have been formatted for easier reading; Syngress has a tendency to use fonts that are way too large and thereby distracting. Still, I recommend anyone involved with IT-related SOX issues and/or COBIT give SOICUCAOST a try.15 of 15 people found the following review helpful. Two books in oneBy Stephen NorthcuttThis is the hardest review I have ever written. The book has enormous potential. The concepts behind the book can probably save organizations a lot of money. The book is a primer to COBIT, which is the model most people use to implement Sarbanes-Oxley. It is also a book about open source tools that may be able to support a COBIT framework.As a pointer to tools and ideas, you cannot beat this book. However, if you are not already a part of the Linux open source world, I don't think this book can get you there. I had trouble with the CD and had to use a Knoppix cheat code to get it to boot. In addition, the examples on the CD are not populated with enough data to let you play with the tools.The bottom line, I think this has all the earmarks to become a really important book in the auditing and compliance world in its next edition. I have purchased a copy for every one of my students in my management class and I am flying the authors out to demonstrate the tools to my class. I honestly don't think you can afford to miss this book if you have responsibility for Sarbanes-Oxley or GLBA for that matter. However, you are going to have to find a Linux geek to actually put any of this into practice.0 of 0 people found the following review helpful. Open Source Compliance Using CobiTBy Kenny McNees, CPA, CISSP, CISA, CAP, CISMThis book is a winner. It is clever, and fresh, and offers some really great concepts and ideas for companies needing to, or wanting to (yes there is such a thing), comply with SOX. Also, I really like the open source 'tool kit' that they provide, and being a big fan of CobiT, and Linux, I was a pretty easy sell. Note: I got the CD to run without any problems at all, but perhaps I got a later 'bugless' version.I guess my only reservations about the book are its target audience. Frankly, I can't see a bunch of deep pocket corporations with millions on the line if they come up short in the SOX compliance department, worrying too much about saving $50K on some (admittedly pretty cool) compliance tools. However, I do think that the ideas presented would certainly apply to the mid-caps and small-caps who are perhaps looking to seriously reduce compliance costs, and also speed up the documentation (read: collaborative documentation) required of SOX.I would also point out that COSO - the primary framework endorsed by the SEC for (financial) internal controls - and CobiT - the framework primarily endorsed by the book - can live happily ever after. Since this book approaches SOX compliance from the IT perspective, I find this totally logical, consistent, and practical. I only raise it because some would probably wonder were COSO fits into all this.I would have rated the book 5 stars, but I think it got bogged down a little in the technical, and would leave your typical SOX enthusiast nodding off and reaching for the remote. Being part geek myself - I rather enjoyed the excellent technical dissertations.The book is clever. The approach is smart, original and timely. It would definitely work for small and mid caps. And those iPod toting, Wikipedia GenXers you have helping out on SOX, would take to it like Frisbees to a frat house.

This book illustrates the many Open Source cost savings opportunities available to companies seeking Sarbanes-Oxley compliance. It also provides examples of the Open Source infrastructure components that can and should be made compliant. In addition, the book clearly documents which Open Source tools you should consider using in the journey towards compliance. Although many books and reference material have been authored on the financial and business side of Sox compliance, very little material is available that directly address the information technology considerations, even less so on how Open Source fits into that discussion.Each chapter begins with an analysis of the business and technical ramifications of Sarbanes-Oxley as regards to topics covered before moving into the detailed instructions on the use of the various Open Source applications and tools relating to the compliance objectives.Shows companies how to use Open Source tools to achieve SOX compliance, which dramatically lowers the cost of using proprietary, commercial applicationsOnly SOX compliance book specifically detailing steps to achieve SOX compliance for IT Professionals

From the Back CoverThis book illustrates the many Open Source cost savings opportunities available to companies seeking Sarbanes-Oxley compliance. It also provides examples of the Open Source infrastructure components that can and should be made compliant. In addition, the book clearly documents which Open Source tools you should consider using in the journey towards compliance. Although many books and reference material have been authored on the financial and business side of Sox compliance, very little material is available that directly address the information technology considerations, even less so on how Open Source fits into that discussion.Each chapter begins with an analysis of the business and technical ramifications of Sarbanes-Oxley as regards to topics covered before moving into the detailed instructions on the use of the various Open Source applications and tools relating to the compliance objectives. The bootable CD contains fully configured demonstrations of Open Source tools.About the AuthorChristian Lahti is a computer services consultant and an expert in security. He is a regular speaker at industry shows such as LinuxWorld and OSCON. He is the technical editor of Windows to Linux Migration Toolkit (Syngress, ISBN: 1931836396).Roderick Peterson is the Information Technology Director at NeoMagic. He has more than 20 yeras' experience in the IT industry and has successfully led the development and deployment of major applications at several global companies.