AHIA FINDINGS

Book Review
Network Auditing:
A Control Assessment Approach

Gail Hormats, CISA, CIA

CONDUCTING A NETWORK AUDIT? HIRE AN EXPERT.

BOOK DESIGNED FOR CONSULTING FIRM RATHER THAN INTERNAL AUDIT SHOP!

Let me begin by quoting from a seminar description offered by the Greater Hartford Chapter of the Information Systems Audit and Control Association: "Performing a security assessment (aka vulnerability assessment or penetration test) against a network environment requires preparation, the right tools, methodology, knowledge, and more..." Let me add that the more very much includes experience. A network audit is not the type of audit someone unfamiliar with the technology should perform. If you are not previously experienced in the area and you need to have a network audit, hire the expertise and get trained; if you are experienced, you probably will be disappointed in this book. I was.

In slightly more than 250 pages, ***Network Auditing*** by Gordon Smith introduces you to the layers and technologies involved in understanding networks. He begins with the communications layer, moves through the hardware layer (circuits), dwells on hardening (tightening security) your NT and UNIX environments, and ends with a discussion on disaster planning and management reporting. Sounds helpful, doesn't it? Well, the truth is, if you know only a little bit about networks and use this book as your audit program, you will likely get into trouble, and if you already know a lot about networks, you don't need this book. If you know nothing about this field, it will provide some useful information; however too many assumptions are made about the reader's understanding of the technical jargon to be helpful for a novice.

Network Auditing was published in 1999, and given the time it takes a book to reach publication, we can surmise the material was written in 1997 or 1998. The technology Mr. Smith discusses is therefore five or more years old. The older technology is still with us – UNIX is still UNIX – although there are many new flavors; Microsoft NT is still NT, again with several different releases. However, Microsoft 2000, Linux, and other new technologies such as wireless networks and Virtual Private Networks (VPNs) are either not addressed or only minimally addressed. For example, there is only one paragraph on wireless technology which boils down to "it needs to be encrypted". As a result of being so dated, the text is unable to discuss more recent developments in the various methods for securing newer technologies.

My second disappointment is with the inconsistent formatting throughout the book. The first chapter, which provides an overview of networks ends with a Telecommunications Glossary–which includes general network terminology as well as telecommunications specific definitions. This is the first, and only time the author defines technical terms in an organized fashion. For the novice reader, glossaries at the end of each chapter would be helpful; for the advanced reader, this one glossary is unlikely to provide new knowledge.

At the end of each chapter the book provides risk-control summaries, an audit program, and a checklist, each of which is also included on the accompanying CD. The information in the risk-control summary is not always discussed in the chapter, as a reader might expect. Also, the checklists are also apparently used to pad the book, being repeated in the 76 page appendix, as well as appearing in each chapter. Furthermore, some of the recommended controls – such as performing a penetration test quarterly- are not feasible in the real world. As we all know there are limited audit

Networking, continued on page 54

Coding Compliance, continued from page 52

used as a checklist to ensure you are covering all necessary steps in your audit program as well as keeping the auditor within the scope of the coding audit. This book does not give the reader a good handle on the differences between conducting an inpatient vs. an outpatient-coding audit. It would have been helpful to list out the data elements that are required for an outpatient coding audit and identify the trends an auditor might expect to see to help begin the correction process at that facility.

The chapter on Formal Audit Reporting has suggestions on how to tailor your reports to your audience. This section provides a nice analysis of the various parties that may need to know about the audit and the type of information that should be included on various parties' reports. The examples provide the reader with enough information to use to create your own report to the board of directors, medical staff, the clinical department, physicians, senior management, financial management, health information management, coders and patient accounting. The chapter concludes with information on how providers could disclose irregularities found with their coding for Medicare and Medicaid. Self-disclosure should have been a separate chapter that goes into detail on why a provider may disclose irregularities. In addition, examples should be given on situations where self-disclosure has occurred and the type of violations that were associated with not complying with regulations. The authors did indicate a facility wanting to self-disclose should perhaps seek the advice of legal counsel; however examples of when seeking legal counsel is appropriate was not provided to the reader.

The final chapter deals with how to conduct follow-up once a coding audit has been completed. The authors identify the audit follow-up to be conducted in three phases. Audit follow-up is simply the time when deficiencies in the audit conducted are corrected. The first phase typically is when dealing with any significant (high risk) concerns. The high-risk issues are usually addressed immediately after identifying the issues. The second phase that Russo and Russo identify is the long-term follow-up; this is when the issues are of a lower risk and take one to three months to address. The final phase discussed is the pre-planning phase. The authors describe this phase as gathering all data from the audit and using it to help create your scope for the next audit. This chapter describes the phases in detail and can help an auditor identify what type of issues would fall into the various phases. In addition, good examples are provided on how to address significant coding concerns and the criteria one should be looking at to resolve the audit issues.

Overall, this book is a good, though basic, reference guide to conducting a coding audit. The sample forms, reports and tools provided in the book are very clear and helpful for anyone to use. Unfortunately, there were several areas where I wished the authors would have given more explanation or more examples to reference outpatient coding audits instead of focusing solely on inpatient coding audits. Although some areas of the book were not as detailed as I would have hoped, the authors do provide additional resources where one could be provided with more information on topics covered lightly in this book.

This book is published by HCPro and is available at the following web sites www.hcpro.com, www.hcmarketplace.com, www.hminfo.com and www.compliance.com or by calling 1-800-650-6787 or 781-639-1872. ▪

Pooja Walia, CPC, is Manager of Internal Audit at the Alexian Brothers Health System in Elk Grove Village, Illinois. She can be reached at waliap@alexian.net.

Networking,continued from page 53

resources available that must be spent on the highest risk areas. If the skills exist in-house to perform penetration testing, those skills are also valuable for other technical audits; if the skills do not exist in-house, the cost of this control performed at the recommended frequency may not be justified.

The audit program and checklists provided at the end of each chapter are feasible and potentially helpful. The caveat of course is to answer the following question - Do the skills to perform the audit exist within the department? If they do, the auditor can use the program and the checklists to validate any audit programs already developed. If the skills are not available in the department, these programs can be dangerous. A network audit (actually any audit) should not be performed by rote, i.e. simply following the outlined steps. IIA standard 1210 Proficiency and ISACA standard 040 Competence both require that the auditor should have the skills, competency, and knowledge to perform an audit.

To summarize: Caveat Emptor. You get what you pay for. There are better, more recent books on network security if you need to understand the technology; otherwise, if this is beyond your concern, look into hiring an external audit firm to perform such audits. As well, the auditing approach outlined in the book, in my opinion, is better designed for a consulting firm than for an internal audit shop. Simply put, there are more constructive ways to use the $25-50 the book will cost you. ▪

Gail Hormats, CISA, CIA, has more than 16 years experience in business process redesign, medical billing audits, information system audits, and operational internal audit. She is Project Leader for Baystate Audit Services in Springfield, MA. She can be reached at gail.hormats@bhs.org.