Auditing is not, at first appearance, an exciting topic. So why would anyone volunteer to spend months of effort writing a booklet that may never be read? Well, for a real answer, we have to look beyond the simple, well-known notion of the security audit.

Auditing is about the rigorous examination of a system, the identification of any shortfalls in compliance or practices, and the organised repair and improvement of that system. It is about ensuring that appropriate controls and processes are in place, and that staff are able to perform their jobs with appropriate training, resources and support.

Auditing is a very important tool for technical communities such as system administrators to have at their disposal. It can help them gain a better appreciation of the surrounding context of their actions and the impact of the changes they are planning. It allows them to step out of the day-to-day mire of problems, to see the wood for the trees, and to plot the path forward.

It is also a system administrator’s most valuable tool in convincing management that there is a problem that needs addressing or a subsystem that needs improvement. It is your most strategic way to show management the true nature of what it is you do for a living, and how much effort is involved in doing that job well.

Most important, auditing should be your tool. It should not be seen as some biannual chore inflicted upon you from above. It should be the tool you call on to help you in understanding complex systems and in implementing change, including enlisting necessary support from management.

A Personal Perspective

I have been a consulting system administrator for over ten years. In that time, I have moved from site to site, cleaning up the mess of generations of decay. Each time I encountered the same problem: how do I determine what sort of mess I’m dealing with, and how do I fix that mess? Like many of my peers, as my first step I built up a toolkit of scripts and utilities of my own and from the Internet to help me.

Systems administration is a very young profession. Each of us builds up our own toolkits and procedures, and this leads to the great hidden cost of staff turnover; every system administrator re-creates each site they administer in their own image—one that they are comfortable with. This is a major source of the very entropy that we seek to conquer. It is clear that we, as a profession, need to work towards a common, well-defined framework and set of standards of practice. But that’s another story.

As a consultant newly encountering a site with a prior history of consultant-instigated changes, I had a major task ahead of me of a non-technical nature: I had to con-
vince management that the changes I was proposing were necessary. Actually, that’s not quite correct. They were usually already feeling the effect of decay on their operations in the form of reduced system and application availability. The problem was really to convince them that there was a solid basis for believing that the changes I was proposing would actually improve things. (After a couple of generations of consultants making such promises, people become a little suspicious of such claims.)

What I discovered was that the audit, if done correctly, is a system administrator’s most valuable tool in dealing with management. Indeed, the only reason I initially undertook a formal audit was for management’s sake. Since then, I have performed a variety of audits of varying complexity and breadth of coverage. Each one of those has been vital to obtaining organisational commitment to change.

Over time, my original questions have become slightly more refined: how do I quantify the degree of entropy, and how much effort is required to repair the practices of the site? These are subtly different questions.

The audit is the starting point for technical improvement works. It quantifies how much effort (and money) is going to be required to improve things, raises management’s awareness of the complexity of the systems administration role, and allows both the system administrator and management to review progress against agreed goals.

Goals of This Booklet

As should become clear, this is not another text on auditing computers by an auditor. Nor is it intended to replace the use of properly trained auditors. This booklet is directed towards the systems administration community, and it focuses on helping to bridge the gaps in understanding between that community and those with whom it interacts.

Reading this booklet will not make you an auditor. Those interested in becoming an auditor should consult one of the resources mentioned in Appendix B.

It should, however, help you and professionals from similar technical communities to conduct audits of varying degrees of formality, and to understand and use formal techniques to assist you in your role. It should especially help you in proactively planning your workload and in communicating with other key business communities. It should also provide a better understanding of the role and importance of auditing and, hence, better equip you to facilitate any external auditor so that both you and your organisation reap the maximum benefit.

The audit is your friend. If done right, it will get you a direct line to your manager’s ear, with positive effects throughout the organisation.

My goal in writing this booklet is to help you, the system administrator, to harness the power that an audit provides.

Acknowledgments

I would like to thank a number of people for their help in bringing this text to fruition. Thanks go to Hal Miller, who forced me to write this thing in the first place.
Thanks also to Anton Aylward, Mark Teicher, Bret Watson, Richard Dempsey, Gordon Rowell and Mike Ciavarella for their comments on the text at various stages.

Finally, a special thanks to Bill LeFebvre for his work in shepherding this text through the editorial process, and for pushing me to completion, if on a somewhat expanded timeframe than originally planned.

An Apology

My apologies to any non-U.S. readers. This booklet was written in English. Any Americanisation of the text occurred during the editing stage.