

# 6

*Short Topics in*  
**Systems Administration**

---

*Edited by William LeFebvre*

**A System  
Administrator's Guide  
to Auditing**

*Geoff Halprin*

©Copyright 2000 by Geoff Halprin  
ISBN 1-880446-21-9

To purchase additional copies and for membership information, contact:

The USENIX Association  
2560 Ninth Street, Suite 215  
Berkeley, CA USA 94710  
Email: [office@sage.org](mailto:office@sage.org)  
Web: <http://www.sage.org>

First Printing July 2000

USENIX and SAGE are registered trademarks of the USENIX Association.  
USENIX acknowledges all trademarks herein.

Printed in the United States of America, on 50% recycled paper, 10–15%  
post-consumer waste.



# Contents

<b>Foreword by William LeFebvre</b>	v
<b>Glossary</b>	vi
<b>Preface</b>	vii
<i>A Personal Perspective</i>	vii
<i>Goals of This Booklet</i>	viii
<i>Acknowledgments</i>	viii
<i>An Apology</i>	ix
<b>1. Introduction</b>	1
<i>Why Audit?</i>	1
<i>Three Audit Perspectives</i>	2
<i>Auditing as an Agent for Positive Change</i>	4
<b>2. What Is an Audit?</b>	5
<i>Assessments and Audits</i>	5
<i>When Is an Audit Not an Audit?</i>	6
<i>Technology Audits—The Never-Ending Story</i>	6
<i>Security Audits</i>	7
<i>Beyond Security Audits</i>	9
<i>When to Audit</i>	11
<i>How Often Should Audits Be Performed?</i>	13
<i>Who Should Perform the Audit?</i>	13
<i>The Politics of an Audit</i>	15
<b>3. Audit Concepts and Principles</b>	17
<i>The Baseline</i>	17
<i>Evidence</i>	17
<i>Some Audit Principles</i>	18
<b>4. The Context of an Audit</b>	20
<i>Assessment and Repair</i>	20
<i>The Audit Process</i>	21
<i>The Body of Knowledge</i>	21
<i>Controlled Improvement Programmes</i>	22

<b>5. The Audit Process</b>	23
<i>The Audit Time Line</i>	23
<i>Distribution of Effort</i>	24
<b>6. How to Perform an Audit</b>	25
<i>Step 1: Familiarisation</i>	25
<i>Step 2: Agreement</i>	26
<i>Step 3: Inspection and Evaluation</i>	27
<i>Step 4: Preliminary Assessment</i>	28
<i>Iterate</i>	29
<i>Step 5: Reporting</i>	29
<i>So, What Are We Looking For?</i>	29
<b>7. Interviews</b>	31
<i>The Familiarisation Interview</i>	31
<i>The First-Round Interviews</i>	31
<i>Subsequent Interviews</i>	32
<i>Interview Techniques</i>	32
<i>Who to Interview?</i>	32
<b>8. System Inspections</b>	34
<i>Active Versus Passive</i>	34
<i>Automated Probes</i>	35
<i>Data Storage and Security</i>	36
<b>9. The Audit Report</b>	37
<i>Know Your Audience</i>	37
<i>A Walk Through an Audit Report</i>	38
<b>10. Assessment Criteria</b>	44
<i>Rating Systems</i>	44
<i>Categories and Weightings</i>	45
<i>Showstoppers</i>	46
<b>11. Controlled Improvement Programmes</b>	47
<i>Step 1—Study</i>	47
<i>Step 2—Plan</i>	49
<i>Step 3—Authorisation</i>	49
<i>Step 4—Controlled Repair</i>	50
<i>Step 5—Evaluate (Re-Audit and Review)</i>	50
<b>Appendix A. System Inspection Checklists</b>	51
<b>Appendix B. Audit Resources</b>	53
<b>Bibliography</b>	54