



THE UNIX[®] AUDIT

***Using UNIX to
Audit UNIX***



Michael G. Grottola



2-005-562-1

The UNIX Audit

Using UNIX to Audit UNIX

Michael G. Grottola

McGraw-Hill, Inc.

New York San Francisco Washington, D.C. Auckland Bogotá
Caracas Lisbon London Madrid Mexico City Milan
Montreal New Delhi San Juan Singapore
Sydney Tokyo Toronto

Contents

Introduction	xi
--------------	----

Chapter 1. Audit Basics

Why Audit?	1
UNIX in Particular	2
The Right Approach	4
Audit Preplanning	5
Not All Audits Are the Same	6
The Right Audit at the Right Time	6
Audit Roles	8
System Owner	8
Applications Users	9
MIS Users	9
Auditor	10
The Bigger Audit Picture	10

Chapter 2. Audit Plan Deliverable

Design the Report First	13
Executive Report Details	15
Audit Abstract	15
Action Items	17
Management Report Details	19
Methodology	19
Findings	21
Conclusions	21

Chapter 3. Prerequisites

UNIX File Structure	24
UNIX Commands	25
Commands Organized by Use	25
Alphabetical Reference	27

Chapter 4. Audit Baseline	43
Creating a Baseline	44
Overview of the Creation Process	44
Resource Administration Files	44
Application Usage	44
Production History	45
Details of Baseline Creation	45
System Resource Files	45
Recording Information	55
Application Usage	63
Software	63
Data	64
Configuration Information	64
Recording Information	64
Production History	65
System Logs	65
Procedures	65
Recording Information	65
Saving the Baseline	66
 Chapter 5. Audit Previews	 67
The Management Meeting	67
User Interviews	68
Application Users	68
Technical Users	70
System Users	70
Document Review	71
Original Purchase and Installation	71
Subsequent Documentation	73
Conducting the Right Audit	75
Audit Response	75
Assessing Audit Resources	75
Prior Audit History	75
Personnel	76
Status Meeting	76
Examination Directives	76
 Chapter 6. Capture and Examine	 77
The Tools	77
Programs	78
Files	81
Procedures	84
File System Examination	88
Security	88
Resources	94
Usage	95

Chapter 7. System Response	97
Signs	97
Causes and Remedies	98
UNIX Accounting	98
UNIX Accounting Reports	99
System Activity Reports (SARs)	102
Inadequate Hardware Resources	102
Compromising Software	103
Hidden Interrupts	103
Poor Resource Planning	103
 Chapter 8. Delivering the Audit	 105
The Reports	105
The Executive Report	106
The Management Report	106
Verbal Reports	106
Different Audits	106
Upgrade audits	107
Emergency audit	109
Methodology of the Emergency Audit	111
Phase 1	111
Phase 2 If There Was a Previous Audit	112
Phase 2 If There Was No Previous Audit	113
Typical Outcomes	118
Cost and Benefits	118
Likely Next Steps	119
If the Resources Are Different	119
Proceed with Caution	120
 Chapter 9. Forms for the Management Report	 121
Request for Proposal Audit Form	122
System Proposal Audit Form	123
Vendor Quotation Audit Form	124
Product Receipt and Warranty Audit Form	127
Software License and Support Audit Form	130
Hardware Maintenance and Support Audit Form	133
Application User Interview Audit Form	136
Technical User Interview Addendum	138
System User Interview Addendum	139
 Appendix A. Program Listings	 141
 Appendix B. TLIST Contents	 153

Appendix C. Reports Generated by Shell Programs	155
Appendix D. Example of Sizing Template	157
Appendix E. Audit-Type Decision Flowchart	163
Index	167
About the Author	175