

IT Auditing: Assuring Information Assets Protection



Robert E. Davis, MBA, CISA, CICA

(C) 2008 ROBERT E. DAVIS. 6513 CREEKRUN DRIVE. RICHMOND, VA 23234. ALL RIGHTS RESERVED

Preface

Objectives

“IT Auditing: Assuring Information Assets Protection” was written to create training material enabling auditing, governance, risk and compliance practitioners quality subject matter details for audits and reviews. Hopefully, the stated objective is accomplished to the satisfaction of those who decided to utilize this publication.

This publication is one in a series of titles addressing information security governance, asset protection risks, and security compliance. In contrast with other publications in this series addressing information security assurance, this publication contributes researchable supporting coverage of key information assets protection disciplines as well as functional knowledge of Government-Entity-Audit convergences.

“IT Auditing: Assuring Information Assets Protection” provides a proven approach to assessing IT security frameworks, architectures, methods, and techniques. In terms of content, this publication converts selected audit standards and guidelines into practical applications using detailed examples and vivid graphics. This publication also allows auditors and security professionals to understand various steps and processes required to adequately initiate, document, and compile information assets protection audit or review phases. Through this publication, auditors and security professionals will acquire an appreciation for the complexities associated with assuring information security programs.

“IT Auditing: Assuring Information Assets Protection” can function as a study guide for CISA or CISM examination preparation as well as an audit or security practice reference manual.

Organization of Publication

This publication is divided into three parts.

Part 1, **Information Security Laws and Regulations**, provides general knowledge regarding fiduciary relationships, fiduciary responsibilities, multiple compliance requirements, as well as legal compliance audit practice areas.

Part 2, **Information Security Governance**, contains four chapters detailing framing information assets protection, control environment influencers, security management processes, and entity employee responsibilities. As a particular, information security management essential concepts and standard practices are presented for enabling entity-centric design, deployment and maintenance of a cohesive suite of processes and systems to effectively provide information assets protection that minimizes information security risks.

Part 3, **IT Audits and Reviews**, provides five generally accepted audit or review process phases: planning, studying and evaluating controls, testing and evaluating controls, reporting, and follow-up. These phases are utilized for explaining information assets protection assurance focus area procedures.

Each chapter contains a bibliography and footnotes of material discussed. Most of this publication's bibliographies are delineated by major sections discussed in the chapter. Furthermore, throughout the publication, statements are cross referenced to footnotes. For instance, "...verifies digital certificates;¹⁹⁹" means that this specific statement references item 199 of the chapter's footnotes utilizing the Chicago literary research style for supporting subject material as well as commentary.

Related Material

As training companions, Pleier Corporation offers *IT Auditing: Information Assets Protection* as well as *IT Auditing: Information Security Governance* -- consisting of PowerPoint slides, Participant's Guides and Administrator's Guides -- for enhancing knowledge regarding information security dynamics. The PowerPoint slides associated with these publications are organized to provide initial training of potential IT auditors and information security professionals as well as continuing training of auditors, security professionals, audit managers, or security managers. Utilizing the PowerPoint slides, in conjunction with the Participant's Guides, can ensure adequate understanding of subject matter audit and review engagement requirements. Furthermore, participant attentiveness to the material and completion of the knowledge diagnostics in the guides can enhance audit or security professionalism in corresponding job responsibilities. Lastly, the Administrator's Guides provides tools to lead audit and/or security training in a group setting. During self-study situations, the Administrator's Guides present researched answers to questions posed in the Participant's Guides for maximum training effectiveness.

Other similarly formatted Pleier Corporation publications - details available at www.pleier.com - include:

IT Auditing: An Adaptive Process
IT Auditing: Irregular and Illegal Acts
IT Auditing: IT Governance
IT Auditing: IT Service Delivery and Support
IT Auditing: The Process

To enhance certification candidate preparation, Boson Software offers practice tests traversing ISACA CISA and CISM examination domains. These practice tests are excellent knowledge diagnostic and test simulation tools, furnishing a variety of question formats for the purchaser. Lastly, the practice tests are customizable, therefore, allowing selected CISA or CISM domain study.

Disclaimer

Robert E. Davis (the “Owner”) and Pleier Corporation (“Publisher”) have designed and created this publication -- titled *IT Auditing: Assuring Information Assets Protection* (the “Work”) -- primarily as a training resource. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, practicing IT auditors and information security professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or IT environment. Furthermore, the information in the Work is not intended as legal advice. Therefore, many of the questions raised by the statutes cited will require careful analysis by legal counsel. This may be particularly true with regards to lawful consent.

Table of Contents

Part I

Chapter 1: Information Security Laws & Regulations	9
1.0 Introduction	10
1.1.0 Government-Entity Convergence	12
1.1.1 Fiduciary Relationships	14
1.1.2 Fiduciary Responsibilities	15
1.2.0 Multiple Legal Requirements	17
1.2.1 Security, Privacy, and Intellectual Property Edicts	22
1.2.2 Preserving Electronically Encoded Evidence	25
1.3.0 Government-Audit Convergence	28
1.3.1 Audit Practice Areas	30
Appendix A Selected IAP Related Governance Initiatives	36
Appendix B Laws & Regulations – IAP Templates	39
Chapter 1 Knowledge Check	40
Bibliography for Chapter 1	41

Part 2

Chapter 2: Information Security Governance	46
2.0 Introduction	47
2.1.0 Framing ISG	48
2.2.0 Program Development and Deployment	56
2.2.1 Responsibilities Separation	63
2.2.2 Information Assets Protection	64
2.2.3 ISG Managerial Aids	66
2.3.0 Entity-Audit Convergence	68
Chapter 2 Knowledge Check	72
Bibliography for Chapter 2	73

Chapter 3: Control Environment	76
3.0 Introduction	77
3.1.0 Entity-centric Considerations	78
3.2.0 Risk Determinants	82
3.2.1 Entity-level Policies	82
3.2.2 Managerial Practices	86
Chapter 3 Knowledge Check	88
Bibliography for Chapter 3	89
Chapter 4: IAP Management	91
4.0 Introduction	92
4.1.0 Planning	94
4.1.1 Control Objectives Selection	96
4.1.2 Control Goals Selection	101
4.1.3 Risk Management	102
4.2.0 Organizing	133
4.3.0 Coordinating	134
4.4.0 Directing	135
4.5.0 Controlling	136
Appendix A Selected Information Assets Classifications	138
Appendix B Potential Control Evaluation Worksheets	140
Chapter 4 Knowledge Check	141
Bibliography for Chapter 4	142

Chapter 5: Entity Employees	147
5.0 Introduction	148
5.1.0 Employment Practices	149
5.2.0 Decisional Quality, Responsibility Delegation, and Societal Engineering	151
5.3.0 IT Employees	155
5.3.1 Monitoring and Evaluating Resources	156
5.3.2 Incident Response Team	157
Chapter 5 Knowledge Check	162
Bibliography for Chapter 5	163

Part 3

Chapter 6: IT Audits and Reviews	166
6.0 Introduction	167
6.1.0 Planning	169
6.1.1 Considering Laws and Regulations	171
6.1.2 Audit Risk Assessment	172
6.1.3 Internal Control Assessment	174
6.2.0 Studying and Evaluating Controls	175
6.2.1 Access Management	181
6.2.2 Network Infrastructure	197
6.2.3 Risk Analysis	221
6.2.4 Environmental Controls	223
6.2.5 Confidential Information Asset Life Cycle	225

6.3.0 Testing and Evaluating Controls	229
6.4.0 Reporting	230
6.5.0 Follow-up	231
Appendix A Pro Forma IT Audit IAP Risk Assessment Template	232
Appendix B Generic Control Environment: Awareness Lead-sheet	233
Appendix C Computer Viruses	234
Appendix D IAP RACI or RASCI Templates	236
Appendix E IAP Control Classification Template	237
Appendix F Authentication Mechanisms Table	238
Appendix G Peer-to-Peer Networking	239
Appendix H Trans-border Communication Protection	240
Appendix I Suggested Access Controls Testing Checklist	242
Chapter 6 Knowledge Check	243
Bibliography for Chapter 6	244
Acronyms Used Throughout This Publication	252
Glossary of Terms Used Throughout This Publication	259
Biography of the Author	264