

NO FRILLS Exam Prep Books

Intellectual Properties, Trademarks and Copyrights

ExamREVIEW.NET (a.k.a. ExamREVIEW) is an independent content developer not associated/affiliated with the certification vendor(s) mentioned throughout this book. The name(s), title(s) and award(s) of the certification exam(s) mentioned in this book are the trademark(s) of the respective certification vendor(s). We mention these name(s) and/or the relevant terminologies only for describing the relevant exam process(es) and knowledge.

We are NOT affiliated with IAPP. This book is also NOT endorsed by IAPP. The CIPP certification exams are the property of IAPP.

ExamREVIEW(TM) and ExamFOCUS(TM) are our own trademarks for publishing and marketing self-developed examprep books worldwide. The EXAMREVIEW.NET web site has been created on the Internet since January 2001. The EXAMFOCUS.NET division has its web presence established since 2009.

Copyright 2012, 13. ExamREVIEW.NET. All rights reserved.

Contents of this book are fully copyrighted. We develop study material entirely on our own. Braindump is strictly prohibited. We provide essential knowledge contents, NOT any generalized "study system" kind of "pick-the-right-answer-every time" techniques or "visit this link" referrals.

Contents Update



All books come with LIFE TIME FREE UPDATES. When you find a newer version of the purchased book all you need to do is to go and download. **Please check our web site's Free Updates section regularly:**

http://www.examreview.net/free_updates.htm

Page Formatting and Typeface

To accommodate the needs of those with weaker vision, we use LARGER PRINT throughout the book whenever practical. The text in this book was created using Garamond (size 16). A little bit of page resizing, however, may have happened along the actual book printing process.

Exam topics covered in this book

According to the IAPP, candidates seeking their IAPP privacy certification must pass the MC based Certification Foundation exam which covers elementary concepts of privacy and data protection from a global perspective. The major exam components are:

- I. Introduction to Privacy: Common Principles and Approaches
- II. Information Security: Protecting and Safeguarding Personal Information
- III. Online Privacy: Using Personal Information on Websites and with Other Internet-related Technologies

After this exam the next step is to take the CIPP/US exam which has a lot of legal topics. Simply put, to earn the CIPP designation you need to pass both exams. It is our opinion that you need to possess both technical knowledge and legal knowledge in order to succeed.

Table of Contents (2013 Revised Edition)

INTELLECTUAL PROPERTIES, TRADEMARKS AND COPYRIGHTS.....1

CONTENTS UPDATE.....2

PAGE FORMATTING AND TYPEFACE2

EXAM TOPICS COVERED IN THIS BOOK.....2

TABLE OF CONTENTS (2013 REVISED EDITION)3

OVERVIEW OF PRIVACY AND PRIVACY RIGHTS8

LEGAL ORIGIN8

ONLINE PRIVACY9

THE IMPORTANCE OF THE HIPAA PRIVACY RULES.....11

PERSONALLY IDENTIFIABLE INFORMATION.....12

THE GENERAL PRINCIPLES CONCERNING PRIVACY12

POSSIBLE CIVIL CLAIMS.....13

SUMMARY14

BASIC KNOWLEDGE ON THE US LEGAL SYSTEM.....16

THE CONSTITUTION AND THE BRANCHES OF GOVERNMENT16

CONSTITUTIONS18

LEGISLATIVE ENACTMENTS (STATUTES)19

THE US COURT SYSTEM.....19

CLASSIFICATIONS OF LAW	21
PRIMARY AND SECONDARY AUTHORITIES.....	22
STATE LAW VS FEDERAL LAW	23
CASE LAW.....	24
JUDICIAL DECISION MAKING AND COMMON LAW.....	24
RULES VS LAWS	25
THE APPELLATE PROCESS.....	25
ELEMENTS OF A CRIME.....	27
THE INTENT	28
DEFAMATION	29

BASIC KNOWLEDGE ON NETWORK INFRASTRUCTURE, PROTOCOLS AND TECHNOLOGIES

OPEN SYSTEM INTERCONNECT	32
IP ADDRESSING.....	34
WIRELESS BASED LOCAL AREA NETWORKING.....	34
WAN AND VOIP	37
SSO MECHANISMS, INFOCARD AND OPENID.....	39
OTP AND KYPS.....	39
DACS	40
SAML AND WS-SECURITY.....	40
OVAL.....	40
OPSEC.....	41

ADVANCED KNOWLEDGE ON COMPUTER AND NETWORK SECURITY 43

SECURITY PLANNING	43
EQUIPMENTS AND DEVICES.....	44
POINTS OF FAILURE	46
MALWARE.....	46
VIRUSES AND WORMS	47
SPYWARE.....	47
TROJAN HORSE	48
KEYSTROKE LOGGER.....	48
SOFTWARE FLAWS.....	49
SNIFFING, EAVESDROPPING AND FOOTPRINTING	49
DoS AND DDoS.....	50
SOCIAL ENGINEERING	51

IDENTITY THEFT	52
BACKDOORS AND ROOTKITS	52
OTHER VULNERABILITIES	53
P3P	54
DATABASE SPECIFIC RISKS	54
CONCEALING HARD DISK DATA	56
<u>CRYPTOGRAPHY</u>	<u>60</u>
OVERVIEW	60
DES	60
IPSEC AND SSL	60
SYMMETRIC AND ASYMMETRIC ALGORITHMS	61
DIGITAL SIGNATURE	62
HASH FUNCTION.....	62
PGP	62
DISK BASED ENCRYPTION.....	63
EES	63
OPENSSL	64
OCSP AND CRL.....	64
<u>SECURITY THEORIES AND STRATEGIES</u>	<u>66</u>
DEFAULT DENY AND DEFAULT PERMIT	66
TRUSTED SYSTEM VS UNTRUSTED SYSTEM.....	66
THE COMPUTER SYSTEM ITSELF AS LARGELY AN UNTRUSTED SYSTEM	67
DEFENSE IN DEPTH.....	67
MODELS	68
INFORMATION SECURITY BASELINES.....	70
POLICIES AND CONTROLS	70
INTERNAL PREVENTIVE CONTROLS VERSUS COMPENSATING CONTROLS.....	75
ORANGE BOOK	76
INTERNET SECURITY	76
FIREWALL SECURITY	77
VIRUS SECURITY	78
WEB SERVER SECURITY.....	78
NAME RESOLUTION SECURITY	79
MAIL SERVER SECURITY.....	79
RAS SERVER SECURITY	80

PROXY SERVER SECURITY	80
AUTHENTICATION SERVER SECURITY.....	81
IM SECURITY.....	81
INCIDENT RESPONSE	81
COVERT CHANNEL ANALYSIS.....	82
CHANGE CONTROL	84
PLANNING AND SCOPING OF THE ASSESSMENT OF RISK.....	85
METHODOLOGIES FOR PROPER ASSESSMENT OF RISK.....	86
INCIDENT MONITORING.....	88
CSIRT	89
OWNERSHIP & RESPONSIBILITY.....	91
ACCOUNTS AND PASSWORD MANAGEMENT.....	92
SECURITY AWARENESS TRAINING.....	93

THE BASICS OF RECORDS MANAGEMENT.....95

SECURITY ACTS, STANDARDS AND GUIDELINES101

HIPAA	101
THE PRIVACY ACT OF 1974	102
THE FREEDOM OF INFORMATION ACT FOIA	103
THE CABLE COMMUNICATIONS POLICY ACT OF 1984	104
COPPA	104
THE CLINGER-COHEN ACT	105
THE FAIR INFORMATION PRACTICES	106
THE E-GOVERNMENT ACT AND THE GOVERNMENT PAPERWORK ELIMINATION ACT	106
THE OMB GUIDANCE FOR IMPLEMENTING THE PRIVACY PROVISIONS OF THE E- GOVERNMENT ACT.....	107
DPPA	109
ECPA	109
FERPA.....	109
UETA AND E-SIGN.....	110
VPPA.....	110
WORKPLACE PRIVACY STANDARDS	111
THE INTELLIGENCE REPORT AND TERRORISM PREVENTION ACT, THE FRCA, AND EMPLOYMENT SCREENING/CHECKS	112
EMPLOYEE SCREENING LAWS.....	113
BACKGROUND CHECK AND THE LAW	114

WIRETAPPING AND THE LAW.....	116
TELE-MARKETING AND TCPA.....	117
THE SARBANES–OXLEY ACT AND THE COSO FRAMEWORK.....	117
SoGP.....	118
COMMON CRITERIA CC.....	119
OECD GUIDELINES.....	119
COBIT.....	121
ISO STANDARDS.....	121
VAL IT.....	122
ITAF.....	123
FISMA.....	123
OTHER STANDARDS.....	123