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.

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 When you find a newer version of the purchased book all you need to do is to go and download.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 or the CIPP/E exam, both of which have a lot of legal topics. It is our opinion that you need to possess both technical knowledge and legal knowledge in order to succeed. **For the EU specialization, the focus of this book is on the various EU laws and regulations.**

Table of Contents (2013 Revised Edition)

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

CONTENTS UPDATE.....2

PAGE FORMATTING AND TYPEFACE.....2

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

TABLE OF CONTENTS (2013 REVISED EDITION).....3

OVERVIEW OF PRIVACY AND PRIVACY RIGHTS.....8

LEGAL ORIGIN.....8
ONLINE PRIVACY.....9
THE IMPORTANCE OF THE HIPAA PRIVACY RULES.....11
PERSONALLY IDENTIFIABLE INFORMATION.....12
THE GENERAL PRINCIPLES CONCERNING PRIVACY.....12
POSSIBLE CIVIL CLAIMS.....13
SUMMARY.....14

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

THE CONSTITUTION AND THE BRANCHES OF GOVERNMENT.....16
CONSTITUTIONS.....18
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 THE EU LEGAL SYSTEM AND THE LEGAL GROUND FOR DATA PROTECTION....32

BACKGROUND, STRUCTURE AND BINDING FORCE....32
THE EU LEGAL SYSTEM....33
CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA....35
DATA PROTECTION IN EU – AN OVERVIEW....36
KEY POINTS OF ARTICLE 6....37
KEY POINTS OF ARTICLE 8....38
KEY POINTS OF ARTICLE 10 AND 11....38
KEY POINTS OF ARTICLE 13 AND 15....39
KEY POINTS OF ARTICLE 16 AND 17....39
KEY POINTS OF ARTICLE 18, 20 AND 21....40
THE PRINCIPLES OUTLINED IN ARTICLE 25....40
DIRECTIVE 97/66/EC....40
SI 535/2003....41
DIRECTIVE 2006/24/EC....42
EMPLOYEE PRIVACY, BACKGROUND CHECKS AND MONITORING....42
PRIVACY AND WEB USE....44
PRIVACY, CCTV AND EMAIL....44

BASIC KNOWLEDGE ON NETWORK INFRASTRUCTURE, PROTOCOLS AND TECHNOLOGIES....48

OPEN SYSTEM INTERCONNECT....48
IP ADDRESSING....50

WIRELESS BASED LOCAL AREA NETWORKING....50
WAN AND VOIP....53
SSO MECHANISMS, INFOCARD AND OPENID....55
OTP AND KYPS....55
DACS....56
SAML AND WS-SECURITY....56
OVAL....56
OPSEC....57

ADVANCED KNOWLEDGE ON COMPUTER AND NETWORK SECURITY 59

SECURITY PLANNING....59
EQUIPMENTS AND DEVICES....60
POINTS OF FAILURE....62
MALWARE....62
VIRUSES AND WORMS....63
SPYWARE....63
TROJAN HORSE....64
KEYSTROKE LOGGER....64
SOFTWARE FLAWS....65
SNIFFING, EAVESDROPPING AND FOOTPRINTING....65
DOS AND DDOS....66
SOCIAL ENGINEERING....67
IDENTITY THEFT....68
BACKDOORS AND ROOTKITS....68
OTHER VULNERABILITIES....69
P3P....70
DATABASE SPECIFIC RISKS....70
CONCEALING HARD DISK DATA....72

CRYPTOGRAPHY....76

OVERVIEW....76
DES....76
IPSEC AND SSL....76
SYMMETRIC AND ASYMMETRIC ALGORITHMS....77
DIGITAL SIGNATURE....78
HASH FUNCTION....78
PGP....78

DISK BASED ENCRYPTION 79
EES 79
OPENSSL 80
OCSP AND CRL 80

SECURITY THEORIES AND STRATEGIES 82

DEFAULT DENY AND DEFAULT PERMIT 82
TRUSTED SYSTEM VS UNTRUSTED SYSTEM 82
THE COMPUTER SYSTEM ITSELF AS LARGELY AN UNTRUSTED SYSTEM 83
DEFENSE IN DEPTH 83
MODELS 84
INFORMATION SECURITY BASELINES 86
POLICIES AND CONTROLS 86
INTERNAL PREVENTIVE CONTROLS VERSUS COMPENSATING CONTROLS 91
ORANGE BOOK 92
INTERNET SECURITY 92
FIREWALL SECURITY 93
VIRUS SECURITY 94
WEB SERVER SECURITY 94
NAME RESOLUTION SECURITY 95
MAIL SERVER SECURITY 95
RAS SERVER SECURITY 96
PROXY SERVER SECURITY 96
AUTHENTICATION SERVER SECURITY 97
IM SECURITY 97
INCIDENT RESPONSE 97
COVERT CHANNEL ANALYSIS 98
CHANGE CONTROL 100
PLANNING AND SCOPING OF THE ASSESSMENT OF RISK 101
METHODOLOGIES FOR PROPER ASSESSMENT OF RISK 102
INCIDENT MONITORING 104
CSIRT 105
OWNERSHIP & RESPONSIBILITY 107
ACCOUNTS AND PASSWORD MANAGEMENT 108
SECURITY AWARENESS TRAINING 109

THE BASICS OF RECORDS MANAGEMENT 111

SECURITY ACTS, STANDARDS AND GUIDELINES 117

HIPAA 117
THE PRIVACY ACT OF 1974 118
THE FREEDOM OF INFORMATION ACT FOIA 119
THE CABLE COMMUNICATIONS POLICY ACT OF 1984 120
COPPA 120
THE CLINGER-COHEN ACT 121
THE FAIR INFORMATION PRACTICES 122
THE E-GOVERNMENT ACT AND THE GOVERNMENT PAPERWORK ELIMINATION ACT 122
THE OMB GUIDANCE FOR IMPLEMENTING THE PRIVACY PROVISIONS OF THE E-GOVERNMENT ACT 123
DPPA 125
ECPA 125
FERPA 125
UETA AND E-SIGN 126
VPPA 126
WORKPLACE PRIVACY STANDARDS 127
THE INTELLIGENCE REPORT AND TERRORISM PREVENTION ACT, THE FRCA, AND EMPLOYMENT SCREENING/CHECKS 128
EMPLOYEE SCREENING LAWS 129
BACKGROUND CHECK AND THE LAW 130
WIRETAPPING AND THE LAW 132
TELE-MARKETING AND TCPA 133
THE SARBANES–OXLEY ACT AND THE COSO FRAMEWORK 133
SOGP 134
COMMON CRITERIA CC 135
OECD GUIDELINES 135
COBIT 137
ISO STANDARDS 137
VAL IT 138
ITAF 139
FISMA 139
OTHER STANDARDS 139