

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 When you find a newer version of the purchased book all you need to do is to go and download.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 or the CIPP/C exam 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.

Table of Contents (2013 Revised Edition)

<u>INTELLECTUAL PROPERTIES, TRADEMARKS AND COPYRIGHTS.....</u>	<u>1</u>
<u>CONTENTS UPDATE.....</u>	<u>2</u>
<u>PAGE FORMATTING AND TYPEFACE</u>	<u>2</u>
<u>EXAM TOPICS COVERED IN THIS BOOK.....</u>	<u>2</u>
<u>TABLE OF CONTENTS (2013 REVISED EDITION).....</u>	<u>3</u>
<u>OVERVIEW OF PRIVACY AND PRIVACY RIGHTS</u>	<u>8</u>
LEGAL ORIGIN.....	8
ONLINE PRIVACY	9
THE IMPORTANCE OF THE HIPAA PRIVACY RULES.....	11
PERSONALLY IDENTIFIABLE INFORMATION.....	12
THE IMPORTANCE OF THE PIPEDA (CANADA) PRIVACY RULES.....	12
THE GENERAL PRINCIPLES CONCERNING PRIVACY	13
POSSIBLE CIVIL CLAIMS.....	14
SUMMARY	14
<u>BASIC KNOWLEDGE ON THE US LEGAL SYSTEM.....</u>	<u>17</u>
THE CONSTITUTION AND THE BRANCHES OF GOVERNMENT	17
CONSTITUTIONS	19
LEGISLATIVE ENACTMENTS (STATUTES).....	20
THE US COURT SYSTEM.....	20

CLASSIFICATIONS OF LAW	22
PRIMARY AND SECONDARY AUTHORITIES.....	23
STATE LAW VS FEDERAL LAW	24
CASE LAW.....	25
JUDICIAL DECISION MAKING AND COMMON LAW.....	25
RULES VS LAWS	26
THE APPELLATE PROCESS.....	26
ELEMENTS OF A CRIME.....	28
THE INTENT	29
DEFAMATION	30

OVERVIEW OF THE CANADIAN LEGAL SYSTEM.....33

OVERVIEW OF THE GOVERNMENT	33
OVERVIEW OF THE LEGAL SYSTEM.....	33
CIVIL LAW VS COMMON LAW.....	34
FEDERAL LEVEL LAW VS LOCAL LAW	34
BLASPHEMOUS LIBEL AND DEFAMATORY LIBEL	35
TERRORIST ACTIVITIES.....	35

BASIC KNOWLEDGE ON NETWORK INFRASTRUCTURE, PROTOCOLS AND TECHNOLOGIES37

OPEN SYSTEM INTERCONNECT	37
IP ADDRESSING.....	39
WIRELESS BASED LOCAL AREA NETWORKING.....	39
WAN AND VOIP	42
SSO MECHANISMS, INFOCARD AND OPENID.....	44
OTP AND KYPS.....	44
DACS	45
SAML AND WS-SECURITY.....	45
OVAL.....	45
OPSEC.....	46

ADVANCED KNOWLEDGE ON COMPUTER AND NETWORK SECURITY 48

SECURITY PLANNING	48
EQUIPMENTS AND DEVICES.....	49
POINTS OF FAILURE	51

MALWARE	51
VIRUSES AND WORMS	52
SPYWARE.....	52
TROJAN HORSE	53
KEYSTROKE LOGGER.....	53
SOFTWARE FLAWS.....	54
SNIFFING, EAVESDROPPING AND FOOTPRINTING	54
DoS AND DDoS.....	55
SOCIAL ENGINEERING	56
IDENTITY THEFT	57
BACKDOORS AND ROOTKITS	57
OTHER VULNERABILITIES	58
P3P	59
DATABASE SPECIFIC RISKS	59
CONCEALING HARD DISK DATA	61
 <u>CRYPTOGRAPHY</u>	 <u>65</u>
OVERVIEW	65
DES	65
IPSEC AND SSL	65
SYMMETRIC AND ASYMMETRIC ALGORITHMS	66
DIGITAL SIGNATURE	67
HASH FUNCTION.....	67
PGP	67
DISK BASED ENCRYPTION.....	68
EES	68
OPENSSL	69
OCSP AND CRL.....	69
 <u>SECURITY THEORIES AND STRATEGIES</u>	 <u>71</u>
DEFAULT DENY AND DEFAULT PERMIT	71
TRUSTED SYSTEM VS UNTRUSTED SYSTEM.....	71
THE COMPUTER SYSTEM ITSELF AS LARGELY AN UNTRUSTED SYSTEM	72
DEFENSE IN DEPTH.....	72
MODELS	73
INFORMATION SECURITY BASELINES	75
POLICIES AND CONTROLS	75

INTERNAL PREVENTIVE CONTROLS VERSUS COMPENSATING CONTROLS	80
ORANGE BOOK	81
INTERNET SECURITY	81
FIREWALL SECURITY	82
VIRUS SECURITY	83
WEB SERVER SECURITY.....	83
NAME RESOLUTION SECURITY	84
MAIL SERVER SECURITY.....	84
RAS SERVER SECURITY	85
PROXY SERVER SECURITY	85
AUTHENTICATION SERVER SECURITY.....	86
IM SECURITY.....	86
INCIDENT RESPONSE	86
COVERT CHANNEL ANALYSIS.....	87
CHANGE CONTROL	89
PLANNING AND SCOPING OF THE ASSESSMENT OF RISK.....	90
METHODOLOGIES FOR PROPER ASSESSMENT OF RISK.....	91
INCIDENT MONITORING.....	93
CSIRT	94
OWNERSHIP & RESPONSIBILITY.....	96
ACCOUNTS AND PASSWORD MANAGEMENT.....	97
SECURITY AWARENESS TRAINING.....	98
 <u>THE BASICS OF RECORDS MANAGEMENT.....</u>	 <u>100</u>
 <u>SECURITY ACTS, STANDARDS AND GUIDELINES (US)</u>	 <u>106</u>
 HIPAA	 106
THE PRIVACY ACT OF 1974	107
THE FREEDOM OF INFORMATION ACT FOIA	108
THE CABLE COMMUNICATIONS POLICY ACT OF 1984	109
COPPA	109
THE CLINGER-COHEN ACT	110
THE FAIR INFORMATION PRACTICES	111
THE E-GOVERNMENT ACT AND THE GOVERNMENT PAPERWORK ELIMINATION ACT	111
THE OMB GUIDANCE FOR IMPLEMENTING THE PRIVACY PROVISIONS OF THE E- GOVERNMENT ACT.....	112
DPPA	114

ECPA	114
FERPA.....	114
UETA AND E-SIGN.....	115
VPPA.....	115
WORKPLACE PRIVACY STANDARDS	116
THE INTELLIGENCE REPORT AND TERRORISM PREVENTION ACT, THE FRCA, AND EMPLOYMENT SCREENING/CHECKS	117
EMPLOYEE SCREENING LAWS.....	118
BACKGROUND CHECK AND THE LAW	119
WIRETAPPING AND THE LAW.....	121
TELE-MARKETING AND TCPA	122
THE SARBANES–OXLEY ACT AND THE COSO FRAMEWORK	122
SoGP	123
COMMON CRITERIA CC.....	124
OECD GUIDELINES.....	124
COBIT	126
ISO STANDARDS	126
VAL IT	127
ITAF	128
FISMA.....	128
OTHER STANDARDS	128
 <u>SECURITY ACTS, STANDARDS AND GUIDELINES (CANADA)</u>	 133
THE CHARTER OF RIGHTS AND FREEDOMS.....	133
THE OFFICE OF THE PRIVACY COMMISSIONER OPC	133
PIPEDA AND PHIPA	134
THE PRIVACY ACT AND ITS DIRECTIVE ON PRIVACY IMPACT ASSESSMENT	136
THE ACCESS TO INFORMATION ACT.....	138
THE POLICY ON GOVERNMENT SECURITY AND THE SECURITY OF INFORMATION ACT	138
THE DIRECTIVE ON IDENTITY MANAGEMENT	139
THE CRIMINAL RECORDS ACT AND THE DNA IDENTIFICATION ACT	139
PRIVACY IN THE WORKPLACE	139
PRE-EMPLOYMENT SCREENING.....	140