

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 FITSI. This book is also NOT endorsed by FITSI. The FITSP certification exams are the property of FITSI.

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 When you find a newer version of the purchased book all you need to do is to go and download.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

The Federal IT Security Professional FITSP Certification is being administered by the Federal IT Security Institute. Its mission is to help secure the nation's federal information systems by certifying that federal workforce members understand and can apply appropriate federal IT security standards. The FITSP program is broken into the four separate roles, which are manager, operator, designer and auditor. This product covers the auditor version.

The FITSP certification contents are based on the NIST/FISCAM material. These material cover knowledge that are the mainstream common standards in use today. Still, NIST/FISCAM specific topics are always of primary focus. When we develop our material we do not classify topics the BOK way. We follow our own flow of instructions which we think is more logical for the overall learning process.

Don't worry, it does not hurt to do so, as long as you truly comprehend the material.

To succeed in the exam, you need to read as many reference books as possible. There is no single book that can cover everything! You also need to have real world experience. **FOR THIS AUDITOR EXAM IN PARTICULAR, YOU WILL NOT SURVIVE THE EXAM UNLESS YOU HAVE REAL EXPERIENCE IN THE FIELD.** This ExamFOCUS book focuses on the more difficult topics that will likely make a difference in exam results. The book is NOT intended to guide you through every single official topic. You should therefore use this book together with other reference books for the best possible preparation outcome.

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

FOUNDATION TECH KNOWLEDGE: COMPUTER AND NETWORK SECURITY9

SECURITY PLANNING9

THE NIST DEFINITION OF SECURITY PLANNING AND THE ROLES INVOLVED10

MAJOR APPLICATIONS VS GENERAL SUPPORT SYSTEMS.....11

EQUIPMENTS AND DEVICES.....12

POINTS OF FAILURE14

MALWARE14

VIRUSES AND WORMS15

SPYWARE.....15

TROJAN HORSE	15
KEYSTROKE LOGGER.....	16
SOFTWARE FLAWS	16
SNIFFING, EAVESDROPPING AND FOOTPRINTING	17
DOS AND DDoS.....	18
SOCIAL ENGINEERING	19
IDENTITY THEFT	20
BACKDOORS AND ROOTKITS	20
OTHER VULNERABILITIES	21
P3P	22
DATABASE SPECIFIC RISKS	22
CONCEALING HARD DISK DATA	24
TELEWORKER DEVICE AND REMOTE ACCESS SECURITY	25
ENDPOINT SECURITY	26
SOFTWARE AS A SERVICE SECURITY	27
VIRTUALIZATION SECURITY	27
STORAGE SECURITY.....	28
NAME RESOLUTION SECURITY	29

BASIC KNOWLEDGE: SECURITY THEORIES AND ACCESS CONTROL

<u>MODELS.....</u>	33
---------------------------	-----------

THE NIST DEFINITIONS OF SECURITY.....	33
THE NIST DEFINITION OF SECURITY DOMAINS	34
DEFAULT DENY AND DEFAULT PERMIT	34
TRUSTED SYSTEM VS UNTRUSTED SYSTEM.....	35
THE COMPUTER SYSTEM ITSELF AS LARGELY AN UNTRUSTED SYSTEM	36
DEFENSE IN DEPTH.....	36
MODELS	37
ACLs VERSUS CAPABILITIES.....	38
THE AAA CONCEPT	40
RECOMMENDED ACCESS CONTROL MEASURES.....	42

BACKGROUND KNOWLEDGE: MAJOR STANDARDS AND GUIDELINES .48

THE YELLOW BOOK.....	48
FISCAM AND THE GAO	48
NIST AND FIPS.....	49
THE NIST CERTIFICATION AND ACCREDITATION EFFORTS	49

THE NIST PRINCIPLES OF SECURING INFORMATION SYSTEMS.....	50
FIPS 200	52
THE OMB CIRCULAR A130	52
SCAP	54
THE SARBANES–OXLEY ACT AND THE COSO FRAMEWORK	54
SoGP	55
COMMON CRITERIA (CC)	55
HIPAA	55
COBIT	56
ISO STANDARDS	56
VAL IT	57
ITAF	57
FISMA.....	57
OTHER STANDARDS	57
RELEVANT LEGISLATIVE ACTS FROM A FEDERAL PERSPECTIVE.....	58
RELEVANT OMB CIRCULARS AND HOMELAND SECURITY DIRECTIVES.....	59

BASIC KNOWLEDGE: CRYPTOGRAPHY.....62

OVERVIEW.....	62
DES.....	62
IPSEC AND SSL.....	62
SYMMETRIC AND ASYMMETRIC ALGORITHMS	63
DIGITAL SIGNATURE	63
HASH FUNCTION.....	64
PGP	64
DISK BASED ENCRYPTION.....	65
EES	65
OPENSSL	66
OCSP AND CRL.....	66
FIPS 140-2.....	66

SECURITY STRATEGIES69

INFORMATION SECURITY BASELINES.....	69
TYPES OF POLICIES	69
TYPES OF CONTROLS	72
INTERNAL PREVENTIVE CONTROLS VERSUS COMPENSATING CONTROLS	76
THE NIST WAY OF DEFINING SYSTEM BOUNDARIES AND MAJOR APPLICATIONS	77

THE NIST/FISCAM WAY OF CLASSIFYING CONTROLS	78
THE ENTIRE NIST CONTROL FAMILIES	79
THE NIST WAY OF STRUCTURING AND ASSURING CONTROLS	90
THE NIST SECURITY CONTROL CATALOG	90
THE NIST WAY OF REVIEWING AND MONITORING CONTROLS	91
THE NIST WAY OF DEFINING COMPENSATING CONTROLS	91
ORANGE BOOK.....	92
INTERNET SECURITY.....	93
FIREWALL SECURITY	93
VIRUS SECURITY	94
WEB SERVER SECURITY.....	95
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.....	99
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
NIST AND PRIVACY CONTROLS.....	109
SECURITY AWARENESS TRAINING.....	111
<u>PHYSICAL SECURITY FOR COMPUTER EQUIPMENTS</u>	<u>116</u>
GENERAL GUIDELINES	116
PHYSICAL SITE PREPARATION AND MANAGEMENT	117
FIRE PROTECTION	118
MAINTENANCE AND TESTING.....	119
EQUIPMENT AND MEDIA MANAGEMENT.....	120
THE NIST CLASSIFICATIONS OF PHYSICAL AND ENVIRONMENTAL SECURITY CONTROLS	122

MANAGING SECURITY125

IT STRATEGIC PLANNING	125
SWOT ANALYSIS.....	126
IT OPERATIONS MANAGEMENT	127
INFORMATION MANAGEMENT POLICY	128
ENTERPRISE SECURITY	128
IS GOVERNANCE.....	129
ORGANIZATIONAL STRUCTURE AND SUPPORT	130
THE NIST SUGGESTED GOVERNANCE MODELS	131
SENIOR MANAGEMENT SUPPORT	132
THE ROLE OF THE INFORMATION SECURITY PRACTITIONER.....	133
INFORMATION SECURITY PROGRAM AND POLICY DEVELOPMENT FROM A STRATEGIC PERSPECTIVE	134
HR AND SECURITY	137
CONCERNS ON M & A	138
CHANGE MANAGEMENT	139
RMF AND CHANGE MANAGEMENT.....	140
RMF AND SYSTEM INVENTORY	140
CONFIGURATION MANAGEMENT AND RELEASE MANAGEMENT.....	141
RMF AND SECURITY CONFIGURATION MANAGEMENT	142
RMF AND CONFIGURATION CONTROL BOARD	143
PREPARING FOR EMERGENCY RESPONSE.....	143
RESPONDING TO INCIDENTS AND MANAGING RECOVERY	145
INVESTIGATION	148
COMPUTER FORENSICS	150

MANAGING, MONITORING AND CONTROLLING RISKS.....153

IS RISK MANAGEMENT	153
THE VARIOUS RISK MANAGEMENT DISCIPLINES	153
THE NIST RMF	155
RMF AND SECURITY CATEGORIZATION.....	156
RMF AND SECURITY CONTROLS SELECTION	156
THE NIST SUGGESTED RISK ASSESSMENT METHODOLOGY.....	157
THREATS AND VULNERABILITIES.....	159
SECURITY AND CONTROL CHECKLISTS.....	160
LIKELIHOOD AND IMPACTS	162
THE NIST WAY OF DETERMINING IMPACT LEVELS	163

RISK LEVEL DETERMINATION AND RESPONSE STRATEGIES.....	164
THE NIST ISCM.....	165
LOSS CALCULATIONS	166
<u>CONTINGENCY AND CONTINUITY</u>	169
OVERVIEW.....	169
THE NIST SUGGESTED STEPS AND CONTROLS FOR SUCCESSFUL CONTINGENCY	
PLANNING	169
BCP, DRP AND COOP	171
THE NIST DEFINED CIKR, CIP, ISCP AND OEP	172
BUSINESS IMPACT ANALYSIS	173
RECOVERY VALIDATION AND PLAN DEACTIVATION THE NIST WAY.....	174
<u>SECURITY SYSTEM DESIGN</u>	178
GENERAL GUIDELINES	178
INFORMATION SECURITY ASSESSMENT METHODOLOGY THE NIST WAY.....	178
DEVELOPMENT MODELS AND FRAMEWORKS.....	179
SDLC AND RISK MANAGEMENT	184
SOFTWARE TESTING	184
<u>IS AUDITING.....</u>	190
THE ROLE, RIGHT AND ETHICS OF AN AUDITOR	192
THE AUDIT PROCESS	193
OVERALL STRATEGIES	194
THE GAO DEFINED PHASES.....	195
THE GAO DEFINED IS CONTROLS AUDIT OBJECTIVES AND SCOPES	196
AUDIT PLANNING	200
THE GAO DEFINED RISK FACTORS	206
THE GAO DEFINED CONTROL POINTS AND CRITICAL CONTROL POINTS.....	207
AUDIT TECHNIQUES AND TOOLS.....	208
THE FISCAM DEFINED CONTROL OBJECTIVES AND STEPS	209
THE FISCAM WAY OF PERFORMING AUDIT TESTS.....	212
CONFLICTS OF INTEREST AND INDEPENDENCE.....	213
AUDIT FIELDWORKS AND TOOLS	214
AUDIT PROGRAM AND REPORT	216