

**SSCP 2009**

# **ExamESSENTIALS**

**Study Guide & Review Questions**

**2009**

**Ed.**

*ExamReview.NET*  
*ExamReview Press*

**The Number One Source of Exam and On-the-Job Information**

STUDY INFORMATION FOR EXAM CANDIDATES

# **SSCP ExamESSENTIALS Guide**

---

Covering the 2009 Syllabus

© ExamREVIEW PRO & ExamREVIEW PRESS  
2008, 09

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

**Important – Please Read**

**Due to the variety of fonts installed on the users' systems, Acrobat may prompt you to download an additional language component (which is FREE from Adobe anyway).**

**If you receive a message saying that a Traditional Chinese language pack has to be downloaded in order to load this eBook, please click YES to have Acrobat download the update. The size of the update is about 7M. Don't worry, this download is safe.**

# Table of Contents

<b>END USER LICENSE AGREEMENT</b>	<b>6</b>
<b>EXAM FORMAT</b>	<b>12</b>
<b>ABOUT THIS BOOK</b>	<b>13</b>
<b>EXAM TOPICS</b>	<b>14</b>
<b>EXAM REGISTRATION CONTACTS</b>	<b>15</b>
<b>STUDY PSYCHOLOGY &amp; EXAM TACTICS</b>	<b>16</b>
<b><i>KEY EXAM STRATEGIES</i></b>	<b>17</b>
STRATEGY ONE: KEYWORD OR KEY PHRASE MATCHING.	17
STRATEGY TWO: CHOICES GROUPING.	18
STRATEGY THREE: THINK TRICKY.	19
<b><i>SECURITY THEORIES</i></b>	<b>21</b>
THE COMPUTER SYSTEM ITSELF AS LARGELY AN UNTRUSTED SYSTEM	23
DEFENSE IN DEPTH	23
VULNERABILITIES	24
SECURITY MEASURES	42
STANDARDS, GUIDELINES AND LAWS	50
TCP/IP SPECIFIC RISKS	56
<b><i>INFORMATION SECURITY PRACTICES</i></b>	<b>59</b>
IS MANAGEMENT ACTIVITIES	60
INFORMATION MANAGEMENT POLICY	61
ORGANIZATIONAL STRUCTURE AND SUPPORT	63
THE ROLE OF AN INFORMATION SECURITY PROFESSIONAL	64
IS CONTROL CLASSIFICATION	66
ACCESS CONTROL MODELS	73
ACLs VERSUS CAPABILITIES	74
WHAT IS ORANGE BOOK, BY THE WAY?	75
TYPES OF ACCESS CONTROL	76
THE AAA CONCEPT	78
PRACTICAL ACCESS CONTROL MEASURES	81

ESTABLISHING ACCOUNTABILITY THROUGH EVENT LOGGING	87
IS GOVERNANCE	90
BASIC OUTCOMES OF IS GOVERNANCE	92
<b><i>IT STRATEGIC PLANNING</i></b>	<b>94</b>
<hr/>	
IT STRATEGIC PLANNING DEFINED	94
<b><i>PROTECTION OF INFORMATION ASSETS THROUGH SECURITY POLICY</i></b>	<b>97</b>
<hr/>	
INFORMATION ASSETS DEFINED	97
DATA CLASSIFICATIONS AND LAYER OF RESPONSIBILITIES	99
SECURITY POLICY	100
EFFECTIVE SECURITY PRACTICES	107
OWNERSHIP & RESPONSIBILITY	108
SECURITY AWARENESS TRAINING	110
PHYSICAL SECURITY SURVEY	113
PROTECTION IN DEPTH	116
PERIMETER DEFENSE	117
SECURITY MODELS AND MODES OF OPERATIONS	118
EXAMPLE POLICY	120
CONSEQUENCES OF VIOLATIONS	122
EVALUATION	123
DEVisING YOUR OWN CLASSIFICATION SCHEME	124
CHANGE CONTROL	125
<b><i>RISK MANAGEMENT, BCP, BIA AND RESPONSE MANAGEMENT</i></b>	<b>128</b>
<hr/>	
RISK MANAGEMENT DEFINED	129
THE RISK MANAGEMENT STEPS	130
RISK MANAGEMENT AND THE IS PROFESSIONAL	131
BCP DEFINED	132
BCP vs BPCP vs DRP	133
BCP PHASES	134
STAKEHOLDERS AND CRISIS COMMUNICATIONS	135
THE RISK ASSESSMENT FLOW	137
RISK VS THREAT AND VULNERABILITY	138
IDENTIFYING RISKS	139
LOSS CALCULATIONS	140
BUSINESS IMPACT ANALYSIS DEFINED	143
BIA GOALS AND STEPS	144
BIA CHECKLIST	145
PREPARING FOR EMERGENCY RESPONSE	149
RESPONDING TO INCIDENTS AND MANAGING RECOVERY	151
TESTING THE PLAN	155
USER ACCEPTANCE	156
PLAN MAINTENANCE	157

<b><u>IS PROGRAM MANAGEMENT, PROJECT MANAGEMENT AND CHANGE MANAGEMENT</u></b>	<b>159</b>
INFORMATION SECURITY PLAN	159
INFORMATION SECURITY BASELINES	159
PROJECT MANAGEMENT DEFINED	160
CHANGE MANAGEMENT DEFINED	162
CHANGE MANAGEMENT STRATEGIES	164
CHANGE MANAGEMENT VS CHANGE CONTROL	166
CONFIGURATION MANAGEMENT	167
GENERAL GUIDELINES	170
SYSTEM CHANGE CONTROL	171
SOFTWARE DEVELOPMENT PROCESSES AND MODELS	172
<b><u>MODERN WIRELESS SECURITY</u></b>	<b>176</b>
<b><u>BLUETOOTH SECURITY</u></b>	<b>178</b>
<b><u>IM SECURITY</u></b>	<b>178</b>
<b><u>FURTHER TECHNICAL READINGS</u></b>	<b>179</b>
SECTION 1: TOPICS ON SECURITY THEORY	180
SECTION 2: TOPICS ON HACKING, ATTACKING, DEFENDING AND AUDITING.	180
SECTION 3: TOPICS ON ENCRYPTION AND VPN.	180
SECTION 4: TOPICS ON RESPONDING TO ATTACKS	180
SECTION 5: TOPICS ON VIRUSES.	180
<b><u>EXCELLENT PUBLIC RESOURCES</u></b>	<b>271</b>
<b><u>EXAMREADINESS TECHNICAL DRILL PRACTICE QUESTIONS FOR SSCP CANDIDATES</u></b>	<b>277</b>