

# 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 ISC2. This book is also NOT endorsed by ISC2. The CAP certification exam is the property of ISC2.

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 When you find a newer version of the purchased book all you need to do is to go and download.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

## The Exam

The ISC2 Certified Authorization Professional CAP certification indicates a professional level of knowledge and skills on the subject of federal information system authorization. Authorization means operating a federally owned information system with formal acceptance of risk from an Authorization Officer who has the authority to make major risk related decisions within a federal organization. The CAP exam covers security practices and federal information security/protection laws as well as NIST publications and OMB regulations. Officially there are seven knowledge domains, including:

1. Understanding the Security Authorization of Information Systems
2. Categorize Information Systems
3. Establish the Security Control Baseline

4. Apply Security Controls
5. Assess Security Controls
6. Authorize Information System
7. Monitor Security Controls

When we develop our material we do not classify topics the BOK way. In fact, we follow our own flow of instructions which we think is more logical for the overall learning process. **To succeed in the exam, you need to read as many reference books as possible. There is no single book that can cover everything!**

## Table of Contents (2013 Revised Edition)

|                                                         |    |
|---------------------------------------------------------|----|
| INTELLECTUAL PROPERTIES, TRADEMARKS AND COPYRIGHTS..... | 1  |
| CONTENTS UPDATE .....                                   | 2  |
| PAGE FORMATTING AND TYPEFACE .....                      | 2  |
| THE EXAM.....                                           | 2  |
| COMPUTER AND NETWORK SECURITY .....                     | 7  |
| SECURITY PLANNING.....                                  | 7  |
| EQUIPMENTS AND DEVICES.....                             | 8  |
| POINTS OF FAILURE AND VULNERABILITY TESTING .....       | 11 |
| MALWARE .....                                           | 12 |
| VIRUSES AND WORMS.....                                  | 12 |
| SPYWARE .....                                           | 12 |
| TROJAN HORSE.....                                       | 13 |
| KEYSTROKE LOGGER.....                                   | 13 |
| SOFTWARE FLAWS.....                                     | 14 |
| SNIFFING, EAVESDROPPING AND FOOTPRINTING .....          | 14 |
| DoS AND DDoS.....                                       | 15 |
| SOCIAL ENGINEERING.....                                 | 16 |
| IDENTITY THEFT .....                                    | 17 |
| BACKDOORS AND ROOTKITS .....                            | 17 |
| OTHER VULNERABILITIES.....                              | 18 |
| CRYPTOGRAPHY AND FIPS 140-2.....                        | 19 |
| DES, RSA AND OTHERS.....                                | 20 |
| MD5 AND SHA.....                                        | 22 |

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| IPSEC, IKE AND SSL .....                                                | 24        |
| DIGITAL CERTIFICATE.....                                                | 24        |
| OCSP AND CRL.....                                                       | 26        |
| SYMMETRIC AND ASYMMETRIC ALGORITHMS .....                               | 26        |
| HASH FUNCTION .....                                                     | 27        |
| PGP .....                                                               | 27        |
| DISK BASED ENCRYPTION.....                                              | 27        |
| EES .....                                                               | 28        |
| OPENSSL.....                                                            | 28        |
| P3P .....                                                               | 29        |
| XACML, SOAP, SAML AND SPML .....                                        | 29        |
| CAS AND OTHER SSO MECHANISMS .....                                      | 30        |
| INFOCARD AND OPENID.....                                                | 30        |
| OTP AND KYPS .....                                                      | 31        |
| DACS.....                                                               | 31        |
| OVAL .....                                                              | 32        |
| OPSEC.....                                                              | 32        |
| DATABASE SPECIFIC RISKS .....                                           | 32        |
| DATABASE ACTIVITY MONITORING.....                                       | 34        |
| VIRTUALIZATION THROUGH HYPER-V .....                                    | 34        |
| FREWARE, SHAREWARE, OPENSOURCE, LICENSING AND DRM .....                 | 35        |
| <b>SECURITY STRATEGIES.....</b>                                         | <b>41</b> |
| INFORMATION SECURITY BASELINES .....                                    | 41        |
| TYPES OF POLICIES.....                                                  | 41        |
| TYPES OF CONTROLS .....                                                 | 44        |
| INTERNAL PREVENTIVE CONTROLS VERSUS COMPENSATING CONTROLS.....          | 48        |
| THE NIST WAY OF DEFINING SYSTEM BOUNDARIES AND MAJOR APPLICATIONS ..... | 49        |
| THE NIST WAY OF CLASSIFYING CONTROLS.....                               | 50        |
| THE ENTIRE NIST CONTROL FAMILIES.....                                   | 51        |
| THE NIST WAY OF STRUCTURING AND ASSURING CONTROLS .....                 | 60        |
| THE NIST SECURITY CONTROL CATALOG .....                                 | 61        |
| THE NIST WAY OF REVIEWING AND MONITORING CONTROLS .....                 | 61        |
| THE NIST WAY OF DEFINING COMPENSATING CONTROLS .....                    | 62        |
| INTERNET SECURITY .....                                                 | 62        |
| FIREWALL SECURITY.....                                                  | 63        |
| VIRUS SECURITY .....                                                    | 64        |
| WEB SERVER SECURITY .....                                               | 64        |
| NAME RESOLUTION SECURITY.....                                           | 65        |
| DNS SOCKET POOL , QUERY BLOCK LIST AND CACHE LOCKING.....               | 66        |
| MAIL SERVER SECURITY.....                                               | 66        |
| RAS SERVER SECURITY.....                                                | 67        |
| PROXY SERVER SECURITY .....                                             | 67        |
| AUTHENTICATION SERVER SECURITY .....                                    | 68        |
| CONCEALING HARD DISK DATA.....                                          | 68        |
| ENDPOINT SECURITY.....                                                  | 69        |
| SOFTWARE AS A SERVICE SECURITY.....                                     | 70        |

|                                                                                       |            |
|---------------------------------------------------------------------------------------|------------|
| <b>VIRTUALIZATION SECURITY .....</b>                                                  | <b>70</b>  |
| <b>STORAGE SECURITY.....</b>                                                          | <b>71</b>  |
| <b>INCIDENT RESPONSE.....</b>                                                         | <b>72</b>  |
| <b>COVERT CHANNEL ANALYSIS .....</b>                                                  | <b>73</b>  |
| <b>NIST AND PRIVACY CONTROLS .....</b>                                                | <b>74</b>  |
| <b>CHANGE CONTROL .....</b>                                                           | <b>76</b>  |
| <b>PLANNING AND SCOPING OF THE ASSESSMENT OF RISK .....</b>                           | <b>77</b>  |
| <b>METHODOLOGIES FOR PROPER ASSESSMENT OF RISK.....</b>                               | <b>79</b>  |
| <b>THE INFOSEC ASSESSMENT METHODOLOGY IAM .....</b>                                   | <b>80</b>  |
| <b>INCIDENT MONITORING .....</b>                                                      | <b>81</b>  |
| <b>CSIRT .....</b>                                                                    | <b>82</b>  |
| <b>OWNERSHIP &amp; RESPONSIBILITY.....</b>                                            | <b>84</b>  |
| <b>ACCOUNTS AND PASSWORD MANAGEMENT .....</b>                                         | <b>85</b>  |
| <b>BACKUP SCHEMES.....</b>                                                            | <b>85</b>  |
| <b>SECURITY AWARENESS TRAINING.....</b>                                               | <b>86</b>  |
| <b>IT SERVICE MANAGEMENT .....</b>                                                    | <b>87</b>  |
| <b>SIEM, SIM AND SEM .....</b>                                                        | <b>88</b>  |
| <b>PCI ASSESSMENT .....</b>                                                           | <b>89</b>  |
| <b>USER ACCOUNT PROVISIONING .....</b>                                                | <b>89</b>  |
| <b>IS RISK MANAGEMENT AND THE NIST RMF.....</b>                                       | <b>94</b>  |
| <b>OVERVIEW .....</b>                                                                 | <b>94</b>  |
| <b>THE VARIOUS RISK MANAGEMENT DISCIPLINES.....</b>                                   | <b>94</b>  |
| <b>THE NIST RMF .....</b>                                                             | <b>96</b>  |
| <b>RMF AND SECURITY CATEGORIZATION .....</b>                                          | <b>97</b>  |
| <b>RMF AND SECURITY CONTROLS SELECTION .....</b>                                      | <b>97</b>  |
| <b>THE NIST SUGGESTED RISK ASSESSMENT METHODOLOGY.....</b>                            | <b>98</b>  |
| <b>THREATS AND VULNERABILITIES.....</b>                                               | <b>100</b> |
| <b>SECURITY AND CONTROL CHECKLISTS .....</b>                                          | <b>100</b> |
| <b>LIKELIHOOD AND IMPACTS.....</b>                                                    | <b>102</b> |
| <b>THE NIST WAY OF DETERMINING IMPACT LEVELS .....</b>                                | <b>103</b> |
| <b>RISK LEVEL DETERMINATION AND RESPONSE STRATEGIES.....</b>                          | <b>104</b> |
| <b>THE NIST ISCM AND CONTINUOUS MONITORING .....</b>                                  | <b>106</b> |
| <b>BCP, DRP AND COOP .....</b>                                                        | <b>107</b> |
| <b>BUSINESS IMPACT ANALYSIS.....</b>                                                  | <b>108</b> |
| <b>LOSS CALCULATIONS .....</b>                                                        | <b>109</b> |
| <b>THE NIST SUGGESTED STEPS AND CONTROLS FOR SUCCESSFUL CONTINGENCY PLANNING.....</b> | <b>111</b> |
| <b>THE NIST DEFINED CIKR, CIP, ISCP AND OEP .....</b>                                 | <b>112</b> |
| <b>RECOVERY VALIDATION AND PLAN DEACTIVATION THE NIST WAY.....</b>                    | <b>113</b> |
| <b>SECURITY THEORIES AND ACCESS CONTROL MODELS.....</b>                               | <b>117</b> |
| <b>DEFAULT DENY AND DEFAULT PERMIT.....</b>                                           | <b>117</b> |
| <b>TRUSTED SYSTEM VS UNTRUSTED SYSTEM .....</b>                                       | <b>117</b> |
| <b>THE COMPUTER SYSTEM ITSELF AS LARGELY AN UNTRUSTED SYSTEM.....</b>                 | <b>118</b> |
| <b>DEFENSE IN DEPTH .....</b>                                                         | <b>118</b> |
| <b>INFORMATION CLASSIFICATION, TCSEC, TNI AND TDI .....</b>                           | <b>119</b> |
| <b>MODELS .....</b>                                                                   | <b>121</b> |

|                                                                     |            |
|---------------------------------------------------------------------|------------|
| ACLs VERSUS CAPABILITIES .....                                      | 122        |
| THE AAA CONCEPT .....                                               | 123        |
| RECOMMENDED ACCESS CONTROL MEASURES.....                            | 124        |
| <b>STANDARDS AND GUIDELINES .....</b>                               | <b>130</b> |
| OVERVIEW OF C&A/AUTHORIZATION .....                                 | 130        |
| DIACAP .....                                                        | 135        |
| EAL.....                                                            | 135        |
| ATO .....                                                           | 136        |
| AUTHORIZATION DECISIONS, APPROACHES AND SUPPORTING EVIDENCE.....    | 137        |
| INFORMATION ASSURANCE AND THE IATF.....                             | 139        |
| THE NIST SPONSORING ORGANIZATION MODEL .....                        | 141        |
| NIST AND FIPS .....                                                 | 142        |
| THE NIST CERTIFICATION AND ACCREDITATION EFFORTS .....              | 143        |
| THE NIST PRINCIPLES OF SECURING INFORMATION SYSTEMS .....           | 143        |
| FIPS 200.....                                                       | 145        |
| THE OMB CIRCULAR A130 .....                                         | 145        |
| SCAP.....                                                           | 147        |
| THE RELATIONSHIP BETWEEN THE VARIOUS NIST RECOMMENDATIONS AND FISMA |            |
| COMPLIANCE.....                                                     | 147        |
| THE ISC2 CODE OF ETHICS .....                                       | 148        |
| THE SARBANES–OXLEY ACT AND THE COSO FRAMEWORK .....                 | 148        |
| SoGP .....                                                          | 149        |
| COMMON CRITERIA (CC).....                                           | 150        |
| HIPAA .....                                                         | 150        |
| OECD GUIDELINES .....                                               | 152        |
| CEI’S COMMANDMENTS OF ETHICS .....                                  | 153        |
| COBIT .....                                                         | 155        |
| ISO STANDARDS .....                                                 | 156        |
| VAL IT .....                                                        | 156        |
| NISPOM .....                                                        | 157        |
| OTHER STANDARDS .....                                               | 158        |
| RELEVANT LEGISLATIVE ACTS FROM A FEDERAL PERSPECTIVE.....           | 159        |
| RELEVANT OMB CIRCULARS AND HOMELAND SECURITY DIRECTIVES .....       | 160        |
| <b>SECURITY SYSTEM DESIGN .....</b>                                 | <b>165</b> |
| GENERAL GUIDELINES.....                                             | 165        |
| INFORMATION SECURITY ASSESSMENT METHODOLOGY THE NIST WAY.....       | 165        |
| DEVELOPMENT MODELS AND FRAMEWORKS .....                             | 166        |
| SOFTWARE TESTING.....                                               | 169        |
| PROGRAM REVIEW .....                                                | 172        |