



## **ISC CISSP**

Certified Information Systems  
Security Professional

Study Guide

Demo Version 1.0

**Leading The Way**  
in IT Testing And Certification Tools

**[www.testking.com](http://www.testking.com)**

## TABLE OF CONTENTS

<b>LIST OF TABLES</b> .....	<b>10</b>
<b>LIST OF FIGURES</b> .....	<b>10</b>
<b>LIST OF ABBREVIATIONS</b> .....	<b>11</b>
<b>Topic 1: Security Management</b> .....	<b>20</b>
<b>Section 1.1: Risk Assessment</b> .....	<b>20</b>
1.1.1: Risk Management.....	20
1.1.2: Identifying the Threats and Vulnerabilities.....	21
1.1.3: Assessing Asset Value.....	21
1.1.3.1: Quantitative Assessment.....	21
1.1.3.2: Qualitative Assessment.....	22
1.1.4: Handling Risk.....	22
<b>Section 1.2: Security Policies and Procedures</b> .....	<b>22</b>
1.2.1: The Objectives of a Security Policy .....	23
1.2.2: Standards, Guidelines and Procedures.....	24
1.2.3: Roles and Responsibility .....	24
<b>Section 1.3: Information Classification</b> .....	<b>25</b>
<b>Section 1.4: Security Training and Awareness</b> .....	<b>25</b>
<b>Topic 2: Access Control and Accountability</b> .....	<b>27</b>
<b>Section 2.1: Access Control Models</b> .....	<b>27</b>
2.1.1: Discretionary Access Control (DAC).....	27
2.1.2: Mandatory Access Control (MAC).....	28
2.1.3: Role-based Access Control (RBAC).....	28
<b>Section 2.2: Access Control Types</b> .....	<b>28</b>
<b>Section 2.3: Identification and Authentication</b> .....	<b>30</b>
2.3.1: Passwords .....	30
2.3.2: Tokens.....	30
2.3.3: Biometrics.....	31
2.3.4: Multifactor Authentication.....	31
2.3.5: Single Sign-On (SSO) .....	31
2.3.5.1: Kerberos.....	31
2.3.5.2: Secure European System and Applications in a Multivendor Environment (Sesame).....	32
2.3.5.3: KryptoKnight and NetSP.....	32
<b>Section 2.4: Access Control Systems</b> .....	<b>33</b>
2.4.1: Centralized Access Control.....	33

2.4.1.1: Remote Authentication Dial-In User Service (RADIUS) and DIAMETER	33
2.4.1.2: Terminal Access Controller Access Control System	33
2.4.2: Decentralized/Distributed Access Control	34
<b>Section 2.5: Threats Against Access Control</b>	<b>34</b>
2.5.1: Password Attacks	34
2.5.1.1: Dictionary Attacks	34
2.5.1.2: Brute-Force Attacks	34
2.5.2: Back Door Attacks	35
2.5.3: Spoofing	35
2.5.4: Man-in-the-Middle Attacks	35
2.5.5: Replay Attacks	35
2.5.6: Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks	36
2.5.7: TCP Hijacking	36
2.5.8: Social Engineering	36
2.5.9: Dumpster Diving	37
2.5.10: Software Exploitation	37
<b>Section 2.6: Monitoring and Intrusion Detection</b>	<b>37</b>
2.6.1: Monitoring	37
2.6.2: Intrusion Detection System (IDS)	38
2.6.2.1: Host-Based IDS (HIDS)	38
2.6.2.2: Network-Based IDS (NIDS)	38
2.6.2.3: Knowledge-Based IDS	39
2.6.2.4: Behavior-based IDS	39
2.6.3: Honeypots	39
<b>Section 2.7: Penetration Testing</b>	<b>39</b>
<b>Topic 3: Telecommunications and Network Security</b>	<b>41</b>
<b>Section 3.1: OSI Reference Model</b>	<b>41</b>
3.1.1: Inter-OSI Layer Interaction	42
<b>Section 3.2: Transmission Control Protocol/Internet Protocol (TCP/IP)</b>	<b>43</b>
3.2.1: TCP/IP Protocols	44
<b>Section 3.3: Communication and Network Security</b>	<b>46</b>
3.3.1: Types of Networks	46
3.3.2: Network Topologies	47
3.3.3: Network Cabling	48
3.3.3.1: Coaxial Cable	48
3.3.3.1.1: Thick Ethernet	48
3.3.3.1.2: Thin Ethernet	48
3.3.3.2: Twisted Pair Cable	48
3.3.3.2.1: UTP Cable Grades	49
3.3.3.2.2: STP Cable Grades	49
3.3.3.3: Fiber Optic Cable	50
3.3.3.4: Wireless Networks	50

3.3.3.4.1 Wireless Network Standards.....	51
3.3.3.4.2: Wireless Network Modes.....	52
3.3.3.4.3: Bluetooth.....	52
3.3.3.4.4: IrDA.....	53
3.3.4: Networking Devices.....	53
3.3.5: Network Technologies.....	55
3.3.5.1: Ethernet.....	55
3.3.5.2: Fast Ethernet.....	56
3.3.5.3: Gigabit Ethernet.....	56
3.3.5.4: Token Ring.....	57
3.3.5.4.1: Token Ring Operation.....	58
3.3.5.4.2: Early Token Release (ETR).....	58
3.3.6: Areas of the Network.....	58
<b>Section 3.4 Common Data Network Services.....</b>	<b>59</b>
3.4.1: File Transfer Protocol (FTP).....	59
3.4.2: Secure File Transfer Protocol (SFTP).....	59
3.4.3: Secure Shell (SSH) and Secure Shell version 2 (SSH-2).....	59
3.4.4: Trivial File Transfer Protocol (TFTP).....	60
<b>Section 3.5: Types of Data Networks.....</b>	<b>60</b>
<b>Section 3.6: Wide Area Networks.....</b>	<b>61</b>
3.6.1: Internet.....	62
3.6.2: Intranet.....	62
3.6.3: Extranet.....	62
3.6.4: WAN Technologies.....	62
3.6.4.1: Dedicated Lines.....	62
3.6.4.2: WAN Switching.....	62
3.6.4.2.1: Circuit-Switched Networks.....	62
3.6.4.2.2: Packet-Switched Networks.....	63
3.6.5: Network Address Translation (NAT).....	64
<b>Section 3.7: Remote Access.....</b>	<b>65</b>
3.7.1: Remote Access Requirements.....	67
3.7.2: Virtual Private Networks (VPNs).....	67
3.7.2.1: VPN Applications.....	67
3.7.2.1.1: Remote Access VPN.....	68
3.7.2.1.2: Intranet Access VPN.....	68
3.7.2.1.3: Extranet Access VPN.....	68
3.7.2.1.4: Integrating VPN in a Routed Intranet.....	68
3.7.2.2: VPN and Remote Access Protocols.....	69
3.7.2.2.1: Point-to-Point Protocol (PPP).....	69
3.7.2.2.2: Point-to-Point Tunneling Protocol (PPTP).....	70
3.7.2.2.3: Layer 2 Tunneling Protocol (L2TP).....	70
3.7.2.2.4: IP Security Protocol (IPSec).....	71
3.7.2.2.5: Remote Authentication Dial-In User Service (RADIUS) and DIAMETER.....	71
3.7.2.2.6: Terminal Access Controller Access Control System.....	71

Section 3.8: E-Mail Security.....	72
3.8.1: E-Mail Security Issues.....	72
3.8.2: E-Mail Security Solutions.....	73
Section 3.9: Voice Communications.....	73
<b>Topic 4: Cryptography.....</b>	<b>75</b>
Section 4.1: Encryption.....	75
4.1.1: Symmetric Algorithms.....	75
4.1.2: Asymmetric Algorithms.....	76
Section 4.2: Advanced Encryption Standard (Rijndael).....	77
Section 4.3: Public Key Infrastructure (PKI).....	77
4.3.1: Components of a PKI.....	77
4.3.2: Digital Certificates.....	78
4.3.2.1: Certificate Policies.....	78
4.3.2.2: Certificate Practice Statements.....	78
4.3.2.3: Revocation.....	78
4.3.3: Standards and Protocols.....	79
4.3.4: Key Management Life Cycle.....	80
4.3.4.1: Centralized versus Decentralized Keys.....	80
4.3.4.1.1: Storage.....	80
4.3.4.1.2: Software Storage.....	81
4.3.4.1.3: Hardware Storage.....	81
4.3.4.2: Centralized Key Management.....	81
4.3.4.2.1: Private Key Protection.....	81
4.3.4.2.2: Key Escrow.....	81
4.3.4.2.3: Certificate Expiration.....	81
4.3.4.2.4: Certification Revocation List.....	81
4.3.5: M of N Control.....	82
4.3.6: Key Usage.....	83
<b>Topic 5: System Architecture and Models.....</b>	<b>84</b>
Section 5.1: Computer Architecture.....	84
5.1.1: The Central Processing Unit (CPU).....	84
5.1.2: Memory.....	84
5.1.3: Data Storage.....	85
5.1.4: Input and Output Devices.....	85
Section 5.2: Security Policy and Computer Architecture.....	86
5.2.1: Vulnerabilities.....	86
5.2.2: Safeguards.....	86
Section 5.3: Security Mechanisms.....	87
5.3.1: Process Isolation.....	87
5.3.2: Single-State and Multistate Systems.....	87

5.3.4: Rings of Protection.....	88
5.3.5: Trusted Computer Base (TCB).....	88
<b>Section 5.4: Security Models.....</b>	<b>89</b>
5.4.1: State Machine Model.....	89
5.4.2: Bell-LaPadula Model.....	89
5.4.3: Biba Integrity Model.....	90
5.4.4: Clark-Wilson Integrity Model.....	90
5.4.5: Information Flow Model.....	91
5.4.6: Noninterference Model.....	91
5.4.7: Take-Grant Model.....	91
5.4.8: Access Control Matrix.....	91
5.4.9: Brewer and Nash Model.....	91
<b>Topic 6: Operational Security.....</b>	<b>92</b>
<b>Section 6.1: Employees and Operational Security.....</b>	<b>92</b>
6.1.1: New-Hire Orientation.....	92
6.1.2: Separation of Duties.....	92
6.1.3: Job Rotation.....	93
6.1.4: Least Privilege.....	93
6.1.5: Mandatory Vacations.....	93
6.1.6: Termination.....	93
<b>Section 6.2: Threats, Vulnerabilities and Attacks.....</b>	<b>93</b>
6.2.1: Threats.....	93
6.2.1.1: Malicious Activities.....	94
6.2.1.2: Accidental Loss.....	94
6.2.1.3: Inappropriate Activities.....	94
6.2.2: Vulnerabilities and Attacks.....	94
6.2.2.1: Traffic Analysis.....	94
6.2.2.2: Default and Maintenance Accounts.....	94
6.2.2.3: Data-Scavenging Attacks.....	95
6.2.2.4: Initial Program Load Vulnerabilities.....	95
6.2.2.5: Social Engineering.....	95
6.2.2.6: Network Address Hijacking.....	95
<b>Section 6.3: Auditing, Monitoring and Intrusion Detection.....</b>	<b>95</b>
6.3.1: Auditing and Audit Trails.....	96
6.3.2: Monitoring.....	96
<b>Section 6.4: Controls for Operational Security.....</b>	<b>96</b>
<b>Section 6.5: Orange Book Controls.....</b>	<b>97</b>
6.5.1: Covert Channel Analysis.....	98
6.5.2: Trusted Facility Management.....	98
6.5.3: Trusted Recovery.....	99
6.5.3.1: Failure Preparation.....	99
6.5.3.2: System Recovery.....	99

<b>Section 6.6: Operations Controls .....</b>	<b>99</b>
6.6.1: Resource Protection.....	99
6.6.2: Hardware Controls.....	100
6.6.3: Software Controls.....	100
6.6.4: Privileged Entity Controls .....	100
6.6.5: Media Resource Protection.....	101
6.6.5.1: Media Security Controls.....	101
6.6.5.2: Media Viability Controls.....	101
6.6.6: Physical Access Controls.....	102
<b>Topic 7: Application and System Development.....</b>	<b>103</b>
<b>Section 7.1: Malicious Code .....</b>	<b>103</b>
7.1.1: Viruses.....	103
7.1.2: Worms.....	104
7.1.3: Logic Bombs.....	104
7.1.4: Trojan Horses.....	104
7.1.5: Active Content.....	104
7.1.6: Spyware.....	104
7.1.7: SQL Injection.....	105
<b>Section 7.2: System Development Life Cycle (SDLC).....</b>	<b>105</b>
<b>Section 7.3: Application Development .....</b>	<b>105</b>
7.3.1: The Waterfall Model.....	106
7.3.2: The Spiral Model.....	106
7.3.3: Cost Estimation Models.....	107
<b>Section 7.4: Information Security and the Life Cycle Model .....</b>	<b>107</b>
7.4.1: Testing.....	107
7.4.2: The Software Maintenance and Change Control.....	107
<b>Section 7.5: Object-Oriented Programming.....</b>	<b>108</b>
<b>Section 7.6: Database Management .....</b>	<b>109</b>
7.6.1: Transaction Processing.....	109
7.6.2: Data Warehousing.....	111
7.6.3: Data Mining.....	111
7.6.4: Data Dictionaries.....	111
7.6.5: Knowledge Management.....	112
<b>Topic 8: Business Continuity Planning and Disaster Recovery Planning.....</b>	<b>113</b>
<b>Section 8.1: Business Continuity Planning (BCP).....</b>	<b>113</b>
8.1.1: Project Scope and Planning .....	113
8.1.1.1: Business Organization Analysis.....	113
8.1.1.2: BCP Team Selection.....	114
8.1.1.3: Resource Requirements.....	114
8.1.2: Business Impact Assessment (BIA) .....	114

8.1.2.1: Priority Identification.....	115
8.1.2.2: Risk Identification.....	115
8.1.2.3: Likelihood Assessment.....	115
8.1.2.4: Impact Assessment.....	115
8.1.3: Continuity Planning.....	116
8.1.3.1: Strategy Development.....	116
8.1.3.2: Provisions and Processes.....	116
8.1.4: Plan Approval and Implementation.....	117
8.1.5: BCP Documentation.....	117
8.1.5.1: Continuity Planning Goals.....	117
8.1.5.2: Statement of Importance.....	117
8.1.5.3: Statement of Priorities.....	118
8.1.5.4: Statement of Organizational Responsibility.....	118
8.1.5.5: Statement of Urgency and Timing.....	118
8.1.5.6: Risk Assessment.....	118
8.1.5.7: Risk Acceptance/Mitigation.....	118
8.1.5.8: Vital Records Program.....	119
8.1.5.9: Emergency Response Guidelines.....	119
<b>Section 8.2: Disaster Recovery Planning (DRP) .....</b>	<b>119</b>
8.2.1 Potential Disasters.....	119
8.2.1.1: Natural Disasters.....	119
8.2.1.2: Man-Made Disasters.....	120
8.2.2: Recovery Strategies.....	120
8.2.2.1: Emergency Response.....	120
8.2.2.2: Personnel Notification.....	121
8.2.2.3: Business Unit Priorities.....	121
8.2.2.4: Crisis Management.....	121
8.2.2.5: Emergency Communications.....	121
8.2.3: Alternate Recovery Sites.....	122
8.2.3.1: Cold Sites.....	122
8.2.3.2: Hot Sites.....	122
8.2.3.3: Warm Sites.....	123
8.2.3.4: Mobile Sites.....	123
8.2.3.5: Mutual Assistance Agreements.....	123
8.2.4: Database Recovery.....	123
8.2.5: Training and Documentation.....	124
8.2.6: Testing and Maintenance.....	124
<b>Topic 9: Law, Investigation and Ethics.....</b>	<b>126</b>
<b>Section 9.1: Computer Crimes.....</b>	<b>126</b>
<b>Section 9.2: Common Law .....</b>	<b>126</b>
9.2.1: Intellectual Property Law.....	127
9.2.2: Information Privacy and Privacy Laws.....	128
9.2.2.1: Privacy Policy.....	128
9.2.2.2: Privacy-Related Legislation and Guidelines.....	128
9.2.2.3: The Platform for Privacy Preferences (P3P).....	129

9.2.2.4: Electronic Monitoring.....	129
9.2.3: Computer Security, Privacy, and Crime Laws.....	130
<b>Section 9.3: Computer Forensics .....</b>	<b>133</b>
9.3.1: Evidence.....	133
9.3.1.1: Categories of Evidence.....	134
9.3.1.2 Chain of Custody .....	134
9.3.2: Investigation .....	135
9.3.2.1: The First Responder.....	135
9.3.2.2 The Investigator.....	136
9.3.2.3 The Crime Scene Technician.....	136
<b>Section 9.4: Liability.....</b>	<b>136</b>
<b>Section 9.5: Ethics .....</b>	<b>137</b>
9.5.1: (ISC) <sup>2</sup> Code of Ethics.....	137
9.5.2: The Computer Ethics Institute’s Ten Commandments of Computer Ethics .....	137
9.5.3: The Internet Activities Board (IAB) Ethics and the Internet.....	138
9.5.4: The U.S. Department of Health, Education, and Welfare Code of Fair Information Practices.....	138
9.5.5: The Organization for Economic Cooperation and Development (OECD).....	138
<b>Topic 10: Physical Security.....</b>	<b>140</b>
<b>Section 10.1: Administrative Physical Security Controls.....</b>	<b>140</b>
10.1.1: Facility Requirements Planning .....	140
10.1.2: Secure Facility Design.....	141
10.1.3: Facility Security Management .....	141
10.1.4: Administrative Personnel Controls.....	142
<b>Section 10.2: Physical Access Controls .....</b>	<b>142</b>
<b>Section 10.3: Technical Physical Security Controls.....</b>	<b>144</b>
<b>Section 10.4: Environment and Personnel Safety.....</b>	<b>144</b>
10.4.1: Electrical Power Supply.....	144
10.4.2: Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI).....	146
10.4.3: Heating, Ventilating, and Air Conditioning (HVAC).....	146
10.4.4: Water.....	146
10.4.5: Fire Detection and Fire Suppression.....	147
10.4.5.1: Fire Detection Systems.....	147
10.4.5.2: Fire Suppression Systems.....	147
<b>Section 10.5: Equipment Failure.....</b>	<b>149</b>
<b>INDEX .....</b>	<b>150</b>

## LIST OF TABLES

Table 1.1: Threat, Vulnerability and Risk.....	22
Table 1.2: Roles and Responsibilities.....	25
Table 1.3: Commercial and Military Information Classifications.....	26
Table 3.1: Coaxial Cable Specifications.....	49
Table 3.2: EIA/TIA UTP Cable Grades.....	50
Table 3.3: Types of Wireless Network and Their Standards.....	51
Table 3.4: Coaxial Cable for Ethernet.....	56
Table 3.5: Twisted-Pair and Fiber Optic Cable for Ethernet.....	56
Table 3.6: Fast Ethernet Cabling and Distance Limitations.....	57
Table 3.7: Gigabit Ethernet Cabling and Distance Limitations.....	57
Table 3.8: Network Definitions.....	61
Table 6.1: TCSEC Hierarchical Classes of Security.....	98
Table 7.1: Database Terminology.....	111
Table 10.1: Common Power Supply Problems.....	146
Table 10.2: Possible Damage from Static Electricity.....	147
Table 10.3: Fire Extinguisher Classes.....	149

## LIST OF FIGURES

Figure 3.1: The OSI Reference Model.....	42
Figure 3.2: OSI and TCP/IP.....	45
Figure 3.3: The Star Topology.....	48
Figure 3.4: The Bus Topology.....	48
Figure 3.5: The Ring Topology.....	48
Figure 3.6: The Mesh Topology.....	48
Figure 5.1: Rings of Protection.....	89

## **LIST OF ABBREVIATIONS**

3DES	Triple Data Encryption Standard (Triple DES)
AAA	Authentication, Authorization, and Accounting
ACK	Acknowledgement (Message)
ACL	Access Control List
ADSL	Asymmetrical Digital Subscriber Line
AES	Advanced Encryption Standard
ALE	Annual Loss Expectancy
ALU	Arithmetic Logic Unit
AM	Active Monitor (Token Ring)
ANSI	American National Standards Institute
ARO	Annual Rate of Occurrence
ARP	Address Resolution Protocol
AS	Authentication Server (Kerberos)
ATM	Asynchronous Transfer Mode
AV	Asset Value
BCP	Business Continuity Planning
BGP	Border Gateway Protocol
Etc	Etc

## LIST OF TABLES

Table 1.1: Threat, Vulnerability and Risk .....	22
Table 1.2: Roles and Responsibilities.....	25
Table 1.3: Commercial and Military Information Classifications.....	26
Table 3.1: Coaxial Cable Specifications.....	49
Table 3.2: EIA/TIA UTP Cable Grades.....	50
Table 3.3: Types of Wireless Network and Their Standards.....	51
Table 3.4: Coaxial Cable for Ethernet.....	56
Table 3.5: Twisted-Pair and Fiber Optic Cable for Ethernet.....	56
Table 3.6: Fast Ethernet Cabling and Distance Limitations.....	57
Table 3.7: Gigabit Ethernet Cabling and Distance Limitations.....	57
Table 3.8: Network Definitions.....	61
Table 6.1: TCSEC Hierarchical Classes of Security .....	98
Table 7.1: Database Terminology.....	111
Table 10.1: Common Power Supply Problems.....	146
Table 10.2: Possible Damage from Static Electricity.....	147
Table 10.3: Fire Extinguisher Classes.....	149

## LIST OF FIGURES

Figure 3.1: The OSI Reference Model.....	42
Figure 3.2: OSI and TCP/IP.....	45
Figure 3.3: The Star Topology.....	48
Figure 3.4: The Bus Topology.....	48
Figure 3.5: The Ring Topology.....	48
Figure 3.6: The Mesh Topology.....	48
Figure 5.1: Rings of Protection.....	89

# Certified Information Systems Security Professional

## Certifications:

**Certified Information Systems Security Professional (CISSP)  
(ISC)<sup>2</sup> Associate for CISSP (Associate of (ISC)<sup>2</sup>)**

**Core  
Core**

## Prerequisites:

At least 4 years' experience or a college degree with 3 years' experience as a practicing security professional. Candidates without the required experience can become an (ISC)<sup>2</sup> Associate for CISSP (Associate of (ISC)<sup>2</sup>).

## About This Study Guide

This Study Guide provides all the information required to pass the (ISC)<sup>2</sup> CISSP exam. It however, does not represent a complete reference work but is organized around the specific skills that are tested in the exam. Thus, the information contained Study Guide is specific to the CISSP exam and not Information Systems security. It includes the information required to answer questions related to the CISSP exam. Topics covered in this Study Guide includes: Understanding Security Management, Risk Management, and Risk Assessment; Identifying Threats and Vulnerabilities; Performing Quantitative and Qualitative Assessment of Assets; Understanding Security Policies and Procedures, including Security Policy Objectives, Security Policy Standards, Guidelines and Procedures, and the Various Types of Information Classification; Providing Security Training and Education; Understanding and Implementing Access Control and Accountability; Understanding the Various Access Control Models, including Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-based Access Control (RBAC); Understanding Access Control Types, including Passwords, Tokens, Biometrics, Multifactor Authentication, Single Sign-On, Kerberos, Secure European System and Applications in a Multivendor Environment (SESAME), KryptoKnight and NetSP; Understanding Access Control Systems, including Centralized Access Control, Remote Authentication Dial-In User Service (RADIUS) and DIAMETER, and Terminal Access Controller Access Control System, as well as Decentralized/Distributed Access Control; Understanding Threats against Access Control, including Password Attacks, Dictionary Attacks, Brute-Force Attacks, Back Door Attacks, Spoofing, Man-in-the-Middle Attacks, Replay Attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, TCP Hijacking, Social Engineering, Dumpster Diving and Software Exploitation; Monitoring Information Systems for Possible Intrusion and Implementing Intrusion Detection; Understanding Intrusion Detection System (IDS) and Honeypots; Performing Penetration Testing; Understanding Telecommunications and Network Security; Understanding the OSI Reference Model; Understanding the Protocols of the Transmission Control Protocol/Internet Protocol (TCP/IP) Architecture; Understanding and Implementing Communication and Network Security; Identifying the Various Types of Networks, Network Topologies and Network Cabling; Understanding Wireless Networks, including IEEE 802.11x, Bluetooth, and IrDA; Understanding Network Technologies, including Ethernet, and Token Ring; Understanding Data Network Services, including File Transfer Services (FTP), Secure File Transfer Protocol (SFTP), Trivial File Transfer Protocol (TFTP), Secure Shell (SSH) and Secure Shell version 2 (SSH-2), Understanding Wide Area Networks, including the Internet, Intranets, and Extranets, Understanding WAN Technologies, including Dedicated Lines, WAN Switching, Circuit-Switched

Networks, and Packet-Switched Networks Understanding Network Address Translation (NAT); Understanding and Implementing Remote Access; Understanding Virtual Private Networks (VPNs) and VPN Applications; Integrating VPN in a Routed Intranet; Understanding and Implementing E-mail Security and E-mail Security Solutions; Understanding and Implementing Cryptography; Understanding Data Encryption, including Symmetric and Asymmetric Algorithms; Understanding and Implementing a Public Key Infrastructure (PKI); Understanding Certificates and Certificate Policies; Understanding System Architecture, including Computer Architecture; Understanding Security Policies and Computer Architectures; Implementing Security Mechanisms for Computer Architectures, including Process Isolation, Rings of Protection and Trusted Computer Base (TCB); Understanding Single-State and Multistate Systems; Understanding the Various Security Models, including the State Machine Model, the Bell-LaPadula Model, the Biba Integrity Model, the Clark-Wilson Integrity Model, the Information Flow Model, the Noninterference Model, the Take-Grant Model, the Access Control Matrix, and the Brewer and Nash Model; Understanding and Implementing Operational Security; Understanding the Role of Employees in Operational Security; Implementing New-Hire Orientation, Understanding the Importance of Separation of Duties and Job Rotation; Understanding Threats and Vulnerabilities to Operational Security, including Traffic Analysis, Insecurities Associated with Default and Maintenance Accounts, Data-Scavenging Attacks, Initial Program Load Vulnerabilities, Social Engineering, and Network Address Hijacking; Understanding the Importance of Auditing, Monitoring and Intrusion Detection; Understanding Audit Trails; Understanding Controls for Operational Security, including Orange Book Controls; Understanding and Implementing Operations Controls, including Resource Protection, Hardware Controls, Software Controls, Privileged Entity Controls, Media Security Controls, Media Viability Controls, and Physical Access Controls; Understanding Application and System Development; Understanding, Identifying and Protecting against Malicious Code, including Viruses, Worms, Logic Bombs, Trojan Horses, Active Content, Spyware, and SQL Injection; Understanding the System Development Life Cycle (SDLC); Understanding Software Development Models, including the Waterfall Model, the Spiral Model, and Cost Estimation Models; Understanding and Implementing Information Security and the Life Cycle Model; Understanding Object-Oriented Programming; Understanding Implementing Secure Database Management; Understanding the Importance Business Continuity Planning and Disaster Recovery Planning; Understanding and Implementing Alternate Recovery Sites, including Cold Sites, Hot Sites, Warm Sites, and Mobile Sites; Understanding Computer Crimes, including the Laws Related to Computer Crimes and the of Computer Crimes Understanding Information Privacy and Privacy Laws; Understanding Computer Forensics; Understanding Ethical Computing and the Various Codes of Ethics; Implementing Physical Security; Designing Secure Facilities; Implementing Physical Access Controls; Understanding Environment and Personnel Safety; Implementing Environmental Controls, including Heating, Ventilating, and Air Conditioning (HVAC), and Fire Detection and Suppression; and Understanding Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI)

### **Intended Audience**

This Study Guide is targeted specifically at people who wish to take the (ISC)<sup>2</sup> CISSP exam. This information in this Study Guide is specific to the exam and is not a complete reference work. Although our Study Guides are aimed at new comers to the world of IT, the concepts dealt with in the exam, and consequently in this Study Guide are rather complex. We therefore suggest that a sound knowledge of CompTIA's A+, N+ and Server+ course work material would be advantageous.

### **How To Use This Study Guide**

To benefit from this Study Guide we recommend that you:

- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work.

**Note:** Remember to pay special attention to these note boxes as they contain important additional information that is specific to the exam.

- Perform all labs that are included in this Study Guide to gain practical experience, referring back to the text so that you understand the information better. Remember, it is easier to understand how tasks are performed by practicing those tasks rather than trying to memorize each step.
- Be sure that you have studied and understand the entire Study Guide before you take the exam.

Good luck!

# Topic 1: Security Management

Security management concepts and principles are inherent elements in a security policy and solution deployment. They encompass of critical documents, such as policies, procedures, and guidelines that define the basic parameters needed for a secure an information system. These documents identify the organization's information assets and define the organization security practices.

The primary goals and objectives of security are contained within the **CIA Triad**, which is the three primary security principles: confidentiality, integrity, and availability. Security controls must address one or more of these three principles.

## Section 1.1: Risk Assessment

Risk is the possibility of experiencing some form of loss. It does not mean the risk will be realized, but that it has the potential to occur. Risk management is used to determine what risks are potential threats and to deal with these risks. By taking a proactive approach to risks, the damage that can occur from them is minimized. Risk identification is the process of ascertaining what threats pose a risk to an organization. There are many different types of risks that can affect an organization. Each business must identify the risks they may be in danger of confronting. Disasters can be naturally occurring or the result of accidents and malfunctions.

Natural disasters include storms, floods, fires, earthquakes, tornadoes, or any other environmental event. They also include situations that may cause damage to an organization, such as when a fire breaks out due to faulty wiring, a pipe bursts, or a power outage occurs. In addition to these risks, the organization is commonly at risk for equipment failures. There are a number of different risks that result from malicious persons and the programs they use and disseminate. Trojan horse attacks, viruses, hackers, and various other attacks can devastate an organization as effectively as any natural disaster. An attack on systems can result in disruption of services or the modification, damage, or destruction of data. Internal risks are risks in which consequences result from the actions of persons employed by an organization. Software and data are also targets of corporate theft. Employees may steal installation CDs or make copies of software to install at home. A single program can cost one thousand dollars or more, while copied CDs that are illegally installed could result in piracy charges and legal liability. If an employee takes sensitive data from a company and sells it to a competitor, the company could lose millions of dollars or face liability suits or even criminal charges if the stolen data breaches client confidentiality.

### 1.1.1: Risk Management

Risk management is the act of determining what threats the organization faces, analyzing vulnerabilities to assess the threat level, and determining how risk should be dealt with. This could involve developing a risk-management team, identifying threats and vulnerabilities, placing a value on the organization's assets, and determining the risks that are uncover will be dealt with. There are three important concepts in risk management: **threat**, which is a man-made or natural event that could have a negative impact on the organization; **vulnerability**, which is a potential weakness resulting from a flaw, loophole, oversight, or

#### Confidentiality

Confidentiality is the process of ensuring that sensitive information is not disclosed to unauthorized persons. When there is an unintentional release of information, confidentiality is lost. Attacks on confidentiality include sniffing, keystroke monitoring, and shoulder surfing

#### Integrity

Integrity is the process of ensuring that data is consistent and that it has not modified without authorization. This applies to data in use, data in storage and data in transit.

#### Availability

Availability ensures that data and systems are always available and can be accessed by authorized personnel whenever needed.

error that could be exploited to violate system security policy; and **controls**, which can be corrective, detective, preventive, or deterrent mechanisms that an organization can use to restrain, regulate, or reduce vulnerabilities.

### 1.1.2: Identifying the Threats and Vulnerabilities

Identifying threats and vulnerabilities is an important part of the risk-management process. Threats can occur as a result of human or natural factors, and can be caused by internal or external events. Threats can also occur because of errors in computer code, accidental buffer overflows, or the unintentional actions of employees.

You can start to analyze the threats, vulnerabilities, and risks the organization faces by creating a table such as the one shown in Table 1.1. This helps demonstrate the relationship among threats, vulnerabilities, and risk. For example, an intruder can represent a threat that exposes the organization to theft of equipment because there is no security guard or controlled entrance.

Table 1.1: Threat, Vulnerability and Risk

Threat	Vulnerability	Risk
Intruder	No security guard or controlled entrance	Theft
Hacker	Misconfigured firewall	Stolen credit card information
Current employee	Poor accountability; no audit policy	Loss of integrity; altered data
Fire	Insufficient fire control	Damage or loss of life
Hurricane	Insufficient preparation	Damage or loss of life
Virus	Out-of-date antivirus software	Virus infection and loss of productivity
Hard drive failure	No data backup	Data loss and unrecoverable downtime

### 1.1.3: Assessing Asset Value

Identifying the assets that are the most crucial to the organization and that should be protected is as important as identifying threats and vulnerabilities because it would be foolish to exceed the value of the asset by spending more on the countermeasure than the asset is worth. Organizations usually have limited funds and resources, so countermeasures must be effectively deployed to protect the most critical assets. For this reason you must assess the value of assets held by the organization. This can be a quantitative assessment, in monetary value, or a qualitative assessment, in importance.

Etc.