

Table of Contents

<u>PREFACE</u>	6
<u>SECURITY THEORIES</u>	7
THE COMPUTER SYSTEM ITSELF AS LARGELY AN UNTRUSTED SYSTEM.....	7
DEFENSE IN DEPTH	8
VULNERABILITIES	8
SECURITY MEASURES	14
STANDARDS, GUIDELINES AND LAWS	16
<u>INFORMATION SECURITY MANAGEMENT AND GOVERNANCE</u>	18
IS MANAGEMENT ACTIVITIES	18
INFORMATION MANAGEMENT POLICY.....	19
ORGANIZATIONAL STRUCTURE AND SUPPORT	19
THE ROLE OF THE INFORMATION SECURITY MANAGER	21
IS CONTROL CLASSIFICATION	21
GENERAL CONTROLS VS APPLICATION CONTROLS	22
ENVIRONMENTAL CONTROLS	24
INTERNAL PREVENTIVE CONTROLS VERSUS COMPENSATING CONTROLS.....	25
ACCESS CONTROL MODELS	25
ACLs VERSUS CAPABILITIES.....	26
WHAT IS ORANGE BOOK, BY THE WAY?	26
TYPES OF ACCESS CONTROL.....	27
THE AAA CONCEPT	27
PRACTICAL ACCESS CONTROL MEASURES.....	28
ESTABLISHING ACCOUNTABILITY THROUGH EVENT LOGGING.....	30
IS GOVERNANCE GUIDANCE	31
BASIC OUTCOMES OF IS GOVERNANCE	32
<u>THE AUDIT PROCESS</u>	32
WHAT IS AUDITING?.....	33
THE ROLE OF AN AUDITOR	34
THE AUDIT PROCESS FLOW	34
OVERALL STRATEGIES.....	37
AUDIT PLANNING	38
RECOMMENDED TYPES OF AUDIT	42
HIGH LEVEL AUDIT RISKS IN GENERAL	44
CONFLICTS OF INTEREST	46
EXAMPLE AUDIT OBJECTIVES AND PROCEDURES	46
AUDIT FIELDWORKS	50
AUDIT PROGRAM	52

AUDIT REPORT	52
AUDIT FOLLOW-UP.....	53
AUDIT ASSESSMENT	53
SPECIAL NOTES ON THE RISK OF PENETRATION TESTING	54
SPECIAL NOTES ON COMPUTER FORENSICS	54
THE INFOSEC ASSESSMENT METHODOLOGY (IAM)	56
COVERT CHANNEL ANALYSIS	56

STANDARDS AND GUIDELINES 57

THE SARBANES–OXLEY ACT AND THE COSO FRAMEWORK.....	57
COMMON CRITERIA (CC)	58
HIPAA.....	59
OECD GUIDELINES	59
CEI’S COMMANDMENTS OF ETHICS.....	60

IT STRATEGIC PLANNING 61

IT STRATEGIC PLANNING DEFINED.....	61
IT OPERATIONS MANAGEMENT	62
DATA STORAGE STRATEGY	63
THE ROLE OF IS AUDITING IN THE PLANNING PROCESS	64
IN-HOUSE OR OUT-SOURCE?	64
AVOIDING CONFLICTS OF INTERESTS	65
SPECIAL CONCERNS ON M & A.....	65
OUTSOURCING IT AUDIT	66
INFORMATION SECURITY PROGRAM AND POLICY DEVELOPMENT FROM A STRATEGIC PERSPECTIVE	66
POLICY AND PROGRAM MANAGEMENT FROM A STRATEGIC PERSPECTIVE	68
INCIDENT RESPONSE (IR) FROM A STRATEGIC PERSPECTIVE	70
BALANCED SCORECARD.....	70
BUSINESS PROCESS REENGINEERING	71
HR AND SECURITY	72
AGENCY THEORY.....	72
BUSINESS ETHICS.....	72
SOCIAL RESPONSIBILITY.....	73

PROTECTION OF INFORMATION ASSETS THROUGH SECURITY POLICY..... 73

INFORMATION ASSETS DEFINED	73
DATA CLASSIFICATIONS AND LAYER OF RESPONSIBILITIES.....	74
HANDLING CLASSIFIED MATERIAL IN THE PRACTICAL WORLD.....	75
SECURITY POLICY.....	75
EFFECTIVE SECURITY MANAGEMENT PRACTICES AND HR.....	78
OWNERSHIP & RESPONSIBILITY	78
SECURITY AWARENESS TRAINING	79
SECURITY MODELS AND MODES OF OPERATIONS.....	80
EXAMPLE POLICY	81
CONSEQUENCES OF VIOLATIONS	82

EVALUATION.....	82
DEVSING YOUR OWN CLASSIFICATION SCHEME	83
CHANGE CONTROL.....	83
INFORMATION RETENTION & DISPOSAL PROCEDURES.....	84
SPECIAL DRILLS ON POLICIES.....	85
INTERNET SECURITY.....	85
FIREWALL SECURITY	86
VIRUS SECURITY	86
WEB SERVER SECURITY	86
NAME RESOLUTION SECURITY.....	87
MAIL SERVER SECURITY	87
RAS SERVER SECURITY.....	87
PROXY SERVER SECURITY	87
AUTHENTICATION SERVER SECURITY	88
PHYSICAL AND ENVIRONMENTAL SECURITY.....	88
PHYSICAL SITE MANAGEMENT	89
EQUIPMENT AND MEDIA MANAGEMENT	90

RISK MANAGEMENT, BCP, BIA AND RESPONSE MANAGEMENT 91

RISK MANAGEMENT DEFINED.....	91
THE RISK MANAGEMENT STEPS	91
RISK MANAGEMENT AND THE IS MANAGER	92
PLANNING AND SCOPING OF THE ASSESSMENT OF RISK	92
METHODOLOGIES FOR PROPER ASSESSMENT OF RISK.....	93
BCP DEFINED.....	94
BCP VS BPCP VS DRP.....	94
BCP PHASES	94
STAKEHOLDERS AND CRISIS COMMUNICATIONS.....	95
THE RISK ASSESSMENT FLOW	96
RISK VS THREAT AND VULNERABILITY	98
IDENTIFYING RISKS	99
LOSS CALCULATIONS.....	99
BUSINESS IMPACT ANALYSIS DEFINED	100
BIA GOALS AND STEPS	101
BIA CHECKLIST	101
PREPARING FOR EMERGENCY RESPONSE.....	103
RESPONDING TO INCIDENTS AND MANAGING RECOVERY.....	104
TESTING THE PLAN.....	106
USER ACCEPTANCE.....	107
PLAN MAINTENANCE	107
INCIDENT HANDLING	107
ERT FORMATION.....	108
ER PLANNING AND PREPARATION	108
COVERAGE, GOAL AND SCOPE	109
EMERGENCY PRIORITIES.....	109
EMERGENCY REPORTING PROCEDURE	110
EMERGENCY ESCALATION PROCEDURE	110
INCIDENT MONITORING	111
CSIRT	111

IS PROGRAM MANAGEMENT, PROJECT MANAGEMENT AND CHANGE MANAGEMENT..... 112

INFORMATION SECURITY PLAN 112
INFORMATION SECURITY BASELINES..... 113
PROJECT MANAGEMENT DEFINED 113
CHANGE MANAGEMENT DEFINED..... 114
CHANGE MANAGEMENT STRATEGIES 115
CHANGE MANAGEMENT VS CHANGE CONTROL..... 116
CONFIGURATION MANAGEMENT 116
GENERAL GUIDELINES 117
SYSTEM CHANGE CONTROL..... 117
VULNERABILITY & PATCH MANAGEMENT 118

APPLICATION DEVELOPMENT, TESTING AND SECURITY 119

SOFTWARE DEVELOPMENT APPROACHES: THE PROS & CONS 119
FROM A PRACTICAL STANDPOINT, YOU MAY HAVE TO REALIZE THAT IN MANY COMPLEX SITUATIONS YOU JUST
HAVE TO USE A HYBRID APPROACH 119
SOFTWARE DEVELOPMENT PROCESSES AND MODELS..... 120
CMM AND CMMI 121
OBJECT ORIENTED DESIGN..... 122
SOFTWARE TESTING 122
ERP SECURITY 126

BASIC NETWORKING TECHNOTES 127

NETWORK INFRASTRUCTURE IMPLEMENTATION..... 128
OSI (OPEN SYSTEM INTERCONNECT)..... 129
LAN NETWORKING 129
ROUTING AND SWITCHING..... 130
IP ADDRESSING..... 131
WIRELESS BASED LOCAL AREA NETWORKING 132
EMERGING WIRELESS SECURITY STANDARDS 133
VOIP..... 134
WAN NETWORKING 134
NETWORK SECURITY DEVICES..... 135
CRYPTOGRAPHY 136
ESCROWED ENCRYPTION STANDARD (EES)..... 137
PLATFORM FOR PRIVACY PREFERENCES PROJECT (P3P)..... 137
EMERGING PROCESSOR TECHNOLOGIES 138
IM SECURITY 139
SYSTEM IMPLEMENTATION & MAINTENANCE 139
SPECIAL DEVICES AND TECHNOLOGIES..... 140
RFID 140
IMAGING TECHNOLOGIES..... 141

LINUX TECHNOTES 141

WINDOWS TECHNOTES..... 142

TCP/IP SPECIFIC SECURITY RISKS 143

WINDOWS SPECIFIC RISKS AND COUNTERMEASURES 149

LINUX SPECIFIC RISKS AND COUNTERMEASURES 152

NETWARE SPECIFIC RISKS AND COUNTERMEASURES 155

WIRELESS SPECIFIC RISKS AND COUNTERMEASURES 157

DATABASE SPECIFIC RISKS AND COUNTERMEASURES 158

CONCEALING HARD DISK DATA 159

PRACTICE REVIEW QUESTIONS..... 161

CONTENTS UPDATE..... 161

ExamREVIEW is an independent content developer not associated/affiliated with the certification vendor of the CISA/CISM exams. These certification exams are the trademarks of the corresponding certification vendor. We at ExamREVIEW develop study material entirely on our own without official endorsement of any kind. And very importantly, absolutely NO braindumps!