CIS 521/421
Introduction to Information Assurance

Text *Management of Information Security* by Whitman and Mattord 2nd Edition
Lecture notes posted on Blackboard

Course Objective and Overview:

This course is designed to give students an understanding of information assurance concepts. The course is rigorous. You are advised to pay careful attention to the class lectures and especially sample problems and lab exercises. Exam questions are based primarily on the material covered in class and are designed to test your *understanding of the underlying concepts of information assurance.* Note we will cover information security management and the Common Body of Knowledge of the CISSP Exam. I urge you to ask questions if you don't understand. You can come during my office hours, email me or (better yet, since everyone will benefit) ask in class. *There are not any dumb questions in this course.* You have to make sure there are no vague areas in your knowledge *before* exams. A discussion board will be used for this course in which questions can be asked in this course. I will answer questions on this board for topics in class lecture and in class projects. You will be surprised at how many of your questions may be addressed in this format.

There is a lot of material in the course and it's sufficiently different from all other MIS topics that most of you will find it very confusing at first. This course deals directly with networks, security, and uses hardware and software for information assurance. You will have to work hard to get an A in the class. On the other hand, many people do get an A in my class so hard work does pay off.

Course Objectives:

Recognize the importance of the manager's role in securing an organization's use of information technology, and understand who is responsible for protecting an organization's information assets
Know and understand the definition and key characteristics of information security
Know and understand the definition and key characteristics of leadership and management
Recognize the characteristics that differentiate information security management from general management
Recognize the importance of planning and describe the principal components of organizational planning
Know and understand the principal components of information security system implementation planning as it functions within the organizational planning scheme
Understand the need for contingency planning
Know the major components of contingency planning
Create a simple set of contingency plans, using business impact analysis

Prepare and execute a test of contingency plans
Understand the unified contingency plan approach
Define information security policy and understand its central role in a successful Information security program
Recognize the three major types of information security policy and know what goes into each type
Develop, implement, and maintain various types of information security policies
Recognize and understand the organizational approaches to information security
List and describe the functional components of the information security program
Determine how to plan and staff an organization's information security program based on its size
Evaluate the internal and external factors that influence the activities and organization of an information security program
List and describe the typical job titles and functions performed in the information security program
Describe the components of a security education, training, and awareness program, and understand how organizations create and manage these programs
Recognize the dominant information security management models, including U.S. government-sanctioned models, and customize them for your organization's needs
Implement the fundamental elements of key information security management practices
Follow emerging trends in the certification and accreditation of U.S. federal IT systems
Define risk management and its role in the organization
Begin using risk management techniques to identify and prioritize risk factors for information assets
Assess risk based on the likelihood of adverse events and the effects on information assets when events occur
Begin to document the results of risk identification
Recognize and select from the risk mitigation strategy options to control risk
Evaluate the risk control classification categories
Understand how to maintain and perpetuate risk controls
Understand the OCTAVE Method and other approaches to managing risk
Describe the various access control approaches, including authentication, authorization, and biometric access controls
Identify the various types of firewalls and the common approaches to firewall implementation
Recognize the current issues in dial-up access and protection
Identify and describe the types of intrusion detection systems and the two strategies on which they are based
Explain cryptography and the encryption process, and compare and contrast symmetric and asymmetric encryption
Identify the skills and requirements for information security positions
Recognize the various information security professional certifications, and identify which skills are encompassed by each
Understand and implement information security constraints on the general hiring processes
Understand the role of information security in employee terminations

Describe the security practices used to control employee behavior and prevent misuse of information

In Class Labs – We will conduct four in class labs using more extensive software. These labs will be conducted in pairs. Again, you will be asked to answer a series of questions concerning your findings in the lab. PLEASE NOTE THE DISCLAIMER AND WHITE HAT AGREEMENT BELOW.

In Class Lab 1 – Passwords and Password Cracking
In Class Lab 2 – Port Scanning (Tennable Nessus, Saint)
In Class Lab 3 – Packet Sniffing (Wireshark, Air Pcap Air Snort)
In Class Lab 4 – Vulnerability Testing (Tennable Nessus, Saint)

Paper – Each student will be required to write a 6-10 page paper concerning a relevant information assurance topic. This paper will provide either a description of an existing information assurance problem and a proposed solution or a new technology and its possible application in the information assurance field.

Presentation - Each student will be required to present their paper topic to the class in a 5-6 minute presentation using PowerPoint. No formal dress is required for the presentation.

Evaluation

The final course grade will be computed from the following inputs:

In Class Labs (Pairs)	**10%**	
Exam 1	**20%**	
Exam 2	**20%**	**3 Tests = 60%**
Final Exam	**20%**	
Paper	**10%**	
Presentation	**5%**	
Research Paper	**10%**	
Class Participation	**10%**	

TOTAL	**100%**	

The final course grade will be determined as follows:

90 or above	A
80-89.99	B
70-79.99	C
60-69.99	D
Less than 60%	F

White Hat Agreement – In this course, we will be using software that has the ability to intrude, disrupt and disable networks. The software is a tool to perform tasks that allow the gathering of information concerning vulnerabilities of computer systems and networks. By taking this course, you will gain expertise and experience with this software. In doing so, you must adhere to legal rules and regulations and only use the software and capabilities where permissions have been granted basically only within this course. Note great damage can be caused by using these tools outside the environment of the course. Any violations of these responsibilities in this course will result in an immediate withdrawal and F for a course grade. No EXCEPTIONS.

Tentative Course Schedule

Date	Scheduled
W1	Class Introduction Introduction to Management of Information Security Module 1 Whitman and Mattord Chapter 1 1.1 Comprehensive Model of Information Systems Security 1.1a NSTISS Model 1.2 Critical Characteristics of Information 1.2aCritical Information Characteristics - Confidentiality 1.2bCritical information characteristics - Integrity 1.2c Critical Information Characteristics - availability 1.3 Key Terms 1.3a Privacy 1.3b Identification 1.3c Authentication 1.3d Authorization 1.3e Accountability 1.4 Information States 1.4a Information States - Processing 1.4b Information States - Storage 1.4c Information States - Transmission 1.5 Threats 1.6 Vulnerabilities 1.7 Security Measures 1.7a Security Countermeasures - Education, Training and Awareness 1.7b Security Countermeasures - Policy, Procedures and Practices 1.7c Security Countermeasures - Technology
W2	Module 2 Planning for Security Whitman and Mattord Chapter 2 2.1 Planning For Information Security Implementation 2.2 CISO Job Description

	2.3Planning for InfoSec 2.4 The Systems Development Life Cycle (SDLC) 2.4a Requirements Definition (e.g., architecture) 2.4b Development 2.4c Demonstration and Validation (testing) 2.4d Implementation 2.4e Operations and Maintenance (e.g., configuration management) 2.4f Security (e.g., certification and accreditation) 2.5 Systems Life Cycle Management 2.5a Acquisition 2.5b Design Review and Systems Test Performance (ensure required safeguards are operationally adequate) 2.5c Determination of Security Specifications 2.5d Evaluation of Sensitivity of the Application Based upon Risk Analysis 2.5e Management Control Process (ensure that appropriate administrative, physical,and technical safeguards are incorporated into all new applications and into significant modifications to existing applications) 2.5f Systems Certification and Accreditation Process 2.6 Key Terms 2.6a Attack 2.6b Threat Agent 2.6c Exploit 2.6d Vulnerability 2.7 Common Attacks 2.8 SETA 2.9 Operational Controls 2.10 Technical Controls 2.11 Contingency Planning 2.12 Physical Security 2.13 Staffing the InfoSec Function 2.14 InfoSec Professionals 2.14a InfoSec Professionals Roles 2.15 Maintenance Model 2.16 Security Management Model In Class Lab 1 – Passwords
W3	Module 3 Planning for Contingencies Whitman and Mattord Chapter 3 3.1Contingency Planning 3.2 Contingency Planning Components 3.3 Business Impact Analysis (BIA) 3.4 Business Impact Analysis (BIA) Stages

3.4a Threat attack identification
3.4b Business unit analysis
3.4c Attack success scenarios
3.4d Potential damage assessment
3.4e Subordinate plan classification
3.5 Incident Response Plan
3.5a Before the Incident
3.5b During the Incident
3.5c After the Incident
3.6 Incident Detection
3.7a Incident Indicators: Possible Indicators
3.7b Incident Indicators: Probable Indicators
3.7c Incident Indicators: Definite Indicators
3.8 Incident Response
3.9a Notification of Key Personnel
3.9b Documenting an Incident
3.9c Incident Containment Strategies
3.9d Incident Escalation
3.9e Initiating Incident Recovery
3.9f After Action Review
3.10 Disaster Recovery
3.11 Disaster Classifications
3.12 Planning for Disaster
3.13 Crisis Management
3.14 Responding to the Disaster
3.15 Business Continuity Planning (BCP)
3.16 Continuity Strategies
3.17 Off-Site Disaster Data Storage

W4

Access Control Module 4
Whitman and Mattord Chapter 9
4.1Control Types
4.2 Administrative Controls
4.3 Technical Controls - Prevention
4.4 Technical Controls - Detective
4.5 Physical Controls - Preventive
4.6 Physical Controls - Detective
4.7 Access Control Services
4.7a Authentication
4.7b Authorization
4.7c Accountability
4.7d Identification
4.8 System Access Controls - Authentication
4.9 Two Factor Authentication
4.10 Password Controls – Best Practices
4.11 Physical Access Controls

4.12 Logical Access Controls
4.13 Biometrics Ratings Measures
4.14 Common Physiological Biometric Access Control Systems
4.14a Finger Scan Systems
4.14b Hand Geometry Systems
4.14c Retina Patterns
4.14d Iris Patterns
4.14e Voice Recognition
4.14f Signature Dynamic Systems
4.15 Access Control Tokens
4.16 Single Sign On
4.17 Kerberos
4.18 Centralized Access Controls
4.18a LDAP
4.18b RAS
4.18c RADIUS
4.18d DIAMETER
4.18e TACACS
4.19 Methods of Attack
In Class Lab 2 – Port Scanning

W5 Information Security Policy Module 5
Whitman and Mattord Chapter 4
5.1 Policies
5.1a Directives and procedures for NSTISS policy *(or organizational policies)*
5.1b NSTISS program budget
5.1c NSTISS program evaluation
5.1d NSTISS training (content and audience definition)
5.2 Bulls Eye Model
5.3 Standards
5.4 Procedures
5.5 Guidelines
5.6 Enterprise Information Security Policy (EISP)
5.6a AIS Equipment Purchase and Maintenance
5.6b Telecommunications Equipment Purchase and Maintenance
5.6c Points of Contact
5.6d Roles and Responsibilities
5.7 Issue-Specific Security Policy (ISSP)
5.7a Points of Contact
5.7b Roles and Responsibilities
5.8 Systems-Specific Policy (SysSP)
5.8a Application Dependent Guidance
5.8b Policy
5.8c Roles and Responsibilities
5.8d Points of Contact

	5.9 Access Control Lists 5.10 Guidelines for Policy Development Risk Management Module 6 Whitman and Mattord Chapter 8 6.1 Risk Control Strategies 6.1a Avoidance 6.1b Transference 6.1c Mitigation 6.1d Acceptance 6.2 Evaluation, Assessment, and Maintenance of Risk Controls 6.3 Risk Control Strategy Selection 6.4 Feasibility Studies and Cost Benefit Analysis 6.5 The OCTAVE Method 6.6 Operation Security (OPSEC) 6.7 INFOSEC and OPSEC interdependency 6.8 OPSEC process 6.9 OPSEC surveys/OPSEC planning 6.10 unclassified indicators 6.11 Microsoft Risk Management Approach Exam 1
W6	Developing the Security Program Module 7 Whitman and Mattord Chapter 5 7.1 Organizing for Security 7.2 Organizational Security Variables 7.2a Organizational Culture 7.2b Size 7.2c Security Personnel Budget 7.2d Security Capital Budget 7.3 Very Large Organizations More than 10,000 Computers 7.4 Large Organizations 1,000 to 10,000 computers 7.5 Medium-Sized Organizations 100 to 1,000 Computers 7.6 Small Organizations 10 to 100 Computers 7.7 Information Security Roles 7.8 Implementing Security Education, Training, and Awareness (SETA) Programs Application Security Module 8 8.1 Distributed Applications Security 8.2 Agents 8.3 Applets 8.4 Object Oriented Environments 8.5 Object Oriented Environments Terms 8.6 Database Security 8.7 System Development Lifecycle 8.8 Lifecycle Phases

	8.9 Change Management 8.10 Configuration Management 8.11 Application Security Controls 8.12 Supervisor and User Modes 8.13 Service Level Agreements 8.14 Assurance 8.15 Configuration Management 8.15a Configuration Management (change controls) 8.15b Configuration Management (documentation) 8.15c Configuration management (programming standards and controls) 8.16 Software Security Mechanisms 8.16a Software Security Mechanisms to Protect Information (access privileges) 8.16b Software Security Mechanisms to Protect Information (application security features) 8.16c Software Security Mechanisms to Protect Information (audit trails and logging) 8.16d Software Security Mechanisms to Protect Information (concept of least privilege) 8.16e Software Security Mechanisms to Protect Information (identification and authentication) 8.16f Software Security Mechanisms to Protect Information (internal labeling) 8.16g Software Security Mechanisms to Protect Information (malicious logic protection) 8.16h Software Security Mechanisms to Protect Information (need-to-know controls) 8.16i Software Security Mechanisms to Protect Information (operating systems security features) 8.16j Software Security Mechanisms to Protect Information (segregation of duties) In Class Lab 3 – Packet Sniffing
W7	Security Management Models and Practices Module 9 Whitman and Mattord Chapter 6 9.1 ISO/IEC 17799:2005 9.2 SANS SCORE and ISO/IEC 17799 9.3 The Eleven Sections Of ISO/IEC 17799 9.4 ISO/IEC 27001:2005 – The InfoSec Management System 9.5 BS7799:2 – Plan-Do-Check-Act 9.6 NIST Security Models 9.7 NIST SP 800-12 The Computer Security Handbook 9.8 NIST Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems

	9.9 NIST Special Publication 800-18 A Guide for Developing Security Plans for Information Technology Systems 9.10 NIST Special Publication 800-26 17 Areas Defining the core of the NIST Security Management Structure 9.11 NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems 9.12 RFC 2196 Site Security Handbook 9.13 Control Objectives for Information and related Technology (COBIT) 9.14 Committee of Sponsoring Organizations of the Treadway Commission (COSO) 9.15 Security Management Practices 9.16 Standards of Due Care/Due Diligence 9.17 The Gold Standard 9.18 Selecting Best Practices 9.19 Benchmarking and Best Practices Limitations 9.20 Baselining 9.21 Metrics in InfoSec Management 9.22 SP 800-37 Guidelines for Security C & A of Federal IT Systems 9.23 SP 800-53: Minimum Security Controls for Federal IT Systems 9.24 Communications Security 9.25 Employee Accountability for Agency Information 9.26 Protection of Information In Class Lab 4 – Vulnerability Testing
W8	Cryptography Module 10 Whitman and Mattord Chapter 9 10.1 Role of Cryptography in Information Security 10.2 Classes of Ciphers 10.3 Types of Ciphers 10.4 Modern Ciphers 10.5 Cryptosystem 10.5a Cryptovariable or Key 10.5b Electronic Key Management System 10.6 Cryptoalgorithm 10.7 Encryption and Decryption 10.7a End to End 10.7b Link 10.7c Network 10.8 Disposable Cipher 10.9 Cryptography Alternatives 10.9a Steganography 10.9b Digital Watermarking 10.10 Symmetric Key Cryptography

10.10a Process
10.10b Advantages
10.10c Disadvantages
10.11 Symmetric Methods
10.11a Data Encryption Standard (DES)
10.11b Triple DES
10.11c Advanced Encryption Standard
10.11d Rijndael Block Cipher
10.11e Twofish algorithm
10.11f IDEA Cipher
10.11g RC5
10.12 Assymmetric key cryptography
10.12a Process
10.12b Advantages
10.12c Disadvantages
10.13 Assymmetric key cryptography – Methods
10.13a RSA
10.13b Diffie Hellman Key Exchange
10.13c El Gamal
10.13d Merkel Hellman Trapdoor Knapsack
10.13e Elliptic Curve
10.14 Message Authentication Methods
10.14a Digital Signatures
10.14b Message Digest
10.14c MD5
10.14d SHA-1
10.14e HMAC
10.15 Public Key Infrastructure (PKI)
10.15a Process
10.15b Key Management Functions
10.16 Key Strength
10.16 Email Security Applications
10.17 Internet Security applications

In Class Lab 5 - Forensics

W9

Protection Mechanisms Module 11
Whitman and Mattord Chapter 9
11.1 Organizational Equipment
11.1a Access Control
11.1b Telecommunications Hardware
11.1c Telecommunications Software
11.1d AIS Firmware
11.1e AIS Hardware
11.1f AIS Software

11.2 Firewalls
11.3 Firewall Architectures
11.4 Packet Filtering
11.5 DMZ
11.5a Trust
11.5b Assurance
11.5c Mechanism
11.5d Policy
11.6 Managing Firewalls
11.7 Firewall Best Practices
11.8 Intrusion Detection Systems (IDS)
11.8a Host Based
11.8b Network Based
11.8c Signature Based
11.8d Statistical Anomaly-Based IDS
11.9 Managing Intrusion Detection Systems
11.10 Dial-Up Protection
11.11 RADIUS and TACACS
11.12 Managing Dial-Up Connections
11.13 Scanning and Analysis Tools
11.14 Wireless Networking Protection
11.15 WEP
11.16 WPA
11.17 Port Scanners
11.18 Vulnerability Scanners
11.19 Packet Sniffers
11.20 Managing Scanning and Analysis Tools
11.21 Emanation Security
11.22 Transmission Security
11.22a Transmission Security Countermeasures
11.23 Modes of Operation
11.23a Compartmented/Partitioned
11.23b Dedicated
11.23c Multilevel
11.23d System-high
11.24 TEMPEST Security
11.24a Attenuation
11.24b Banding
11.24c Cabling
11.24d Filtered power
11.24e Grounding
11.24f Shielding
11.24g TEMPEST Separation
11.24h Zone of control/zoning

	In Class Lab 6 - Forensics
W10	Personnel and Security Module 12 Whitman and Mattord Chapter 10 12.1 Staffing the Security Function 12.2 Qualifications and Requirements 12.3 Entering the Information Security Profession 12.4 Information Security Career Paths 12.5a CISO: Qualifications and Position Requirements 12.5b Security Manager Qualifications and Position Requirements 12.5c Technician Qualifications and Position Requirements 12.6 Employment Policies and Practices 12.6a Security Clearances 12.7 Hiring 12.8 Common Background Checks 12.9 Contracts and Employment 12.10 Security as Part of Performance Evaluation 12.10a Security Training 12.11 Termination Issues 12.11a Hostile Departure 12.11b Friendly Departure 12.12 Personnel Security Practices 12.12a Reporting of Security Violations 12.13 Security of Personnel and Personal Data 12.14 Security Considerations for Non-employees 12.14a Temporary Workers 12.14b Contract Employees 12.14c Consultants
W12	Operations Security Module 13 13.1 Privilege Entry Controls 13.2 Files Sensitive Labels 13.3 Clearances 13.4 Password Handling and Policy 13.4a Password Protection 13.5 Account Characteristics 13.6 Resource Protection 13.6a Area Protection 13.6b Facilities 13.6c Hardware 13.6d Software 13.6e Documentation 13.7 Threats to Operations 13.7a Disclosure 13.7b Destruction 13.7c Interruption

13.7d Corruption and Modification
13.7e Theft
13.7f Espionage
13.7g Hackers
13.8 Control Types
13.8a Prevention
13.8b Detection
13.8c Corrective
13.8d Recovery
13.8e Deterrent
13.9 Control Methods
13.9a Separation of Responsibilities
13.9b Least Privilege
13.9c Job Rotation
13.9d Audits and Review
13.10 Media Protection
13.10a Magnetic Storage Protection
13.11 Object Reuse
13.12 Sensitive Media Handling
13.12a Marking
13.12b Handling
13.12c Storing
13.12d Destruction
13.12e Declassification
13.12f Sanitization
13.12g Transportation
13.13 Continuity of Operations
13.13a Data and File Protection
13.13b Back Up of Data and Files
13.13c Software
13.13d Hardware
13.13e Data Communication Protection
13.13f Facilities
13.13g Equipment Protection
13.13h Protection of Keying Material
13.13i Voice Communication Protection
Physical Security Module 14
14.1 Site Location
14.2 Layered Defense Model
14.3 Infrastructure Support Systems
14.4 Fire Safety Controls
14.4a Prevention
14.4b Detection
14.4c Suppression
14.5 Boundary Protection
14.5 Building Entry Points

14.6 Area Protection
14.6a Keys and Locking Systems
14.6b Walls, Doors, and Windows
14.6c Access Controls
14.6d Closed Circuit TV
14.6e Intrusion Detection Systems
14.6f Portable Device Security
Final Exam