CIS 524/424
Information Assurance Risk Assessment

Text Security Assessment by Miles, Rogers, Fuller, Hoagberg, and Dykstra, ISBN 1932266968
Network Security Evaluation by Cunningham, Dykstra, Fuller, Hoagberg, Little, Miles, and Schack
ISBN 1597490350
Lecture notes posted on Blackboard

Course Objective and Overview:

This course is designed to give students an understanding of information assurance risk assessment 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 risk assessment.* Note we will cover the Common Body of Knowledge of the NSA IAM and NSA IEM Methodologies. 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:

Course Learning Objective: Identify the baseline information categories required for INFOSEC analysis
Describe the Post-assessment activities.
Identify the format and content of the final assessment report
Explain INFOSEC Assessment Training and Rating Program
Reiterate the Security Lifecycle
Learn the INFOSEC Evaluation Methodology (IEM) as a standardized baseline for technical evaluations
Establish a foundation for technical evaluations that can be integrated into your own evaluation procedures
Identify the inherent connections between the IAM and IEM processes
Gain an in-depth understanding of the Pre-Evaluation Phase:

How to coordinate the technical evaluation efforts with customers.
The scope can be defined concurrently or after the IAM Pre-Assessment Site Visit.
Letter of Authorization
How to develop a Technical Evaluation Plan (TEP)
Gain an understanding of how to go about the collection of basic technical information
Gain an in-depth understanding of the IEM On-Site Evaluation Phase
Understand the various pieces of the On-site Evaluation Phase
Learn how to conduct the technical evaluation based on customer security requirements
Understand how to conduct an evaluation of the Security Architecture
Describe the Evaluation Analysis Activities
Introduce Layered Security Concepts
Create the Vulnerability Criticality Matrices and INFOSEC Posture Profile based on evaluation findings, evaluator expertise, and customer input
Identify the format and content of the final evaluation report

Responsibility

The student shall be responsible for all material covered in the class lectures. Each exam will include not only the material from the assigned text chapters, but also from the readings, tours, guest lectures and any other materials covered in the class lectures.

You are also responsible for any announcements made in class. Often times I have to change the Class Schedule or I may announcements relevant for assignments. Schedule changes will be posted on my website. We will have several external speakers during the semester.

I do expect class participation from every individual in the course. Students often learn many things from student colleagues and questions in class. This participation is vital to classroom discussion. It will be a part of the evaluation of this course.

In C lass L abs – We will conduct several in class labs using more extensive software. These labs will be conducted in groups of three. Again, you will be asked to answer a series of questions concerning your findings in the lab. Participation in these labs will contribute to the Participation Portion of the Grade.

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

Paper – Students in CIS 524 will have to write a paper (5-10) concerning some aspect of information security risk. This could be a case or a topic. This will be due on the last day of class, however, the topic must be approved by the end of June.

Group Assessment Project – Students in CIS 524/424 will conduct a security assessment of a live company in the area. The key will to evaluate their current security measures and will not be hands on.

Group Evaluation Project – Students will carry forward their assessment project and we will use Tennable Nessus or Saint to simulate a hands-on security evaluation with an existing network structure. Students will use this information to complete their security evaluation and make recommendations.

Evaluation

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

Exam 1	**25.00%**	
Final Exam	**25.00%**	**2 Tests = 50%**
Class Participation	**10.00%**	
Assessment Project	**10.00%**	
Evaluation Project	**10.00%**	
Presentation	**10.00%**	
Paper	**10.00%**	

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

Tentative Course Schedule

Date	Scheduled
W1	Concepts of Risk Management Module 1 1.1 Consequences (e.g., corrective action, risk assessment) 1.2 Cost/Benefit Analysis of Controls 1.3 Implementation of Cost-Effective Controls 1.4 Monitoring the Efficiency and Effectiveness of Controls (e.g., Unauthorized or Inadvertent Disclosure of information) 1.5 Threat and Vulnerability Assessment 1.6 What is Assessment? 1.7 Information Security Assessment Methodology (IAM) 1.8 Vulnerability Discovery Triad 1.9 Infosec Assessment Characteristics 1.10 Assessment Purposes 1.10a Pre-Assessment 1.10b On Site Activities

	1.10c Post Assessment
W2	Information Criticality Module 2 2.1 Critical Characteristics of Information 2.2 Information States 2.3 Security Measures 2.4 Critical Information Characteristics – Availability 2.5 Critical Information Characteristics – Confidentiality 2.6 Critical Information Characteristics – Integrity 2.7 Information States – Processing 2.8 Information States - Storage 2.9 Information States – Transmission 2.10 Security Countermeasures - Education, Training and Awareness 2.11 Security Countermeasures - Policy, Procedures, and Practices 2.12 Security Countermeasures - Technology 2.13 Threats 2.14 Vulnerabilities
W3	The Assessment Module 3 3.1 Pre Assessment Activity Phase 3.2 Pre-Assessment Goals 3.3 Pre-Assessment Site Visit 3.4 Organizational information Criticality 3.5 Organizational information Criticality Matrix 3.6 Define Impact Values 3.7 System Identification 3.8 System Criticality 3.9 System Criticality Matrix 3.10 Organizational Information Mapping to Systems 3.11 System Security Environment 3.12 Logical and Physical Security Boundaries 3.13 Countermeasures 3.13a Assessments (e.g., Surveys, Inspections) 3.13b Cover and Deception 3.13c Education, Training and Awareness 3.13d HUMINT 3.13e Monitoring (e.g., Data, Line) 3.13f Technical Surveillance Countermeasures 3.14 Countermeasure Constraints 3.15 The Assessment Plan
W4	Assessment On Site Module 4 4.1 On Site Activities 4.2 On Site Information Gathering 4.2a Interviews

	4.2b System Demonstrations 4.2c Documentation Review 4.3 INFOSEC Documentation 4.3a Policy 4.3b Requirements 4.3c System Security Plan 4.3d Standard Operating Procedures 4.3e User Documentation 4.4 Roles of Various Organizational Personnel 4.4a Audit Office 4.4b COMSEC Custodian 4.4c End Users 4.4d Information Resources Management Staff 4.4e INFOSEC Officer 4.4f OPSEC Managers 4.4g Program or Functional Managers 4.4h Security Office 4.4i Senior Management 4.4j System Manager and System Staff 4.4k Telecommunications Office and Staff 4.5 Contingency Planning 4.5a Documented Plan 4.5b System Backup 4.5c Single Points of Failure 4.5d Mirror Sites 4.6 Configuration Management
W5	Assessment Module 5 5.1 Computer Security - Access Control 5.2 Computer Security – Audit 5.3 Session Controls 5.4 Malicious Code Protection 5.5 Maintenance 5.6 Security (e.g., Certification and Accreditation) 5.7 Networking/Connectivity 5.8 Data Communications Security 5.8a Cryptography - Encryption (e.g., Point-to-Point, network, link) 5.9 Media Controls 5.9a Sanitization of Media 5.9b Transportation of Media 5.9c Destruction of Media 5.9d Emergency Destruction 5.10 Labeling 5.10a External Marking of Media

	5.10b Media Downgrade and Declassification 5.11 Physical Environment 5.11a Alarms 5.11b Building Construction 5.11c Cabling 5.11d Communication Center 5.11e Environmental Controls (Humidity and Air Conditioning) 5.11f Filtered Power 5.11g Information System Centers 5.11h Physical Access Control Systems (Key Cards, Locks and Alarms) 5.11i Power Controls (Regulator, Uninterrupted Power Service (UPS), and Emergency Poweroff Switch) 5.11j Protected Distributed Systems 5.11k Shielding 5.11l Stand-Alone Systems and Peripherals 5.11m Storage Area Controls Assessment Module 6 6.1 Personnel Security Practices and Procedures 6.1a Access Authorization/Verification (Need to Know) 6.1b Contractors 6.1c Employee Clearances 6.1d Position Sensitivity 6.1e Security Training and Awareness 6.2 Education Training and Awareness 6.3 Threats and Vulnerabilities of Systems 6.4 Out Briefing Assessment Report Due Midterm Exam
W7	Evaluation Module 1 7.1 National Policy and Guidance 7.1a AIS Security 7.1b Communications Security 7.1c Employee Accountability for Agency Information 7.1d Protection of Information 7.2 Concepts of Trust 7.2a Assurance 7.2b Mechanism 7.2c Policy 7.3 Risk Management 7.3a Acceptance of Risk (Accreditation) 7.3b Corrective Actions 7.3c Information Identification

	7.3d Risk Analysis and/or Vulnerability Assessment Components 7.3e Risk Analysis Results Evaluation 7.3f Roles and Responsibilities of All the Players in the Risk Analysis Process 7.4 Infosec Evaluation Methodology (IEM) Phases
W8	Pre Evaluation Phase Module 8 8.1 Phase Goals 8.2 Vetting Process 8.3 Management Buy-In 8.4 Technical Staff Buy-In 8.5 Scoping the Evaluation 8.6 Rules of Engagement 8.6a Levels of Invasiveness 8.6b Time Frame 8.6c Notification Procedures 8.6d Evaluation Addressing 8.6e Level of Detail of Recommendations 8.7 Information Validation 8.8 Legal Approval 8.9 Letter of Authorization 8.10 Technical Evaluation Plan
W9	On Site Evaluation Phase Module 9 9.1 Vulnerability Definition 9.2 On Site Evaluation Goals 9.3 Evaluation In-Brief 9.4 Evaluation Tools 9.4a Port Scanners 9.4b SNMP Scanners 9.4c Wireless Enumeration Tools 9.4d Enumeration & Banner Grabbing 9.4e Vulnerability Scanners 9.4f Network Device Analysis 9.4g Host Evaluation 9.4h Password Compliance Testing 9.4i Application Specific Scanning 9.4j Network Sniffing 9.4k Penetration Testing 9.4l Denial of Service 9.4m War Dialing 9.5 Network Discovery 9.6 Outbrief Vulnerability Testing Lab

W10	Post Evaluation Activities Module 10 10.1 Post Evaluation Activities 10.2 Layered Security 10.3 System Vulnerability Criticality Matrix (SVCM) 10.4 Organizational Vulnerability Criticality Matrix (OVCM) 10.5 INFOSEC Posture Profile 10.6 Four Aspects of DOD Computer Network Defense (CND) 10.6a Protect 10.6b Detect 10.6c Respond 10.6d Sustain
	Module 11 Red Teaming Final Exam Evaluation Report Due Presentations Paper Due