Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
4016 Points						
*** = Can include a summary justification for that section.**						
FUNCTION 1 - INFORMATION SYSTEM LIFE CYCLE ACTIVITIES						
Life Cycle Duties						
No Subsection						
2. System Disposition/Reutilization						
*E - Discuss processes for disposition of media and data		X		X	X	
E - Identify agency-specific system reutilization policies and procedures		X			X	
3. System Configuration and Management Board (SCMB)						
*E - Identify life cycle management SCMB policies and procedures		X				
4. Operations & Maintenance (O & M)						
*E - Discuss risk analysis processes used in development of life cycle functions		X				
E - Monitor life cycle operation and maintenance project milestones relating to risk		X				
E - Monitor maintenance procedures concerning life cycle operations and analysis issues		X				
E - Monitor performance measurement data in operations and maintenance examination of events and/or changes in an event		X				
5. System Acquisition						
*E - Discuss risk analyst concerns relating to life cycle system security planning		X			X	
E - Monitor process of selecting and purchasing IT designed to implement management risk process					X	
E - Verify that system acquisitions policies and procedures include assessment of risk management policies		X			X	

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
6. System Administration						
*E - Discuss audit mechanism processes used to collect, review, and/or examine system activities					X	
7. System Owners						
*E - Discuss maintenance plans for protective measures to ensure tolerable level of risk		X				
8. System Developers						
*E - Discuss process for selecting and purchasing new information technology (IT)		X			X	
E - Discuss process to ensure that applications function according to specifications		X			X	
E - Explain risk methodologies used to evaluate measures taken to protect system		X			X	
9. Computer Science and Architecture						
*E - Discuss system IA design guidance		X				
10. Security Product Integration						
E - Examine and analyze applied security					X	
11. Information Systems Security Officer (ISSO) Activities						
*E - Discuss maintenance of user accounts		X			X	
E - Discuss processes for timely deletion of accounts		X			X	
E - Discuss processes for updating access		X			X	
E - Discuss processes for verification of authorization prior to adding new account		X			X	
12. Audit Mechanism						
*E - Review policy, guidance and process for the capture, maintenance, and distribution of audit logs					X	
13. Policy Development						
E - Develop risk management methodology which includes evaluation of threats, vulnerabilities, and countermeasures		X			X	

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
14. System Certifiers and Accreditors						
*E - Explain how certification process ensures security requirement implementation		X			X	
E - Explain local policies and procedures to supplement and implement higher-level guidance		X				
15. Automated Tool for Security Test						
E - Discuss utilities used to determine vulnerabilities or configurations not		X			X	
FUNCTION 2 - COUNTERMEASURES IDENTIFICATION,						
Countermeasures						
No Subsection						
1. General						
*E - Identify all component and overall risks inherent in system					X	
E - Assist certifier to determine countermeasures based on threat capabilities and motivations					X	
2. Analyzing Potential Countermeasures						
*E - Discuss security test and evaluation (ST&E) procedures, tools, and equipment					X	
E - Assist certifier to evaluate security requirements as potential countermeasures					X	
E - Discuss respective value of penetration testing post-testing actions, general information principles, and summary comparison of network testing techniques					X	
E - Discuss testing roles and responsibilities					X	
E - Explain process to determine underlying state of system					X	
E - Relate organization IT security needs to countermeasure requirements					X	
3. Determining Countermeasures						
E - Apprise decision makers of existing countermeasure models, tools, and techniques					X	

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
4. Identifying Potential Countermeasures						
*E - Discuss effectiveness of automated security tools that confirm validity of a transmission					X	
E - Assist certifier/IA engineer to evaluate system security safeguards established to determine system security posture					X	
E - Discuss effectiveness of automated security tools that verify an individual?s eligibility to receive specific categories of information					X	
E - Discuss methodologies used to evaluate system security safeguards					X	
5. Determining Cost/Benefit of Countermeasures						
*E - Outline cost/benefit of organization?s IA countermeasure plans					X	
E - Outline cost/benefit of personnel supporting access control policies		X			X	
FUNCTION 3 - CERTIFICATION AND ACCREDITATION						
Certification and Accreditation						
No Subsection						
1. Certification and Accreditation Guidelines and Documentation						
*E - Explain applicable organizational certification and accreditation processes		X				
E - Discuss role of RA in certification and accreditation process		X				
2. Vulnerabilities and Attacks						
*E - Discuss paired interaction of a vulnerability to an attack		X			X	
4. Security Laws						
E - Outline security laws applicable to certification/accreditation process		X				
5. Physical Security Requirements						
E - Discuss risk mitigation decisions derived from analysis and review of		X				
6. Security Inspections						

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
*E - Evaluate security inspections conducted during C&A process		X				
E - Discuss security inspections conducted during C&A process		X				
7. Security Policies and Procedures						
E - Explain security policies and procedures implemented during risk analysis/assessment process		X			X	
8. Security Processing Mode						
E - Discuss vulnerabilities associated with security processing modes					X	
9. System Certification						
*E - Discuss threat and vulnerability analyses input to C&A process		X				
10. Support C&A						
*E - Identify system security policies		X			X	
E - Explain alternative actions permitted on system					X	
11. System Security Profile						
*E - Describe protections offered by security features in specific configurations					X	
E - Assist in helping to identify protections offered by security features in specific configurations					X	
E - Discuss security features of system					X	
12. Threat/Risk Assessment						
*E - Identify threat/risk assessment methodology appropriate for use with system undergoing accreditation		X			X	
13. Information Technology Security Evaluation Criteria						
E - Assist in the use of common criteria guidance to determine hardware and software assurance applications for simultaneous processing of a range of information classes					X	
14. Mission						
E - Discuss impact of security on mission					X	
15. Interviewing/Interrogation						
E - Assist certifier in preparing questions for determining countermeasures during C&A process					X	

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
16. Applications Security						
E - Discuss criticality of applications security		X			X	
FUNCTION 4 - SYNTHESIS OF ANALYSIS						
Synthesis of Analysis Duties						
A. General						
1. Synthesis of Components and Overall Risks						
E - Report synthesis of all component and risks inherent in a system		X			X	
3. Aspects of Security						
E - Discuss security with regard to confidentiality, integrity, authentication, availability, and non-repudiation		X			X	
4. Assessment Methodology						
E - Appraise information acquisition and review process for best use of resources to protect system					X	
5. Associate Threat Probabilities to Vulnerability						
E - Describe process of analyzing paired interactions of system threats and vulnerabilities		X			X	
6. Conducting Risk Analysis						
E - Conduct risk analysis examination and evaluation process to determine relationships among threats, vulnerabilities, and countermeasures		X			X	
7. Countermeasure Analysis						
*E - Conduct detailed examination and evaluation of impact of attacks					X	
E - Conduct detailed examination and evaluation of possible actions to mitigate vulnerabilities					X	
8. Critical Thinking						
E - Discriminate between known and hypothetical variables based on executed test procedures					X	
9. Deductive Reasoning						
*E - Analyze tests results					X	

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
10. Detailed Residual Risk						
*E - Discuss susceptibility of a system to attack after countermeasures have					X	
E - Assist certifier/IA engineer in evaluating susceptibility of a system to attack after countermeasures have been applied					X	
13. All Risk Variables						
E - Evaluate an analysis of threats, vulnerabilities, attacks, and consequences in relationship to risk assessment of a system					X	
14. Risk Assessment (Environment & Threat Description)						
E - Discuss environment in relation to current threat					X	
15. Risk Management Methodology						
E - Discuss organizational capability and ability to evaluate threats, and vulnerabilities					X	
16. Security Countermeasures						
E - Assist certifier/IA engineer in defining countermeasures directed at specific threats and vulnerabilities					X	
17. Technical Vulnerability						
E - Discuss hardware, firmware, communications, or software weaknesses that open an information system to exploitation					X	
18. Threat Analysis						
E - Examine methods through which threat agent adversely affects information system, facility, or operation					X	
19. Threat Description						
E - Define means through which a threat agent can adversely affect information system, facility, or operation					X	
20. Threat/Risk Assessment						
E - Discuss process of formally evaluating degree of threat and describing nature of threat					X	
21. Mission						
*E - Discuss information system support mission					X	

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
22. Vulnerabilities						
*E - Assist in identifying weakness in an information system, system security procedures, internal controls, or implementation that could be exploited					X	
E - Discuss weakness in an information system, system security procedures, internal controls, or implementation that could be exploited					X	
E - Explain hardware or software flow that opens an information system to potential exploitation					X	
23. Vulnerability Analysis						
*E - Analyze an information system to determine adequacy of security measures					X	
B. Documentation						
1. Policies						
*E - Explain applicable national level policies		X		X		
E - Discuss agency/local guidance		X				
9. Technical Knowledge of Information System						
E - Outline technical knowledge required of personnel responsible for networks, servers, workstations, operating systems, etc.		X			X	
C. Effect of Countermeasure						
9. Security Product Testing/Evaluation						
E - Examine analysis of security safeguards of a system as they have been applied to an operational environment to determine security posture					X	
10. Technical Knowledge of Information System						
E - Outline technical knowledge required of personnel responsible for operating and maintaining networks, servers, workstations, operating systems, etc.		X			X	
FUNCTION 5 - TESTING AND EVALUATION						

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
Testing and Evaluation Duties						
No Subsection						
3. Account Administration						
E - Discuss maintenance of accounting files, tools, user accounts, and system statistics		X			X	
4. Assessment Methodology						
E - Define vulnerability analysis process					X	
5. Associate Threat Probabilities to Vulnerability						
E - Explain paired interaction of system threats and vulnerabilities		X			X	
6. Audit Trails and Logging						
E - Team with certifier/IA engineer to compile chronological record of system activities for reconstruction and examination of events and/or changes in an event			X		X	
7. Backups						
E - Discuss purpose of using copies of backup files for later reconstruction of files		X		X		
8. Software Test & Evaluation Results						
E - Ensure software test and evaluation results related to system restoration are performed				X	X	
12. Security Test & Evaluation Plan & Procedure						
E - Assist with the development of ST&E plan and procedure for testing and evaluating a system					X	
13. Error Logs						
E - Interpret files created by operating system for review of audit process			X		X	
14. Non-Technical & Technical Result						
E - Interpret technical and non-technical results from testing and evaluation					X	
15. Evaluation Techniques						

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
E - Team with certifier/IA engineer to integrate technical analysis of components, products, subsystems, or systems security that establishes whether or not component, product subsystem, or system meets a specific set of requirements independently and in					X	
16. Identify All Risk Variables						
E - Explain development of a compendium of relative threats, vulnerabilities, attacks, and consequences related to a system (Common vulnerabilities and exploitations)					X	
18. Certification Tools						
E - Team with certifier/IA engineer to interpret results of certification tools during testing and evaluation					X	
19. Privileges (Class, Nodes)						
E - Influence program or user operations that can be performed during testing and Evaluation					X	
20. Test and Evaluation Strategies						
*E- Identify strengths of alternative test and evaluation strategies					X	
21. Testing Implementation of Security Features						
E - Integrate testing of security features during testing and evaluation					X	
FUNCTION 6 - THREAT AND ADVERSARY ANALYSIS						
Threat and Adversary Analysis Duties						
A. General						
1. Conducting Risk Analysis						
E - Conduct examination of vulnerabilities, attack, threats and consequences that may affect system					X	
2. Cost/Benefit Analysis						
E - Conduct an assessment of costs of data protection for a system versus cost of loss or compromise		X			X	
3. Critical Thinking						

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
E - Discuss known and hypothetical variables based on test procedures					X	
4. Deductive Reasoning						
E - Recommend solutions based on a set of static and variable factors of system					X	
5. Effects of Mitigation						
E - Determine effects of mitigation derived from application of countermeasures to a system					X	
6. Hostile Intelligence Sources						
E - Discuss impact of hostile agents seeking national security information which could potentially cause harm to national security		X				
7. All Risk Variables						
E - Build a compendium of relative threats, vulnerabilities, attacks, and consequences related to system					X	
B. Risk Assessment (Environment & Threat Description)						
1. Risk Management Methodology						
E - Discuss evaluation of threats, vulnerabilities, and countermeasures to determine residual risk					X	
2. Security Countermeasures						
E - Discuss security and software countermeasures during design, implementation, and testing phases to achieve required level of confidence		X			X	
3. Threat Analysis						
E - Conduct examination and evaluation of sources and factors that can adversely impact system					X	
4. Treat Description						
E - Identify level of threat based on its applicability to system					X	
5. Threat/Risk Assessment						

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
E - Recommend life cycle countermeasures based on assessments of threats, capabilities, and motivations to exploit vulnerability					X	
6. Mission						
*E - Discuss current mission and role of information system in supporting mission					X	
E - Determine if an adverse system finding should be allowed to halt mission support operations					X	
7. Vulnerability Analysis						
E - Appraise weaknesses in information system, security procedures, internal controls, or implementations that could be exploited					X	
C. Analysis for Decisions						
1. Agency-Specific Policies and Procedures						
E - Discuss local policies and procedures implementing regulations, laws, and procedures in local environment		X				
H. Technical Surveillance Countermeasures						
1. Technical Surveillance Countermeasures						
E - Discuss Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies		X	X			
FUNCTION 7 - MISSION AND ASSETS ASSESSMENTS						
Mission and Assets Duties						
A. General						
1. Conducting Risk Analysis						
*E - Conduct detailed evaluation of vulnerabilities, attack, threats, and consequences that may affect system					X	
E - Conduct detailed examination of vulnerabilities, attack, threats, and consequences that may affect system					X	
2. Cost/Benefit Analysis						
E - Conduct cost assessment for providing data protection versus cost of data loss or compromise					X	

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
3. Critical Thinking						
E - Understand known and hypothetical variables based on test procedures					X	
4. Deductive Reasoning						
E - Recommend solutions based on a set of static and variable factors					X	
5. Effects of Mitigation						
E - Determine effects of mitigation derived from application of countermeasures					X	
6. Hostile Intelligence Sources						
E - Discuss impact of hostile agents seeking national security information which could potentially cause harm to national security		X				
7. All Risk Variables						
E - Build a compendium of relative threats, vulnerabilities, attacks, and consequences related to system					X	
B. Risk Assessment (Environment & Threat Description)						
1. Risk Management Methodology						
E - Discuss evaluation of threats, vulnerabilities, and countermeasures to determine residual risk		X			X	
2. Security Countermeasures						
E - Discuss security and software countermeasures during design, implementation and testing phases to achieve required level of confidence		X			X	
3. Threat Analysis						
*E - Conduct detailed examination and evaluation of sources and factors that can adversely impact system					X	
4. Treat Description						
E - Identify level of threat based on its applicability to system					X	
5. Threat/Risk Assessment						

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
E - Recommend life cycle countermeasures based on assessment of threats, capabilities, and motivations to exploit vulnerability					X	
6. Mission						
E - Assess mission to determine if an adverse finding should be allowed to affect continued IT operations in a given mission environment					X	
7. Vulnerability Analysis						
E - Appraise exploitable weaknesses in information system, security procedures, internal controls or implementations					X	
D. Agency-Specific Policies and Procedures						
1. Agency-Specific Policies and Procedures						
E - Discuss local policies and procedures implementing regulations, laws, and procedures in local environment		X				
H. Technical Surveillance Countermeasures						
1. Technical Surveillance Countermeasures						
E - Discuss techniques and measures to detect and neutralize hostile penetration technologies		X	X			
FUNCTION 8 - VULNERABILITIES AND ATTACK AVENUES ANALYSIS						
Vulnerability and Attack Avenues Duties						
A. General						
1. Vulnerabilities, attacks, threats, and consequences						
E - Assess vulnerabilities, attacks, threats, and consequences to determine vulnerabilities and attack avenues					X	
2. Cost/Benefit Analysis						
E - Discuss cost analysis of data protection versus cost of data lose or compromise					X	
3. Critical Thinking						
E - Apply discrimination to known and potential vulnerabilities based on test procedures					X	

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
4. Deductive Reasoning						
E - Use test results to determine underlying state of system					X	
5. Effect of Countermeasures on Risk						
E - Determine effect of countermeasures on risk through the analysis of paired interaction of a defense					X	
6. Effects of Mitigation						
E - Determine effects of mitigation derived from application of countermeasures to system					X	
7. Hostile Intelligence Sources						
E - Discuss hostile intelligence sources as part of vulnerabilities and attack venues		X				
8. Risk Variables						
E - Identify risk variables to build a compendium of relative threats, vulnerabilities, attacks, and consequences related to a system					X	
9. Jamming						
E - Discuss jamming as a potential threat	X					
10. Risk Assessment						
E - Define risk assessment methodology in relation to risk analyst function		X				
11. Risk Management Methodology						
E - Define risk management methodology in relation to system security		X				
12. Security Countermeasures						
E - Discuss security countermeasures in relation to vulnerabilities and attack venues					X	
13. Threat Analysis						
E - Use threat analysis to determine vulnerabilities and attack venues					X	
14. Threat/Risk Assessment						

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
E - Apply threat and/or risk assessment in determining vulnerabilities and attack venues					X	
15. Mission						
E - Support organizational mission in conjunction with vulnerabilities and attack venues					X	
16. Vulnerabilities						
E - Discuss weaknesses in system, system security procedures, and internal controls and implementation					X	
17. Vulnerability Analysis						
E - Use vulnerability analysis to determine adequacy of security measures, identify security deficiencies, and provide data to predict effectiveness of security measures					X	
B. Developing Attack Avenues						
1. Avenues of Attack						
E - Describe known avenues of attack such as operating system bugs, network vulnerabilities, human threats, etc.					X	
C. Characterizing Vulnerabilities						
1. Characterizing Vulnerabilities						
*E - Discuss aspects of security in a vulnerability testing and evaluation plan					X	
E -Evaluate threats and vulnerabilities					X	
D. Researching Vulnerability Report						
1. Researching Vulnerability Report						
E -Evaluate vulnerability assessment methodologies					X	
E. Collecting and Reviewing Vulnerabilities						
1. Collecting and Reviewing Vulnerabilities						
*E - List potential vulnerabilities that may lead to defeat of security services					X	
F. Comparing and Contrasting Attack Avenues						

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
1. Comparing and Contrasting Attack Avenues						
*E - Discuss techniques and measures to detect or neutralize a wide variety of hostile penetration technologies		X	X			
E - Evaluate payoff to and liabilities incurred by an attacker in a successful attack		X			X	
G. Risk of Detection and Response						
1. Risk of Detection and Response						
E - Characterize impact of security breaches and estimate an attacker?s probable Response					X	
I. Technology Necessary to Mount Attack						
1. Technology Necessary to Mount Attack						
E - Describe technology needed to mount an attack based on existing countermeasures		X				
FUNCTION 9 - TRAINING AND AWARENESS						
Training and Awareness Duties						
A. Policies / Procedures / Methodology						
1. Access Control Policies						
*E - Summarize national and local level access control policies		X				
2. Laws, Regulations, and Other Public Policy						
*E - Identify local application of IA laws, regulations, and policies		X	X			
E - Discuss applicable IA laws, regulations, and policies		X	X			
3. Agency-Specific IA and IT Policies and Procedures						
*E - Summarize agency-specific policies and procedures in relation to risk environment					X	
5. Audit Trails and Logging Policies						
*E - Discuss audit trails and logging policies		X			X	
6. Change Control Policies						
*E - Discuss change control policies for incorporation in IA training		X				
7. Communications Security Policy and Guidance						

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
*E - Discuss communications security policy and guidance for incorporation into IT training		X				
E - Identify communications security policy and guidance for incorporation into IT training		X				
8. Emergency Destruction Planning and Procedures (EDPP)						
*E - Discuss EDPP for incorporation in IA training				X		
9. Personnel Security Policies and Guidance						
E - Discuss role of personnel security policies and guidance as part of overall risk management plan		X				
10. Formal Methods for Security Design						
E - Outline role of formal methods in security design as part of risk management plan		X				
11. Information Categorization						
E - Discuss various categorization schemas		X				
12. Information Classification						
*E - Discuss classification policies as part of risk management plan		X				
14. Methods of Defining Security Requirements						
*E - Discuss definitions of security requirements		X				
15. Physical Security Requirements						
*E - Discuss physical security requirements		X				
17. Risk Management Methodology						
E - Summarize approaches to risk management		X				
B. Technology						
1. Applications Security						
E - Discuss state of security features embedded in commercial-off-the-shelf (COTS) products in relation to risk management plan		X				
2. Database Security Features						
*E - Discuss elements of database security features		X				
E - Identify critical database security pitfalls		X				

Courses	CIS 444: Computer Networking	CIS 521/421: Introduction to Information Assurance	CIS 522/422: Computer Forensics and Incidence Response	CIS 523/423: Disaster Recovery and Business Continuity	CIS 524/424: Information Assurance Risk Assessment	CIS 525/425: Principles of Cryptography
E - List database best practices and pitfalls in database security		X				
3. Distributed Systems Security						
E - Discuss risks associated with distributed systems security		X				
4. Firmware Security						
E - Discuss differences between security features and capabilities		X				
7. Network Security Software						
E - Discuss state and vulnerabilities in network security software		X				
9. Technology Trends						
E - Summarize technology trends in context of future security management plan					X	
10. Environmental/Natural Threats						
*E - List environmental and natural threats as part of security management plan				X		
E - Discuss environmental and natural threats as part of security management plan				X		