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
4012 Points						
*** = Can include a summary justification for that section.**						
FUNCTION 1 - GRANT FINAL ATO						
A. Responsibilities						
1. Aspects of Security						
*Explain the importance of SSM role in Information Assurance (IA)	X					
2. Accreditation						
*Discuss accreditation	X					
Discuss the certification process leading to successful accreditation	X					
Explain the importance of accreditation	X					
Explain types of accreditation	X					
Facilitate the certification process leading to successful accreditation	X					
Discuss the significance of NSTISSP No. 6	X					
B. Approvals						
1. Approval to Operate (ATO)						
*Explain ATO	X					
Discuss purpose and contents of ATO	X					
Explain the importance of risk assessment to support granting an ATO	X					
2. Interim Approval to Operate (IATO)						
*Describe IATO	X					
Explain the purpose and contents of IATO	X					
Explain the importance of risk assessment to support granting an IATO	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
Facilitate implementation of risk mitigation strategies necessary to obtain IATO		X				
3. Recertification						
*Describe recertification		X				
Direct the recertification effort		X				
Explain the importance of the recertification process		X				
Identify characteristics of information systems that need re-certification		X				
Initiate the recertification effort		X				
4. Systems Security Authorization Agreement (SSAA)						
*Discuss the Systems Security Authorization Agreement (SSAA)		X				
Explain the importance of the SSAA		X				
5. Waive Policy to Continue Operation						
*Discuss justification for waiver		X				
Discuss risk mitigation strategies necessary to obtain waiver		X				
Ensure risk assessment supports granting waiver		X				
FUNCTION 2 - REVIEW ACCREDITATION						
A. Threats						
1. Attacks						
*Discuss threats/attacks to systems		X			X	
Explain the importance of threats/attacks on systems		X			X	
2. Environmental / Natural Threats						
*Discuss environmental/natural threats		X		X		
3. Human Threats						
*Explain the importance of intentional and unintentional human threats		X				
4. Theft						
*Explain the importance of theft		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
5. Threat						
*Explain threat		X			X	
Explain the importance of organizational threats		X			X	
6. Threat Analysis						
*Explain the importance of threat analysis		X			X	
7. Threat Assessment						
*Explain the importance of threat assessment		X			X	
B. Countermeasures						
1. Education, Training, and Awareness as Countermeasures						
*Explain the importance of educational training, and awareness as countermeasures		X			X	
Ensure educational training, and awareness countermeasures are implemented		X			X	
2. Procedural Countermeasures						
*Explain the importance of procedural/administrative countermeasures		X			X	
Ensure procedural/administrative countermeasures are implemented		X				
3. Technical Countermeasures						
*Explain the importance of automated countermeasures/deterrents		X			X	
Explain the importance of technical countermeasures/deterrents		X			X	
Ensure technical/automated countermeasures/deterrents are implemented		X				
C. Vulnerability						
1. Vulnerability						
*Explain vulnerability		X			X	
2. Vulnerability Analysis						
*Explain the importance of vulnerability analysis		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
3. Network Vulnerabilities						
*Explain the importance of network vulnerabilities					X	
4. Technical Vulnerabilities						
*Explain the importance of technical vulnerabilities					X	
D. Risk Management						
1. Cost / Benefit Analysis of Information Assurance						
*Explain the importance of cost/benefit analysis of information assurance					X	
2. Documentation						
*Explain the importance of documentation role in reducing risk					X	
3. Risk						
*Explain risk		X				
Discuss principles of risk		X			X	
4. Risk Assessment						
*Explain the importance of risk assessment		X			X	
5. Risk Management						
*Explain the importance of risk management		X			X	
6. Residual Risk						
*Explain residual risk		X			X	
7. Risk Acceptance Process						
*Explain the importance of the risk acceptance process		X				
8. Systems Security Authorization Agreement (SSAA)						
*Explain the importance of the certification and accreditation (C&A) effort leading to accreditation		X				
Discuss the contents of SSAA		X				
Discuss the purpose of SSAA		X				
Ensure the certifier understands the mission and it is reflected in SSAA the C&A effort leading to SSAA		X				
Facilitate effort leading to SSAA		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
FUNCTION 3 - VERIFY COMPLIANCE						
A. Laws Related To Information Assurance (Ia) And						
1. Copyright Protection and Licensing						
*Explain the importance of copyright protection		X	X			
Explain the importance of licensing		X	X			
2. Criminal Prosecution						
*Explain the importance of criminal prosecution			X			
3. Due Diligence						
*Explain the importance of due diligence			X			
4. Evidence Collection and Preservation						
*Explain the importance of evidence collection			X			
Explain the importance of evidence preservation			X			
5. Fraud, Waste, and Abuse						
*Explain fraud, waste, and abuse			X			
6. Laws Related To Information Assurance and Security						
*Explain the importance of implications of Electronic Records Management and Federal Records Act		X	X			
Explain the importance of implications of Federal Managers Financial Integrity Act of 1982		X	X			
Explain the importance of implications of Federal Property and Administration Service Act			X			
Explain the importance of implications of USA Patriot Act, GPEA, and Paperwork Reduction Acts		X	X			
Explain the importance of implications of legal issues which can affect Information Assurance (IA)		X	X			
Explain the importance of implications of National Archives and Records Act			X			
Explain the importance of implications of the Computer Fraud and Abuse Act, P.L. 99- 474, 18 U.S. Code 1030		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
Explain the importance of implications of the Freedom of Information Act and Electronic Freedom of Information Act			X			
Explain the importance of Public Law 107-347, E-Government Act 0f 2002, Title III, Federal Information Security Management Act (FISMA), 17 Dec 02		X	X			
Explain the importance of implications of the legal responsibilities of senior systems managers		X				
Explain the importance of implications of the Privacy Act		X	X			
Discuss implications of Public Law 107-347 regarding certification and accreditation		X				
7. Legal and Liability Issues						
*Explain the importance of legal and liability issues as they apply to system and mission		X				
8. Ethics						
*Discuss ethics		X				
B. Policy Direction						
1. Access Control Policies						
*Explain the importance of access control policies		X				X
2. Administrative Security Policies And Procedures						
*Explain the importance of administrative security policies/procedures		X				
3. Audit Trails and Logging Policies						
*Explain the importance of audit trail policy					X	
Explain the importance of logging policies					X	
4. Documentation Policies						
*Explain the importance of documentation policies					X	
5. Evidence Collection and Preservation Policies						
*Explain the importance of evidence collection/preservation policies			X			
6. Information Security Policy						

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
*Define information security policy		X				
Explain the importance of information security policy		X				
7. National Information Assurance (IA) Certification & Accreditation (C&A) Process Policy						
*Explain the importance of the National Information Assurance (IA) Certification & Accreditation (C&A) Policy		X				
8. Personnel Security Policies & Guidance						
Explain the importance of personnel security guidance		X				
C. Security Requirements						
1. Access Authorization						
*Explain the importance of access authorization		X				
2. Auditable Events						
*Explain auditable events					X	
3. Authentication						
*Explain authentication		X				X
4. Background Investigations						
*Explain the importance of background investigations		X				
5. Countermeasures						
*Explain the importance of countermeasures		X				
6. Delegation of Authority						
*Discuss the importance of delegation of authority		X				
Ensure that individuals are assigned to perform IA functions		X				
7. Education, Training, and Awareness						
*Explain the importance of education, training, and awareness as countermeasures		X			X	
Ensure educational, training, and awareness countermeasures are implemented		X			X	
8. Electronic Records Management						
*Discuss electronic records management		X				
Explain the importance of electronic records management		X				
9. Electronic-Mail Security						

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
*Discuss electronic-mail security						X
Explain the importance of electronic-mail security						X
10. Information Classification						
*Discuss information classification		X		X		
Explain the importance of information classification		X		X		
11. Investigative Authorities						
*Discuss investigative authorities			X			
Explain the importance of investigative authorities			X			
12. Key Management Infrastructure						
*Discuss key management infrastructure						X
13. Information Marking						
*Discuss information marking		X		X		
14. Non-repudiation						
*Discuss non-repudiation					X	
Explain the importance and role of non-repudiation					X	
15. Public Key Infrastructure (PKI)						
Explain the importance and role of PKI		X				X
FUNCTION 4 - ENSURE ESTABLISHMENT OF SECURITY						
A. Administration						
1. Accountability for Classified / Sensitive Data						
*Explain the importance of accountability for sensitive data		X		X		
Discuss classification and declassification of information		X		X		
2. Automated Security Tools						
*Explain the importance of automated security tools					X	
3. Backups						
*Discuss backups		X		X		
Explain the importance of backups		X		X		
4. Change Control / Configuration Management						
*Discuss change control		X				
Discuss configuration management		X				
Explain the importance of configuration management		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
5. Declassification / Downgrade of Media						
*Explain the importance of downgrade of media		X		X	X	
Discuss the importance of downgrade of information		X		X	X	
6. Destruction / Purging / Sanitization of Classified / Sensitive Information						
*Explain the importance of destruction/purging/sanitization procedures for classified/sensitive information		X		X	X	
B. Access						
1. Access Controls						
*Define manual/automated access controls		X				
Explain the importance of manual/automated access controls		X				
2. Access Privileges						
*Explain the importance of access privileges		X				
3. Discretionary Access Controls						
*Discuss discretionary access controls		X				
Explain the importance of discretionary access controls		X				
4. Mandatory Access Controls						
*Define mandatory access controls		X				
Explain the importance of mandatory access controls		X				
5. Biometrics / Biometric Policies						
*Explain biometric policies		X				
6. Separation of Duties						
*Define the need to ensure separation of duties where necessary		X				
Explain the importance of the need to ensure separation of duties where necessary		X				
7. Need-To-Know Controls						
*Define need to know controls		X				
Explain the importance of need to know controls		X				
C. Incident Handling And Response						
1. Emergency Destruction Procedures						

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
*Explain the importance of emergency destruction procedures				X		
2. Organizational / Agency Information Assurance Emergency Response Teams						
*Explain the role of organizational/agency information assurance emergency response teams				X		
D. Continuity Of Operations Planning						
1. Business Recovery						
*Define business recovery		X		X		
Explain the importance of business recovery		X		X		
2. Contingency / Continuity of Operations Planning						
*Explain the importance of contingency/continuity of operations planning		X		X		
Ensure the establishment and testing of contingency/continuity of operations plans				X		
3. Disaster Recovery						
*Explain the importance of disaster recovery		X		X		
4. Disaster Recovery Plan						
*Explain the importance of recovery plan		X		X		
Ensure the establishment and testing of recovery plans				X		
5. Incident response policies						
*Explain the importance of incident response policy				X		
6. Law enforcement interfaces / policies						
*Discuss law enforcement interfaces			X			
Discuss law enforcement policies			X			
Explain the importance of law enforcement interfaces			X			
7. Reconstitution						
*Define principles of system reconstitution				X		
Explain the importance of principles of system reconstitution				X		
8. Restoration						
*Explain the importance of restoration to continuity of operation				X		

FUNCTION 5 - ENSURE PROGRAM MANAGERS DEFINE

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
A. Acquisition						
1. Certification Test & Evaluation (CT&E)						
*Define CT&E as part of acquisition process		X				
Discuss the importance of CT&E as part of acquisition process		X				
2. Certification Tools						
*Discuss significance/results of certification tools		X				
3. Product Assurance						
*Explain the importance of product assurance role in acquiring systems, i.e., NSTISSP No. 11, Jan 00		X				
Explain the importance of protection profiles		X				
Explain the importance of security targets		X				
4. Contracting For Security Services						
*Discuss types of contracts for security services					X	
Define where contracting for security services is appropriate					X	
Explain threats from contracting for security services		X			X	
5. Disposition of Classified Material						
*Discuss disposition of classified materials		X		X		
Explain the importance of the correct disposition of classified material		X		X		
Explain the importance of remanence		X		X		
6. Facilities Planning						
*Discuss facilities planning		X				
Explain the importance of facilities planning		X				
7. System Disposition/Reutilization						
*Explain the importance of vulnerabilities from improper disposition/reutilization		X		X		
B. Life Cycle Management						
1. Life Cycle System Security Planning						
*Discuss life cycle security planning		X				
Explain the importance of life cycle system security planning		X				
2. System Security Architecture						

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
*Discuss system security architecture					X	
Explain how system security architecture supports continuity of operations CONOPS					X	
FUNCTION 6 - ASSIGN RESPONSIBILITIES						
N/A						
1. Certification and Accreditation (C&A)						
*Discuss responsibilities associated with accreditation		X				
Discuss roles associated with certification		X				
Explain importance of certification and accreditation (C&A)		X				
Facilitate the C&A process		X				
2. Information Ownership						
*Explain the importance of establishing information ownership					X	
3. System Certifiers and Accreditors						
*Discuss risk as it applies to certification and accreditation		X				
4. Risk Analysts						
*Discuss risk analyst?s reports		X				
Discuss systems certifiers and accreditors in risk mitigation		X				
5. Information System Security Manager (ISSM)						
*Define the role of Information Assurance Manager (ISSM)		X				
6. Information System Security Officer (ISSO)						
*Define the role of System Security Officer (ISSO)		X				
FUNCTION 7 - DEFINE CRITICALITY AND SENSITIVITY						
N/A						
1. Aggregation						
*Explain the importance of the vulnerabilities associated with aggregation					X	
2. Disclosure of Classified/Sensitive Information						
*Explain the liabilities associated with disclosure of classified/sensitive information		X		X		
FUNCTION 8 - ALLOCATE RESOURCES						
N/A						

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. Resource Roles and Responsibilities						
*Discuss the respective roles and responsibilities of resource management staff		X				
Assign/appoint key resource managers		X				
2. Budget / Resource Allocation						
*Evaluate the information assurance budget		X				
Explain the importance of the information assurance budget		X				
Defend the budget for information assurance		X				
3. Business Aspects of Information Security						
*Discuss business aspects of information security					X	
Discuss protection of commercial proprietary information					X	
Explain the importance of business aspects of information security					X	
Explain the importance of protecting commercial proprietary information					X	
FUNCTION 9 - MULTIPLE AND JOINT ACCREDITATION						
N / A						
1. Memoranda of Understanding / Agreement (MOU / MOA)						
*Explain the importance of MOU/MOA		X				
Facilitate development and execution of MOU/MOA		X				
FUNCTION 10 - ASSESS NETWORK SECURITY						
N / A						
1. Connectivity						
*Discuss connected organizations	X					X
Discuss connectivity involved in communications	X					X
Explain the importance of connectivity involved in communications	X					X
2. Emissions Security (EMSEC) and TEMPEST						
*Define TEMPEST requirements		X				
Discuss threats from Emissions Security (EMSEC)		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
Discuss threats from TEMPEST failures		X				
Explain the importance of the threats from Emissions Security (EMSEC)		X				
Explain the importance of the threats from TEMPEST failures.		X				
3. Wireless Technology						
*Discuss electronic emanations	X					X
Discuss threats from electronic emanations						X
Explain the importance of wireless technology	X					X
Explain the risks associated with portable wireless systems, viz., PDAs, etc.						X
Explain the importance of vulnerabilities associated with connected systems wireless technology						X