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*  
   E - Identify agency-specific system reutilization policies and procedures

3. **System Configuration and Management Board (SCMB)**
   *E - Identify life cycle management SCMB policies and procedures*

4. **Operations & Maintenance (O & M)**
   *E - Discuss risk analysis processes used in development of life cycle functions*  
   E - Monitor life cycle operation and maintenance project milestones relating to risk  
   E - Monitor maintenance procedures concerning life cycle operations and analysis issues  
   E - Monitor performance measurement data in operations and maintenance examination of events and/or changes in an event

5. **System Acquisition**
   *E - Discuss risk analyst concerns relating to life cycle system security planning*  
   E - Monitor process of selecting and purchasing IT designed to implement management risk process  
   E - Verify that system acquisitions policies and procedures include assessment of risk management policies
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6. System Administration</td>
<td>*E - Discuss audit mechanism processes used to collect, review, and/or examine system activities</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. System Owners</td>
<td>*E - Discuss maintenance plans for protective measures to ensure tolerable level of risk</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. System Developers</td>
<td>*E - Discuss process for selecting and purchasing new information technology (IT)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>E - Discuss process to ensure that applications function according to specifications</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E - Explain risk methodologies used to evaluate measures taken to protect system</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Computer Science and Architecture</td>
<td>*E - Discuss system IA design guidance</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Security Product Integration</td>
<td>E - Examine and analyze applied security</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Information Systems Security Officer (ISSO) Activities</td>
<td>*E - Discuss maintenance of user accounts</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E - Discuss processes for timely deletion of accounts</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E - Discuss processes for updating access</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E - Discuss processes for verification of authorization prior to adding new account</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Audit Mechanism</td>
<td>*E - Review policy, guidance and process for the capture, maintenance, and distribution of audit logs</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. Policy Development</td>
<td>E - Develop risk management methodology which includes evaluation of threats, vulnerabilities, and countermeasures</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------</td>
<td>----------------------------------------------------</td>
<td>------------------------------------------------------</td>
<td>----------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
</tbody>
</table>

**14. System Certifiers and Accreditors**

*E - Explain how certification process ensures security requirement implementation

E - Explain local policies and procedures to supplement and implement higher-level guidance

**15. Automated Tool for Security Test**

E - Discuss utilities used to determine vulnerabilities or configurations not

**FUNCTION 2 - COUNTERMEASURES IDENTIFICATION, Countermeasures**

**No Subsection**

1. **General**

*E - Identify all component and overall risks inherent in system

E - Assist certifier to determine countermeasures based on threat capabilities and motivations

2. **Analyzing Potential Countermeasures**

*E - Discuss security test and evaluation (ST&E) procedures, tools, and equipment

E - Assist certifier to evaluate security requirements as potential countermeasures

E - Discuss respective value of penetration testing post-testing actions, general information principles, and summary comparison of network testing techniques

E - Discuss testing roles and responsibilities

E - Explain process to determine underlying state of system

E - Relate organization IT security needs to countermeasure requirements

3. **Determining Countermeasures**

E - Apprise decision makers of existing countermeasure models, tools, and techniques
|---------|-----------------------------|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|---------------------------------|---------------------------------|

### 4. Identifying Potential Countermeasures
- **E** - Discuss effectiveness of automated security tools that confirm validity of a transmission
- E - Assist certifier/IA engineer to evaluate system security safeguards established to determine system security posture
- E - Discuss effectiveness of automated security tools that verify an individual’s eligibility to receive specific categories of information

- E - Discuss methodologies used to evaluate system security safeguards

### 5. Determining Cost/Benefit of Countermeasures
- **E** - Outline cost/benefit of organization’s IA countermeasure plans

- E - Outline cost/benefit of personnel supporting access control policies

---

**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
- E - Discuss role of RA in certification and accreditation process

### 2. Vulnerabilities and Attacks
- **E** - Discuss paired interaction of a vulnerability to an attack

### 4. Security Laws
- E - Outline security laws applicable to certification/accreditation process

### 5. Physical Security Requirements
- E - Discuss risk mitigation decisions derived from analysis and review of

### 6. Security Inspections
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS 444: Computer Networking</td>
<td>E - Evaluate security inspections conducted during C&amp;A process</td>
<td>E - Discuss security inspections conducted during C&amp;A process</td>
<td>E - Explain security policies and procedures implemented during risk analysis/assessment process</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 521/421: Introduction to Information Assurance</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 523/423: Disaster Recovery and Business Continuity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 524/424: Information Assurance Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 525/425: Principles of Cryptography</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*E - Evaluate security inspections conducted during C&A process
E - Discuss security inspections conducted during C&A process

7. Security Policies and Procedures
E - Explain security policies and procedures implemented during risk analysis/assessment process

8. Security Processing Mode
E - Discuss vulnerabilities associated with security processing modes

9. System Certification
*E - Discuss threat and vulnerability analyses input to C&A process

10. Support C&A
*E - Identify system security policies
E - Explain alternative actions permitted on system

11. System Security Profile
*E - Describe protections offered by security features in specific configurations
E - Assist in helping to identify protections offered by security features in specific configurations
E - Discuss security features of system

12. Threat/Risk Assessment
*E - Identify threat/risk assessment methodology appropriate for use with system undergoing accreditation

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

14. Mission
E - Discuss impact of security on mission

15. Interviewing/Interrogation
E - Assist certifier in preparing questions for determining countermeasures during C&A process
16. Applications Security
E - Discuss criticality of applications security

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

3. Aspects of Security
E - Discuss security with regard to confidentiality, integrity, authentication, availability, and non-repudiation

4. Assessment Methodology
E - Appraise information acquisition and review process for best use of resources to protect system

5. Associate Threat Probabilities to Vulnerability
E - Describe process of analyzing paired interactions of system threats and vulnerabilities

6. Conducting Risk Analysis
E - Conduct risk analysis examination and evaluation process to determine relationships among threats, vulnerabilities, and countermeasures

7. Countermeasure Analysis
*E - Conduct detailed examination and evaluation of impact of attacks
E - Conduct detailed examination and evaluation of possible actions to mitigate vulnerabilities

8. Critical Thinking
E - Discriminate between known and hypothetical variables based on executed test procedures

9. Deductive Reasoning
*E - Analyze tests results
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10. Detailed Residual Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*E - Discuss susceptibility of a system to attack after countermeasures have been applied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Assist certifier/IA engineer in evaluating susceptibility of a system to attack after countermeasures have been applied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. All Risk Variables</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Evaluate an analysis of threats, vulnerabilities, attacks, and consequences in relationship to risk assessment of a system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. Risk Assessment (Environment &amp; Threat Description)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Discuss environment in relation to current threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. Risk Management Methodology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Discuss organizational capability and ability to evaluate threats, and vulnerabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16. Security Countermeasures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Assist certifier/IA engineer in defining countermeasures directed at specific threats and vulnerabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17. Technical Vulnerability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Discuss hardware, firmware, communications, or software weaknesses that open an information system to exploitation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18. Threat Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Examine methods through which threat agent adversely affects information system, facility, or operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19. Threat Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Define means through which a threat agent can adversely affect information system, facility, or operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20. Threat/Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Discuss process of formally evaluating degree of threat and describing nature of threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21. Mission</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*E - Discuss information system support mission</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**22. Vulnerabilities**

*E - Assist in identifying weakness in an information system, system security procedures, internal controls, or implementation that could be exploited

E - Discuss weakness in an information system, system security procedures, internal controls, or implementation that could be exploited

E - Explain hardware or software flow that opens an information system to potential exploitation

**23. Vulnerability Analysis**

*E - Analyze an information system to determine adequacy of security measures

**B. Documentation**

1. Policies

*E - Explain applicable national level policies

E - Discuss agency/local guidance

**9. Technical Knowledge of Information System**

E - Outline technical knowledge required of personnel responsible for networks, servers, workstations, operating systems, etc.

**C. Effect of Countermeasure**


E - Examine analysis of security safeguards of a system as they have been applied to an operational environment to determine security posture

**10. Technical Knowledge of Information System**

E - Outline technical knowledge required of personnel responsible for operating and maintaining networks, servers, workstations, operating systems, etc.

**FUNCTION 5 - TESTING AND EVALUATION**
Testing and Evaluation Duties

No Subsection

3. Account Administration
E - Discuss maintenance of accounting files, tools, user accounts, and system statistics

4. Assessment Methodology
E - Define vulnerability analysis process

5. Associate Threat Probabilities to Vulnerability
E - Explain paired interaction of system threats and vulnerabilities

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

7. Backups
E - Discuss purpose of using copies of backup files for later reconstruction of files

8. Software Test & Evaluation Results
E - Ensure software test and evaluation results related to system restoration are performed

E - Assist with the development of ST&E plan and procedure for testing and evaluating a system

13. Error Logs
E - Interpret files created by operating system for review of audit process

E - Interpret technical and non-technical results from testing and evaluation

15. Evaluation Techniques
|---------|-------------------------------|-----------------------------------------------|------------------------------------------------------|-------------------------------------------------|----------------------------------------|---------------------------------------|

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

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)

18. Certification Tools
E - Team with certifier/IA engineer to interpret results of certification tools during testing and evaluation

19. Privileges (Class, Nodes)
E - Influence program or user operations that can be performed during testing and Evaluation

20. Test and Evaluation Strategies
*E- Identify strengths of alternative test and evaluation strategies

21. Testing Implementation of Security Features
E - Integrate testing of security features during testing and evaluation

**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

2. Cost/Benefit Analysis
E - Conduct an assessment of costs of data protection for a system versus cost of loss or compromise

3. Critical Thinking
E - Discuss known and hypothetical variables based on test procedures

4. Deductive Reasoning
E - Recommend solutions based on a set of static and variable factors of system

5. Effects of Mitigation
E - Determine effects of mitigation derived from application of countermeasures to a system

6. Hostile Intelligence Sources
E - Discuss impact of hostile agents seeking national security information which could potentially cause harm to national security

7. All Risk Variables
E - Build a compendium of relative threats, vulnerabilities, attacks, and consequences related to system

B. Risk Assessment (Environment & Threat Description)

1. Risk Management Methodology
E - Discuss evaluation of threats, vulnerabilities, and countermeasures to determine residual risk

2. Security Countermeasures
E - Discuss security and software countermeasures during design, implementation, and testing phases to achieve required level of confidence

3. Threat Analysis
E - Conduct examination and evaluation of sources and factors that can adversely impact system

4. Threat Description
E - Identify level of threat based on its applicability to system

5. Threat/Risk Assessment
E - Recommend life cycle countermeasures based on assessments of threats, capabilities, and motivations to exploit vulnerability

6. Mission
*E - Discuss current mission and role of information system in supporting mission
E - Determine if an adverse system finding should be allowed to halt mission support operations

7. Vulnerability Analysis
E - Appraise weaknesses in information system, security procedures, internal controls, or implementations that could be exploited

C. Analysis for Decisions
1. Agency-Specific Policies and Procedures
E - Discuss local policies and procedures implementing regulations, laws, and procedures in local environment

H. Technical Surveillance Countermeasures
1. Technical Surveillance Countermeasures
E - Discuss Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies

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
E - Conduct detailed examination of vulnerabilities, attack, threats, and consequences that may affect system

2. Cost/Benefit Analysis
E - Conduct cost assessment for providing data protection versus cost of data loss or compromise
|-------------------------------|------------------------------|--------------------------------------------------|------------------------------------------------------|-----------------------------------------------------|--------------------------------------------------|-----------------------------------|

### 3. Critical Thinking

E - Understand known and hypothetical variables based on test procedures

### 4. Deductive Reasoning

E - Recommend solutions based on a set of static and variable factors

### 5. Effects of Mitigation

E - Determine effects of mitigation derived from application of countermeasures

### 6. Hostile Intelligence Sources

E - Discuss impact of hostile agents seeking national security information which could potentially cause harm to national security

### 7. All Risk Variables

E - Build a compendium of relative threats, vulnerabilities, attacks, and consequences related to system

#### B. Risk Assessment (Environment & Threat Description)

### 1. Risk Management Methodology

E - Discuss evaluation of threats, vulnerabilities, and countermeasures to determine residual risk

### 2. Security Countermeasures

E - Discuss security and software countermeasures during design, implementation and testing phases to achieve required level of confidence

### 3. Threat Analysis

*E - Conduct detailed examination and evaluation of sources and factors that can adversely impact system

### 4. Treat Description

E - Identify level of threat based on its applicability to system

### 5. Threat/Risk Assessment
|---------|-------------------------------|-------------------------------------------------|-------------------------------------------------|------------------------------------------------|-------------------------------------------------|------------------------------------------------|

E - Recommend life cycle countermeasures based on assessment of threats, capabilities, and motivations to exploit vulnerability

6. Mission

E - Assess mission to determine if an adverse finding should be allowed to affect continued IT operations in a given mission environment

7. Vulnerability Analysis

E - Appraise exploitable weaknesses in information system, security procedures, internal controls or implementations

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

H. Technical Surveillance Countermeasures

1. Technical Surveillance Countermeasures

E - Discuss techniques and measures to detect and neutralize hostile penetration technologies

**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

2. Cost/Benefit Analysis

E - Discuss cost analysis of data protection versus cost of data lose or compromise

3. Critical Thinking

E - Apply discrimination to known and potential vulnerabilities based on test procedures
<table>
<thead>
<tr>
<th>Course Title</th>
<th>Course Code(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS 444: Computer Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 521/421: Introduction to Information Assurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 522/422: Computer Forensics and Incidence Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 523/423: Disaster Recovery and Business Continuity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 524/424: Information Assurance Risk Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 525/425: Principles of Cryptography</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. Deductive Reasoning
E - Use test results to determine underlying state of system

5. Effect of Countermeasures on Risk
E - Determine effect of countermeasures on risk through the analysis of paired interaction of a defense

6. Effects of Mitigation
E - Determine effects of mitigation derived from application of countermeasures to system

7. Hostile Intelligence Sources
E - Discuss hostile intelligence sources as part of vulnerabilities and attack venues

8. Risk Variables
E - Identify risk variables to build a compendium of relative threats, vulnerabilities, attacks, and consequences related to a system

9. Jamming
E - Discuss jamming as a potential threat

10. Risk Assessment
E - Define risk assessment methodology in relation to risk analyst function

11. Risk Management Methodology
E - Define risk management methodology in relation to system security

12. Security Countermeasures
E - Discuss security countermeasures in relation to vulnerabilities and attack venues

13. Threat Analysis
E - Use threat analysis to determine vulnerabilities and attack venues

14. Threat/Risk Assessment
E - Apply threat and/or risk assessment in determining vulnerabilities and attack venues

15. Mission
E - Support organizational mission in conjunction with vulnerabilities and attack venues

16. Vulnerabilities
E - Discuss weaknesses in system, system security procedures, and internal controls and implementation

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

B. Developing Attack Avenues
1. Avenues of Attack
E - Describe known avenues of attack such as operating system bugs, network vulnerabilities, human threats, etc.

C. Characterizing Vulnerabilities
1. Characterizing Vulnerabilities

*E - Discuss aspects of security in a vulnerability testing and evaluation plan
E - Evaluate threats and vulnerabilities

D. Researching Vulnerability Report
1. Researching Vulnerability Report
E - Evaluate vulnerability assessment methodologies

E. Collecting and Reviewing Vulnerabilities
1. Collecting and Reviewing Vulnerabilities

*E - List potential vulnerabilities that may lead to defeat of security services

F. Comparing and Contrasting Attack Avenues
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Comparing and Contrasting Attack Avenues</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*E - Discuss techniques and measures to detect or neutralize a wide variety of hostile penetration technologies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Evaluate payoff to and liabilities incurred by an attacker in a successful attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G. Risk of Detection and Response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Risk of Detection and Response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Characterize impact of security breaches and estimate an attacker's probable Response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I. Technology Necessary to Mount Attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Technology Necessary to Mount Attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Describe technology needed to mount an attack based on existing countermeasures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FUNCTION 9 - TRAINING AND AWARENESS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training and Awareness Duties</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Policies/Procedures/Methodology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Access Control Policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*E - Summarize national and local level access control policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Laws, Regulations, and Other Public Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*E - Identify local application of IA laws, regulations, and policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Discuss applicable IA laws, regulations, and policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Agency-Specific IA and IT Policies and Procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*E - Summarize agency-specific policies and procedures in relation to risk environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Audit Trails and Logging Policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*E - Discuss audit trails and logging policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Change Control Policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*E - Discuss change control policies for incorporation in IA training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Communications Security Policy and Guidance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
*E - Discuss communications security policy and guidance for incorporation into IT training
E - Identify communications security policy and guidance for incorporation into IT training

8. Emergency Destruction Planning and Procedures (EDPP)
*E - Discuss EDPP for incorporation in IA training

E - Discuss role of personnel security policies and guidance as part of overall risk management plan

E - Outline role of formal methods in security design as part of risk management plan

11. Information Categorization
E - Discuss various categorization schemas

12. Information Classification
*E - Discuss classification policies as part of risk management plan

*E - Discuss definitions of security requirements

15. Physical Security Requirements
*E - Discuss physical security requirements

17. Risk Management Methodology
E - Summarize approaches to risk management

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

2. Database Security Features
*E - Discuss elements of database security features
E - Identify critical database security pitfalls
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>E - List database best practices and pitfalls in database security</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Distributed Systems Security</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Discuss risks associated with distributed systems security</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Firmware Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Discuss differences between security features and capabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Network Security Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Discuss state and vulnerabilities in network security software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Technology Trends</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E - Summarize technology trends in context of future security management plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>10. Environmental/Natural Threats</td>
<td>*E - List environmental and natural threats as part of security management plan</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E - Discuss environmental and natural threats as part of security management plan</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>