

DOE CYBERSECURITY:

CORE COMPETENCY TRAINING REQUIREMENTS

Key Cybersecurity Role: **Security Control Assessor** {Also known as Certification Agent (CA)}

Role Definition: The Security Control Assessor is the individual responsible for assessing the management, operational, assurance, and technical security controls implemented on an information system via security testing and evaluation (ST&E) methods. This individual must be independent of system development, operation, and deficiency mitigation.

Competency Area: **Data Security**

Functional Requirement: **Implement**

Competency Definition: Refers to the application of the principles, policies, and procedures necessary to ensure the confidentiality, integrity, availability, and privacy of data in all forms of media (i.e., electronic and hardcopy) throughout the data life cycle.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will understand and assess the policies and procedures implemented to protect all categories of information as well as have a working knowledge of technical controls used to ensure the confidentiality, integrity, and availability of data based on a formally approved need-to-know.

Training concepts to be addressed at a minimum:

- Verify data security access controls, privileges, and associated profiles via the ST&E process.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of DOE/Risk Management Implementation Plans (RMIPs) data security policies, processes, and procedures.
- Demonstrate a **detailed** knowledge of established standards and guidelines.
- Demonstrate the **detailed** ability to analyze implemented controls and evaluate their effectiveness and compliance with policy, standards, and guidelines

- Demonstrate the **detailed** ability to devise tests and procedures for use in ST&E of individual systems
- Demonstrate a **functional** knowledge of security capabilities of the most prominent commercial operating systems

Competency Area: **Data Security**

Functional Requirement: **Evaluate**

Competency Definition: Refers to the application of the principles, policies, and procedures necessary to ensure the confidentiality, integrity, availability, and privacy of data in all forms of media (i.e., electronic and hardcopy) throughout the data life cycle.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will understand and assess the policies and procedures implemented to protect all categories of information as well as have a working knowledge of technical controls used to ensure the confidentiality, integrity, and availability of data based on a formally approved need-to-know.

Training concepts to be addressed at a minimum:

- Evaluate the effectiveness of the sensitivity determination processes by assessing unclassified non-SUI data at rest for OPSEC issues
- Evaluate the effectiveness of solutions implemented to provide the required protection of data, including appropriate authenticator management and encryption controls
- Assess data transmissions (e.g., email, file transfers, etc.) to evaluate the protection mechanisms being utilized (e.g., sensitivity determinations, sensitivity labels, encryption, etc.).
- Evaluate the effectiveness of the media sanitization (clearing, purging, or destroying) and reuse processes.
- Evaluate the effectiveness of the processes and procedures for protecting SUI, including PII.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of Departmental/RMIP data security policies, processes, and procedures.
- Demonstrate a **detailed** knowledge of established standards and guidelines.
- Demonstrate a **detailed** knowledge of identifying sensitive, non-SUI and SUI information
- Demonstrate a **functional** ability to determine sensitive, non-SUI and SUI information protections

- Demonstrate the **detailed** ability to analyze implemented controls and evaluate their effectiveness and compliance with policy, standards, and guidelines

Competency Area: **Enterprise Continuity**

Functional Requirement: **Evaluate**

Competency Definition: Refers to application of the principles, policies, and procedures used to ensure that an organization continues to perform essential business functions within a defined accreditation boundary after the occurrence of a wide range of potential catastrophic events.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will understand and evaluate the policies and procedures implemented to ensure continuity of operations required for essential business functions as a result of a disruption in service.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of the continuity program, processes, and procedures and make recommend changes as appropriate.
- Review test, training, and exercise results to determine if information systems are available within organization or Senior DOE Management mission-requirement time frames.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of Departmental/RMIP data security policies, processes, and procedures.
- Demonstrate a **detailed** knowledge of test methodologies used to evaluate availability controls
- Demonstrate a **detailed** ability to analyze test data, reports, and training records for control compliant continuity operations

Competency Area: **Information Technology (IT) Systems Operations and Maintenance**

Functional Requirement: **Evaluate**

Competency Definition: Refers to the ongoing application of principles, policies, and procedures to maintain, monitor, control, and protect IT infrastructure and the information residing on such infrastructure during the operations phase of an IT system or application. Individuals with these

functions perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are implemented and maintained on information systems.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will be knowledgeable of the policies, procedures, and controls required to protect IT infrastructure and data and will be able to assess technical, operational, and/or administrative security controls as mandated by Departmental/RMIP standards.

Training concepts to be addressed at a minimum:

- Evaluate the performance and correctness of applied security controls in accordance with standards, procedures, directives, policies, and regulations and recommend corrective actions as needed.
- Assess the performance of security administration measurement technologies.
- Assess the effectiveness of the patch and vulnerability management processes.
- Identify improvement actions via a documented POA&M based on reviews, assessments, and other data sources.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of Departmental/RMIP data security policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **detailed** ability to analyze the implementation of controls and propose changes in implementation
- Demonstrate a **detailed** ability to analyze control implementation to determine compliance with Departmental/RMIP data security policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** knowledge of security technologies available for demonstrating and measuring control implementations
- Demonstrate a **functional** knowledge of the purpose of POA&Ms and the procedures for creating and coordinating a POA&M

Competency Area: **Network and Telecommunications Security and Remote Access**

Functional Requirement: **Evaluate**

Competency Definition: Refers to the application of principles, policies, and procedures involved in ensuring the security of basic network and telecommunications services and data and in maintaining the hardware layer on which the data resides. Examples of these practices include perimeter defense strategies, defense-in-depth strategies, and data encryption techniques.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will understand the policies and procedures implemented to protect network and telecommunication services and be able to assess applicable technical security controls such as perimeter defense, defense-in-depth, and data encryption techniques.

Training concepts to be addressed at a minimum:

- Assess network, anti-malware, and perimeter defense policies in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations and recommend corrective actions if needed.
- Assess procedures and controls implemented to protect telecommunication networks from unauthorized access.
- Evaluate interconnected systems to ensure that they do not negatively impact the confidentiality, integrity, and availability of connected systems.
- Assess the implementation of remote access policies to ensure adequate protection of DOE information when processed offsite.
- Evaluate the effectiveness of implemented policies, procedures, and minimum security controls for portable/mobile devices, external information systems, wireless technologies, and P2P network capabilities.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of Departmental/RMIP data security policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **detailed** knowledge of network and telecommunication policies, procedures, and controls and the implementation of technologies used for the interconnection of systems/networks via wired or wireless access, remote access, P2P, and the utilization of external systems
- Demonstrate a **functional** knowledge of the vulnerabilities, issues, and threats that are related to the use of various networking technologies and the interconnection of networks/systems/components
- Demonstrate a **detailed** ability to determine the effectiveness of network, external system, and remote user training

Competency Area: Regulatory and Standards Compliance

Functional Requirement: Implement

Competency Definition: Refers to the application of principles, policies, and procedures that enable an organization to meet applicable information security laws, regulations, standards, and policies to satisfy statutory requirements, perform industry-wide best practices, and achieve information security program goals.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will understand and assess policies and procedures implemented to ensure organizational compliance with applicable laws, regulations, and/or Departmental/RMIP requirements.

Training concepts to be addressed at a minimum:

- Conduct comprehensive assessments via the ST&E process to determine if information security objectives, controls, processes, and procedures are effectively applied and maintained, and perform as expected.

Training Evaluation Criteria: Demonstrate

Methods of Demonstration: Examination; Simulation; Desk Top Analysis

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of Departmental/RMIP data security policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **detailed** knowledge of testing and evaluation methodologies and when each is applicable
- Demonstrate a **detailed** ability to accomplish ST&E activities within cost and schedule constraints
- Demonstrate a **detailed** ability to analyze the implementation of controls, the accomplishment of security objectives, and the operating/performance characteristics

Competency Area: Regulatory and Standards Compliance

Functional Requirement: Evaluate

Competency Definition: Refers to the application of principles, policies, and procedures that enable an organization to meet applicable information security laws, regulations, standards, and policies to satisfy statutory requirements, perform industry-wide best practices, and achieve information security program goals.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will understand and assess policies and procedures implemented to ensure organizational compliance with applicable laws, regulations, and/or Departmental/RMIP requirements.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of compliance security program controls against Departmental/RMIP standards, policies, procedures, guidelines, and regulations.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of Departmental/RMIP data security policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **detailed** ability to determine control implementation compliance with Departmental/RMIP data security policies, processes, procedures, directives, regulations, and public laws (statutes)

Competency Area: **Security Risk Management**

Functional Requirement: **Implement**

Competency Definition: Refers to the knowledge of policies, processes, and technologies used to create a balanced approach to identifying and assessing risks to information assets, personnel, facilities, and equipment, and to manage mitigation strategies that achieve the security needed at an affordable cost.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will understand risk management policies and procedures and will be able to assess the effectiveness of the risk management program to include mitigation strategies.

Training concepts to be addressed at a minimum:

- Implement threat and vulnerability assessments to identify security risks and regularly update applicable security controls as required.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge
Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials
Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** ability to analyze controls for process improvement/continuous monitoring effectiveness in implementing compliance with DOE/RMIP policies, processes, procedures, directives, and regulations and identifying/mitigating vulnerabilities
- Demonstrate a **detailed** ability to evaluate the applicability of threats and vulnerabilities to networks/information systems

Competency Area: **Security Risk Management**

Functional Requirement: **Evaluate**

Competency Definition: Refers to the knowledge of policies, processes, and technologies used to create a balanced approach to identifying and assessing risks to information assets, personnel, facilities, and equipment, and to manage mitigation strategies that achieve the security needed at an affordable cost.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will understand risk management policies and procedures and will be able to assess the effectiveness of the risk management program to include mitigation strategies.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of the risk management program via the ST&E process and recommend changes where required.
- Review the performance of risk management tools and techniques.
- Assess residual risk in the information infrastructure used by the organization.
- Assess the results of threat and vulnerability assessments.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge
Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials
Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of threats and vulnerabilities to evaluate the potential impact and related risk to an Operating Unit infrastructure and individual systems
- Demonstrate a **detailed** knowledge of technologies used within an Operating Unit and its potential to be compromised
- Demonstrate a **detailed** ability to analyze vulnerabilities and threats to determine the likelihood of successful attack and resulting impacts
- Demonstrate a **functional** ability to identify the level of effectiveness for controls, as implemented, to reduce risk to information and information systems
- Demonstrate a **functional** ability to describe the residual risk based on the ST&E results

Competency Area: **System and Application Security**

Functional Requirement: **Manage**

Competency Definition: Refers to the knowledge of principles, practices, and procedures required to integrate information security into an IT system or application during the System Development Life Cycle (SDLC). The goal of this activity is to ensure that the operation of IT systems and software does not present undue risk to the organization and information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation, certification and accreditation (C&A), and software security standards compliance.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will understand SDLC policies and processes and will be able to assess the adequacy of implemented management, operational, assurance, and technical security controls via the ST&E process.

Training concepts to be addressed at a minimum:

- Determine the level of effort and resources requirements needed to conduct ST&E processes and provide such information to the System Owner.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of project management principles and activities
- Demonstrate a **detailed** ability to construct ST&E schedules, activities, and costs estimates

Competency Area: **System and Application Security**

Functional Requirement: **Implement**

Competency Definition: Refers to the knowledge of principles, practices, and procedures required to integrate information security into an IT system or application during the System Development Life Cycle (SDLC). The goal of this activity is to ensure that the operation of IT systems and software does not present undue risk to the organization and information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation, certification and accreditation (C&A), and software security standards compliance.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will understand SDLC policies and processes and will be able to assess the adequacy of implemented management, operational, assurance, and technical security controls via the ST&E process.

Training concepts to be addressed at a minimum:

- Independently validate that engineered IT security and application security controls have been implemented correctly and are effective in their application during ST&E processes.
- Document validation results via the ST&E report documentation.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of various control implementations
- Demonstrate a **detailed** ability to analyze control implementation
- Demonstrate a **detailed** knowledge of security effectiveness measuring methods/schemes
- Demonstrate a **detailed** ability to determine control effectiveness
- Demonstrate a **detailed** knowledge of technical report writing
- Demonstrate a **detailed** ability to prepare written technical reports and summaries

Competency Area: **System and Application Security**

Functional Requirement: **Evaluate**

Competency Definition: Refers to the knowledge of principles, practices, and procedures required to integrate information security into an IT system or application during the System Development Life Cycle (SDLC). The goal of this activity is to ensure that the operation of IT systems and software does not present undue risk to the organization and information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation, certification and

accreditation (C&A), and software security standards compliance.

Behavioral Outcome: Individuals fulfilling the role of Security Control Assessor will understand SDLC policies and processes and will be able to assess the adequacy of implemented management, operational, assurance, and technical security controls via the ST&E process.

Training concepts to be addressed at a minimum:

- Assess and evaluate system compliance with Departmental policies and IT system security controls documented in the System Security Plan (SSP).

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of DOE/RMIP policies, processes, procedures, directives, and regulations
- Demonstrate a **detailed** ability to analyze controls for evaluating compliance of the SSP with DOE/RMIP policies, processes, procedures, directives, and regulations
- Demonstrate a **detailed** ability to analyze controls implementation for evaluating compliance with the SSP