Appendix J
ISSE Relationship to Sample SE Processes

This appendix relates the Information Systems Security Engineering (ISSE) process activities to specific processes for systems engineering (SE) and system acquisition. The purpose of this mapping is to help the reader who is familiar with these or similar processes to have a better understanding of the nature of the ISSE activities and of the SE skills involved. A discussion of the ISSE process is included in Information Assurance Technical Framework (IATF) Chapter 3, The Information Systems Security Engineering Process.

The ISSE Master Activity and Task List breaks down the ISSE process activities into tasks and subtasks. Besides the six technical process activities, two program management activities are included: Plan Technical Effort and Manage Technical Effort. The tasks presented in the list are used to map ISSE activities to SE processes in the tables that follow the list.

ISSE Master Activity and Task List

Activity–01  Discover Information Protection Needs

Task–01.1  Analyze organization’s mission
Task–01.2  Determine relationship and importance of information to mission
Task–01.3  Identify legal and regulatory requirements
Task–01.4  Identify classes of threats
Task–01.5  Determine impacts
Task–01.6  Identify security services
Task–01.7  Document the information protection needs
Task–01.8  Document security management roles and responsibilities
Task–01.9  Identify design constraints
Task–01.10 Assess information protection effectiveness
  Subtask–01.10.1  Provide/present documented information protection needs to the customer
  Subtask–01.10.2  Obtain concurrence from the customer in the information protection needs
UNCLASSIFIED

Appendix J
IATF Release 3.1—September 2002

Task–01.11 Support system certification and accreditation (C&A)
- Subtask–01.11.1 Identify Designated Approving Authority (DAA)/Accreditor
- Subtask–01.11.2 Identify Certification Authority/Certifier
- Subtask–01.11.3 Identify C&A and acquisition processes to be applied
- Subtask–01.11.4 Ensure Accréditor’s and Certifier’s concurrence in the information protection needs

Activity–02 Define System Security Requirements

Task–02.1 Develop system security context
- Subtask–02.1.1 Define system boundaries and interfaces with SE
- Subtask–02.1.2 Document security allocations to target system and external systems
- Subtask–02.1.3 Identify data flows between the target system and external systems and the protection needs associated with those flows

Task–02.2 Develop security Concept of Operations (CONOPS)

Task–02.3 Develop system security requirements baseline
- Subtask–02.3.1 Define system security requirements
- Subtask–02.3.2 Define system security modes of operation
- Subtask–02.3.3 Define system security performance measures

Task–02.4 Review design constraints

Task–02.5 Assess information protection effectiveness
- Subtask–02.5.1 Provide and present security context, security CONOPS, and system security requirements to the customer
- Subtask–02.5.2 Obtain concurrence from the customer in system security context, CONOPS, and requirements

Task–02.6 Support system C&A
- Subtask–02.6.1 Ensure Accreditor’s and Certifier’s concurrence in system security context, CONOPS, and requirements

Activity–03 Design System Security Architecture

Task–03.1 Perform functional analysis and allocation
- Subtask–03.1.1 Analyze candidate systems architectures
- Subtask–03.1.2 Allocate security services to architecture
- Subtask–03.1.3 Select mechanism types
- Subtask–03.1.4 Submit security architecture(s) for evaluation
- Subtask–03.1.5 Revise security architecture(s)
- Subtask–03.1.6 Select security architecture
Task–03.2  Assess information protection effectiveness
   Subtask–03.2.1  Ensure that the selected security mechanisms provide the required security services
   Subtask–03.2.2  Explain to the customer how the security architecture meets the security requirements
   Subtask–03.2.3  Generate risk projection
   Subtask–03.2.4  Obtain concurrence from the customer in the security architecture

Task–03.3  Support system C&A
   Subtask–03.3.1  Prepare and submit final architecture documentation for risk analysis
   Subtask–03.3.2  Coordinate results of the risk analysis with Accradiator and Certifier

Activity–04 Develop Detailed Security Design

Task–04.1  Ensure compliance with security architecture
Task–04.2  Perform trade-off studies
Task–04.3  Define system security design elements
   Subtask–04.3.1  Allocate security mechanisms to system security design elements
   Subtask–04.3.2  Identify candidate commercial off-the-shelf (COTS)/government off-the-shelf (GOTS) security products
   Subtask–04.3.3  Identify custom security products
   Subtask–04.3.4  Qualify element and system interfaces (internal and external)
   Subtask–04.3.5  Develop specifications

Task–04.4  Assess information protection effectiveness
   Subtask–04.4.1  Conduct design risk analysis
   Subtask–04.4.2  Ensure that the selected security design provides the required security services
   Subtask–04.4.3  Explain to the customer how the security design meets the security requirements
   Subtask–04.4.4  Explain to the customer, and document, any residual risks of the design
   Subtask–04.4.5  Obtain concurrence from the customer in the detailed security design
Task–04.5 Support system C&A

Subtask–04.5.1 Prepare and submit detailed design documentation for risk analysis

Subtask–04.5.2 Coordinate results of the risk analysis with Accreditor and Certifier

Activity–05 Implement System Security

Task–05.1 Support security implementation and integration

Subtask–05.1.1 Participate in implementation planning

Subtask–05.1.2 Verify interoperability of security tools and mechanisms

Subtask–05.1.3 Verify implementation against security design

Subtask–05.1.4 Verify that the security components have been evaluated against the selected evaluation criteria

Subtask–05.1.5 Assist in the integration of the components to ensure that their integration meets the system security specifications and does not alter the component specifications

Subtask–05.1.6 Assist in the configuration of the components to ensure that the security features are enabled and the security parameters are correctly set to provide the required security services

Subtask–05.1.7 Ensure that system and component configurations are documented and placed under configuration management

Task–05.2 Support test and evaluation

Subtask–05.2.1 Build test and evaluation strategy (includes demonstration, observation, analysis, and testing)

Subtask–05.2.2 Assess available test and evaluation data for applicability (e.g., CCEP, NIAP, internal)

Subtask–05.2.3 Support development of test and evaluation procedures

Subtask–05.2.4 Support test and evaluation activities

Task–05.3 Assess information protection effectiveness

Subtask–05.3.1 Monitor to ensure that the security design is implemented correctly

Subtask–05.3.2 Conduct or update risk analysis

Subtask–05.3.3 Define the risks and possible mission impacts and advise the customer and the customer’s Certifiers and Accreditors

Task–05.4 Support system C&A

Subtask–05.4.1 Ensure the completeness of the required C&A documentation with the customer and the customer’s Certifiers and Accreditors

Subtask–05.4.2 Provide documentation and analysis as required for the C&A process

Task–05.5 Support security training
Activity–06 Assess Information Protection Effectiveness

Assessing the effectiveness of the information protection occurs in conjunction with the activities of Discover Information Protection Needs, Define System Security Requirements, Design System Security Architecture, Develop Detailed Security Design, and Implement System Security. The Assess Information Protection Effectiveness task and subtasks are listed with the associated activities.

Activity–07 Plan Technical Effort

Planning the technical effort occurs throughout the ISSE process. The information systems security engineer must review each of the following areas to scope support to the customer in conjunction with the other activities. This set of tasks is recognized separately because it is applied similarly across all of the other activities, requires a unique skill set, and is likely to be assigned to senior-level personnel.

- Task–07.1 Estimate project scope
- Task–07.2 Identify resources and availability
- Task–07.3 Identify roles and responsibilities
- Task–07.4 Estimate project costs
- Task–07.5 Develop project schedule
- Task–07.6 Identify technical activities
- Task–07.7 Identify deliverables
- Task–07.8 Define management interfaces
- Task–07.9 Prepare technical management plan
- Task–07.10 Review project plan
- Task–07.11 Obtain customer agreement

Activity–08 Manage Technical Effort

Managing the technical effort occurs throughout the ISSE process. The information systems security engineer must review all technical activities and documentation to ensure quality in conjunction with the other activities. This set of tasks is recognized separately because it is applied similarly across all of the other activities, requires a unique skill set, and is likely to be assigned to senior-level personnel.

- Task–08.1 Direct technical effort
- Task–08.2 Track project resources
- Task–08.3 Track technical parameters
- Task–08.4 Monitor progress of technical activities
Task–08.5  Ensure quality of deliverables  
Task–08.6  Manage configuration elements  
Task–08.7  Review project performance  
Task–08.8  Report project status

DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAP) and Major Automated Information System (MAIS) Acquisition Programs, describes the Systems Engineering Process (SEP) as a comprehensive, iterative, and recursive problem-solving process, applied sequentially, top down. The following table summarizes the DoD 5000.2-R SEP and maps it to similar ISSE tasks.

<table>
<thead>
<tr>
<th>DoD 5000.2-R Systems Engineering Process</th>
<th>ISSE Process</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Systems Engineering Process Inputs</strong></td>
<td><strong>Discover Information Protection Needs</strong></td>
</tr>
<tr>
<td>• Customer needs/objectives/requirements</td>
<td>• Analyze organization’s mission</td>
</tr>
<tr>
<td>– Missions</td>
<td>• Determine relationship and importance of information to mission</td>
</tr>
<tr>
<td>– Measures of effectiveness</td>
<td>• Identify legal and regulatory requirements</td>
</tr>
<tr>
<td>– Environments</td>
<td>• Identify classes of threats</td>
</tr>
<tr>
<td>– Constraints</td>
<td>• Determine impacts</td>
</tr>
<tr>
<td>• Technology base</td>
<td>• Identify security services</td>
</tr>
<tr>
<td>• Output requirements from prior development effort</td>
<td>• Document the information protection needs</td>
</tr>
<tr>
<td>• Program decision requirements</td>
<td>• Document security management roles and responsibilities</td>
</tr>
<tr>
<td>• Requirements applied through specifications and standards</td>
<td>• Identify design constraints</td>
</tr>
<tr>
<td><strong>Requirements Analysis</strong></td>
<td><strong>Define System Security Requirements</strong></td>
</tr>
<tr>
<td>• Analyze missions and environments</td>
<td>• Develop system security context</td>
</tr>
<tr>
<td>• Identify functional requirements</td>
<td>– Define system boundaries and interfaces with SE</td>
</tr>
<tr>
<td>• Define or refine performance and design constraint requirements</td>
<td>– Document security allocations to target system and external systems</td>
</tr>
<tr>
<td></td>
<td>– Identify data flows between the target system and external systems and the protection needs associated with those flows</td>
</tr>
<tr>
<td></td>
<td>• Develop security CONOPS</td>
</tr>
<tr>
<td></td>
<td>• Develop system security requirements baseline</td>
</tr>
<tr>
<td></td>
<td>– Define system security requirements</td>
</tr>
<tr>
<td></td>
<td>– Define system security modes of operation</td>
</tr>
<tr>
<td></td>
<td>– Define system security performance measures</td>
</tr>
<tr>
<td></td>
<td>• Review design constraints</td>
</tr>
<tr>
<td>DoD 5000.2-R Systems Engineering Process</td>
<td>ISSE Process</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Functional Analysis/Allocation</strong></td>
<td><strong>Design System Security Architecture</strong></td>
</tr>
<tr>
<td>• Decompose to lower-level functions</td>
<td>• Analyze candidate systems architectures</td>
</tr>
<tr>
<td>• Allocate performance and other limiting requirements to all functional levels</td>
<td>• Allocate security services to architecture</td>
</tr>
<tr>
<td>• Define or refine functional interfaces (internal and external)</td>
<td>• Select mechanism types</td>
</tr>
<tr>
<td>• Define/refine/integrate functional architecture</td>
<td>• Submit security architecture(s) for evaluation</td>
</tr>
<tr>
<td><strong>Requirements Loop</strong></td>
<td><strong>Assess Information Protection Effectiveness</strong></td>
</tr>
<tr>
<td>• Reconsider Requirements Analysis to establish traceability of functions to requirements</td>
<td>• Provide/present documented information protection needs to the customer</td>
</tr>
<tr>
<td></td>
<td>• Identify the processes, information, users, threats, and security services that are important to the mission or business</td>
</tr>
<tr>
<td></td>
<td>• Explain security services, strengths, and priorities</td>
</tr>
<tr>
<td></td>
<td>• Provide/present security context, security CONOPS, and system security requirements to the customer</td>
</tr>
<tr>
<td></td>
<td>– Explain allocations to the target and external systems</td>
</tr>
<tr>
<td></td>
<td>– Ensure that the security mechanisms of the system meet the mission security needs</td>
</tr>
<tr>
<td></td>
<td>– Obtain concurrence the customer</td>
</tr>
<tr>
<td><strong>Synthesis</strong></td>
<td><strong>Support System C&amp;A</strong></td>
</tr>
<tr>
<td>• Transform architectures (functional to physical)</td>
<td>• Identify DAA/Accreditor</td>
</tr>
<tr>
<td>• Define alternative system concepts, configuration items, and system elements</td>
<td>• Identify Certification Authority/Certifier</td>
</tr>
<tr>
<td>• Select preferred product and process solutions</td>
<td>• Identify C&amp;A and acquisition processes to be applied</td>
</tr>
<tr>
<td>• Define or refine physical interfaces (internal and external)</td>
<td>• Ensure Accreditors and Certifiers concurrence</td>
</tr>
<tr>
<td></td>
<td>– System Security Context</td>
</tr>
<tr>
<td></td>
<td>– Security CONOPS</td>
</tr>
<tr>
<td></td>
<td>– System Security Requirements</td>
</tr>
<tr>
<td><strong>Develop Detailed Security Design</strong></td>
<td><strong>Support System C&amp;A</strong></td>
</tr>
<tr>
<td>• Ensure compliance with security architecture</td>
<td>• Identify DAA/Accreditor</td>
</tr>
<tr>
<td>• Perform trade-off studies</td>
<td>• Identify Certification Authority/Certifier</td>
</tr>
<tr>
<td>• Define system security design elements</td>
<td>• Identify C&amp;A and acquisition processes to be applied</td>
</tr>
<tr>
<td>– Allocate security mechanisms to system security design elements</td>
<td>• Ensure Accreditors and Certifiers concurrence</td>
</tr>
<tr>
<td>– Identify candidate COTS/GOTS security products</td>
<td>– System Security Context</td>
</tr>
<tr>
<td>– Identify custom security products</td>
<td>– Security CONOPS</td>
</tr>
<tr>
<td>– Qualify element and system interfaces (internal and external)</td>
<td>– System Security Requirements</td>
</tr>
<tr>
<td>• Develop specifications</td>
<td><strong>Support System C&amp;A</strong></td>
</tr>
<tr>
<td><strong>DoD 5000.2-R Systems Engineering Process</strong></td>
<td><strong>ISSE Process</strong></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Design Loop</strong></td>
<td><strong>Assess Information Protection Effectiveness</strong></td>
</tr>
<tr>
<td>– Revisiting the functional architecture to verify that the physical design synthesized the required functions at the required level of performance</td>
<td>– Conduct design risk analysis</td>
</tr>
<tr>
<td></td>
<td>– Ensure that the selected security design provides the required security services</td>
</tr>
<tr>
<td></td>
<td>– Explain to the customer how the security design meets the security requirements</td>
</tr>
<tr>
<td></td>
<td>– Explain to the customer, and document, any residual risks of the design</td>
</tr>
<tr>
<td></td>
<td>– Obtain concurrence from the customer in the detailed security design</td>
</tr>
<tr>
<td><strong>Support System C&amp;A</strong></td>
<td><strong>Implement System Security</strong></td>
</tr>
<tr>
<td>– Prepare and submit detailed design documentation for risk analysis</td>
<td>– Support security implementation and integration</td>
</tr>
<tr>
<td></td>
<td>– Participate in implementation planning</td>
</tr>
<tr>
<td></td>
<td>– Verify interoperability of security tools and mechanisms</td>
</tr>
<tr>
<td></td>
<td>– Verify implementation against security design</td>
</tr>
<tr>
<td></td>
<td>– Verify that the security components have been evaluated against the selected evaluation criteria (CCEP, NIAP, FIPS, or other NSA and NIST evaluation criteria)</td>
</tr>
<tr>
<td></td>
<td>– Assist in the integration of the components to ensure that their integration meets the system security specifications and does not alter the component specifications</td>
</tr>
<tr>
<td></td>
<td>– Assist in the configuration of the components to ensure that the security features are enabled and the security parameters are correctly set to provide the required security services</td>
</tr>
<tr>
<td></td>
<td>– Support test and evaluation</td>
</tr>
<tr>
<td>– Support test and evaluation (includes demonstration, observation, analysis, and testing)</td>
<td>– Build test and evaluation strategy (includes demonstration, observation, analysis, and testing)</td>
</tr>
<tr>
<td>– Assess available test and evaluation data for applicability (e.g., CCEP, NIAP, internal)</td>
<td>– Assess available test and evaluation data for applicability (e.g., CCEP, NIAP, internal)</td>
</tr>
<tr>
<td>– Support development of test and evaluation procedures</td>
<td>– Support development of test and evaluation procedures</td>
</tr>
<tr>
<td>– Support test and evaluation activities</td>
<td>– Support test and evaluation activities</td>
</tr>
</tbody>
</table>

**Process Output**

- Development Level Dependent
  - Decision database
  - System and configuration item architecture
  - Specifications and baselines

**Implement System Security**

- Support test and evaluation
  - Build test and evaluation strategy (includes demonstration, observation, analysis, and testing)
DoD 5000.2-R Systems Engineering Process | ISSE Process

| Verification | | Assess Information Protection Effectiveness |
| Comparison of the solution to the requirements | | Monitor to ensure that the security design is implemented correctly |
| | | Conduct or update risk analysis |
| | | Define the risks and possible mission impacts and advise the customer and the customer’s Certifiers and Accreditors |
| | | Support System C&A |
| | | Ensure the completeness of the required C&A documentation with the customer and the customer’s Certifiers and Accreditors |
| | | Provide documentation and analysis as required for the C&A process |


<table>
<thead>
<tr>
<th>IEEE Std 1220-1998 Systems Engineering Process</th>
<th>ISSE Process</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirements Analysis</strong></td>
<td><strong>Discover Information Protection Needs</strong></td>
</tr>
<tr>
<td>Define customer expectations</td>
<td>Analyze organization’s mission</td>
</tr>
<tr>
<td>Define project and enterprise constraints</td>
<td>Determine relationship and importance of information to mission</td>
</tr>
<tr>
<td>Define external constraints</td>
<td>Identify legal and regulatory requirements</td>
</tr>
<tr>
<td>Define operational scenarios</td>
<td>Identify classes of threats</td>
</tr>
<tr>
<td>Define measures of effectiveness</td>
<td>Determine impacts</td>
</tr>
<tr>
<td>Define system boundaries</td>
<td>Identify security services</td>
</tr>
<tr>
<td>Define interfaces</td>
<td></td>
</tr>
<tr>
<td>Define utilization environments</td>
<td>Document the information protection needs</td>
</tr>
<tr>
<td>Define life-cycle process concepts</td>
<td>Document security management roles and responsibilities</td>
</tr>
<tr>
<td>Define functional requirements</td>
<td>Identify design constraints</td>
</tr>
</tbody>
</table>
### IEEE Std 1220-1998 Systems Engineering Process

- Define performance requirements
- Define modes of operations
- Define technical performance measures
- Define design characteristics
- Define human factors
- Establish requirements baseline

### ISSE Process

#### Define System Security Requirements

- Develop system security context
  - Define system boundaries and interfaces with SE
  - Document security allocations to target system and external systems
  - Identify data flows between the target system and external systems and protection needs associated with those flows
- Develop security CONOPS
- Develop system security requirements baseline
  - Define system security requirements
  - Define system security modes of operation
  - Define system security performance measures
  - Review design constraints

#### Requirements Verification and Validation

- Compare to customer expectations
- Compare to enterprise and project constraints
- Compare to external constraints
- Identify variances and conflicts
- Establish validated requirements baseline

#### Assess Information Protection Effectiveness

- Provide and present documented information protection needs to the customer
- Explain security services, strengths, and priorities
- Provide and present security context, security CONOPS, and system security requirements to the customer
- Obtain concurrence from the customer

#### Support System C&A

- Identify DAA/Accreditor
- Identify Certification Authority/Certifier
- Identify C&A and acquisition processes to be applied
- Ensure Accrder’s and Certifier’s concurrence
  - System security context
  - Security CONOPS
  - System security requirements
| **IEEE Std 1220-1998**  
| **Systems Engineering Process** | **ISSE Process**  
| **Functional Analysis** | **Design System Security Architecture**  
| • Functional context analysis  
  – Analyze functional behaviors  
  – Define functional interfaces  
  – Allocate performance requirements  
| • Functional decomposition  
  – Define subfunctions  
  – Define subfunction states and modes  
  – Define functional timelines  
  – Define data and control flows  
  – Define functional failure modes and effects  
  – Define safety monitoring functions  
  • Establish functional architecture | • Perform functional analysis and allocation  
  – Analyze candidate systems architectures  
  – Allocate security services to architecture  
  – Select mechanism types  
  – Submit security architecture(s) for evaluation  
  – Revise security architecture(s)  
  – Select security architecture  
| **Functional Verification** | **Assess Information Protection Effectiveness**  
| • Define verification procedures  
| • Conduct verification evaluation  
  – Verify architecture completeness  
  – Verify functional and performance measures  
  – Verify satisfaction of constraints  
| • Identify variances and conflicts  
| • Verified functional architecture | • Ensure that the selected security mechanisms provide the required security services  
| • Explain to the customer how the security architecture meets the security requirements  
| • Perform risk analysis  
| • Obtain concurrence from the customer in the security architecture  
  **Support System C&A**  
| • Prepare and submit final architecture documentation for risk analysis  
| • Coordinate results with Accredit and Certifier  
| **Synthesis** | **Develop Detailed Security Design**  
| • Group and allocate functions  
| • Identify design solution alternatives  
| • Assess safety and environmental hazards  
| • Assess life-cycle quality factors  
| • Assess technology requirements  
| • Define design and performance characteristics  
| • Define physical interfaces  
| • Identify standardization opportunities  
| • Identify off-the-shelf availability  
| • Identify make or buy alternatives  
| • Develop models and fabricate prototypes  
| • Assess failure modes, effects, and criticality  
| • Assess testability needs  
| • Assess design capacity to evolve  
| • Final design  
| • Initiate evolutionary development  
| • Produce integrated data package  
| • Establish design architecture  
| **Develop Detailed Security Design** |  
| • Ensure compliance with security architecture  
| • Perform trade-off studies  
| • Define system security design elements  
  – Allocate security mechanisms to system security design elements  
  – Identify candidate COTS/GOTS security products  
  – Identify custom security products  
  – Qualify element and system interfaces (internal and external)  
| • Develop specifications |
## Design Verification

- Select verification approach
  - Define inspection, analysis, demonstration, or test requirements
  - Define verification procedures
  - Establish verification environment
  - Conduct verification evaluation
  - Verify architecture completeness
  - Verify functional and performance measures
  - Verify satisfaction of constraints
- Identify variance and conflicts
- Verified design architecture
- Verified design architectures of life-cycle processes
- Verified system architecture
- Establish specifications and configuration baselines
- Develop product breakdown structures

## Assess Information Protection Effectiveness

- Conduct design risk analysis
- Ensure that the selected security design provides the required security services
- Explain to the customer how the security design meets the security requirements
- Explain to the customer, and document, any residual risks of the design
- Obtain concurrence from the customer in the detailed security design

### Support System C&A

- Prepare and submit detailed design documentation for risk analysis
- Coordinate results with Accreditor and Certifier

## System Analysis

- Assess requirement conflicts
- Assess functional alternatives
- Assess design alternatives
- Identify risk factors
- Define trade study scope
  - Select methodology and success criteria
  - Identify alternatives
  - Establish trade study environment
- Conduct trade study
- Analyze life-cycle costs
- Analyze system and cost-effectiveness
- Analyze environmental impacts
- Quantify risk factors
- Select risk handling options
- Select alternative recommendations
- Design effectiveness assessment
- Trade-offs and impacts

* System analysis is part of the risk assessment process, which also is part of the analysis performed in each activity. Therefore, the specific tasks are cited in the relative SEP subprocesses.
<table>
<thead>
<tr>
<th>IEEE Std 1220-1998 Systems Engineering Process</th>
<th>ISSE Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The IEEE standard defines systems engineering as the total development effort and does not address implementation that would be addressed by manufacturing and test processes.</td>
<td><strong>Implement System Security</strong></td>
</tr>
<tr>
<td></td>
<td>• Support security implementation and integration</td>
</tr>
<tr>
<td></td>
<td>– Participate in implementation planning</td>
</tr>
<tr>
<td></td>
<td>– Verify interoperability of security tools and mechanisms</td>
</tr>
<tr>
<td></td>
<td>– Verify implementation against security design</td>
</tr>
<tr>
<td></td>
<td>– Verify that the security components have been evaluated against the selected evaluation criteria (CCEP, NIAP, FIPS, or other NSA and NIST evaluation criteria)</td>
</tr>
<tr>
<td></td>
<td>– Assist in the integration of the components to ensure that their integration meets the system security specifications and does not alter the component specifications</td>
</tr>
<tr>
<td></td>
<td>– Assist in the configuration of the components to ensure that the security features are enabled and the security parameters are correctly set to provide the required security services</td>
</tr>
<tr>
<td></td>
<td>• Support test and evaluation</td>
</tr>
<tr>
<td></td>
<td>– Build test and evaluation strategy (includes demonstration, observation, analysis, and testing)</td>
</tr>
<tr>
<td></td>
<td>– Assess available test and evaluation data for applicability (e.g., CCEP, NIAP, internal)</td>
</tr>
<tr>
<td></td>
<td>– Support development of test and evaluation procedures</td>
</tr>
<tr>
<td></td>
<td>– Support test and evaluation activities</td>
</tr>
<tr>
<td></td>
<td>• Support security training</td>
</tr>
<tr>
<td></td>
<td><strong>Assess Information Protection Effectiveness</strong></td>
</tr>
<tr>
<td></td>
<td>• Monitor to ensure that the security design is implemented correctly</td>
</tr>
<tr>
<td></td>
<td>• Conduct or update risk analysis</td>
</tr>
<tr>
<td></td>
<td>• Define the risks and possible mission impacts and advise the customer and the customer’s Certifiers and Accreditors</td>
</tr>
<tr>
<td></td>
<td><strong>Support C&amp;A</strong></td>
</tr>
<tr>
<td></td>
<td>• Ensure the completeness of the required C&amp;A documentation with the customer and the customer’s Certifiers and Accreditors</td>
</tr>
<tr>
<td></td>
<td>• Provide documentation and analysis as required for the C&amp;A process</td>
</tr>
<tr>
<td>Control</td>
<td>ISSE Process</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| • Technical management  
  – Data management  
  – Configuration management  
  – Interface management  
  – Risk management  
  – Performance-based progress measurements  
• Track system analysis, and verification and test data  
• Track requirements and design changes  
• Track performance against project plans  
• Track performance against technical plans  
• Track product and process metrics  
• Update specifications and configuration baselines  
• Update requirement views and architectures  
• Update engineering plans  
• Update technical plans  
• Integrated database | | Plan Technical Effort |  
• Estimate project scope  
• Identify resources and availability  
• Identify roles and responsibilities  
• Estimate project costs  
• Develop project schedule  
• Identify technical activities  
• Identify deliverables  
• Define management interfaces  
• Prepare technical management plan  
• Review project plan  
• Obtain customer agreement  
  **Manage Technical Effort**  
• Direct technical effort  
• Track project resources  
• Track technical parameters  
• Monitor progress of technical activities  
• Ensure quality of deliverables  
• Manage configuration elements  
• Review project performance  
• Report project status |