Science Applications International Corporation

Process Capability for Information Assurance: Security Engineering Practices for Better Bottom-Line Results

NEbraska CERT Conference 2003

Computer Security and Information Assurance

Matt O'Brien, CISSP
obrienma@saic.com

5 August 2003

SAIC®
An Employee-Owned Company

Objectives

- Importance of Process Capability for Information Assurance
- Overview of the Systems Security Engineering CMM
  - Not a substitute for reading Model Description Document
- Essential Elements of Security Engineering Process
  - Proposal that complements system development lifecycle
- Examples of Security Engineering Practices
  - Example implementations

Process Capability: The Investing Analogy

- Process capability is analogous to a Buy-and-Hold investment strategy
  - Not a “get rich quick” scheme (process capability built over time)
  - Stock selection based upon analysis (rigor of engineering discipline)
  - Portfolio management to measure performance (performance parameters enable “best of breed” determination and on-going enhancements)

- Success is dependent upon constancy
  - No “timing the market” (threat is not predictable)

Process Capability: The Argument

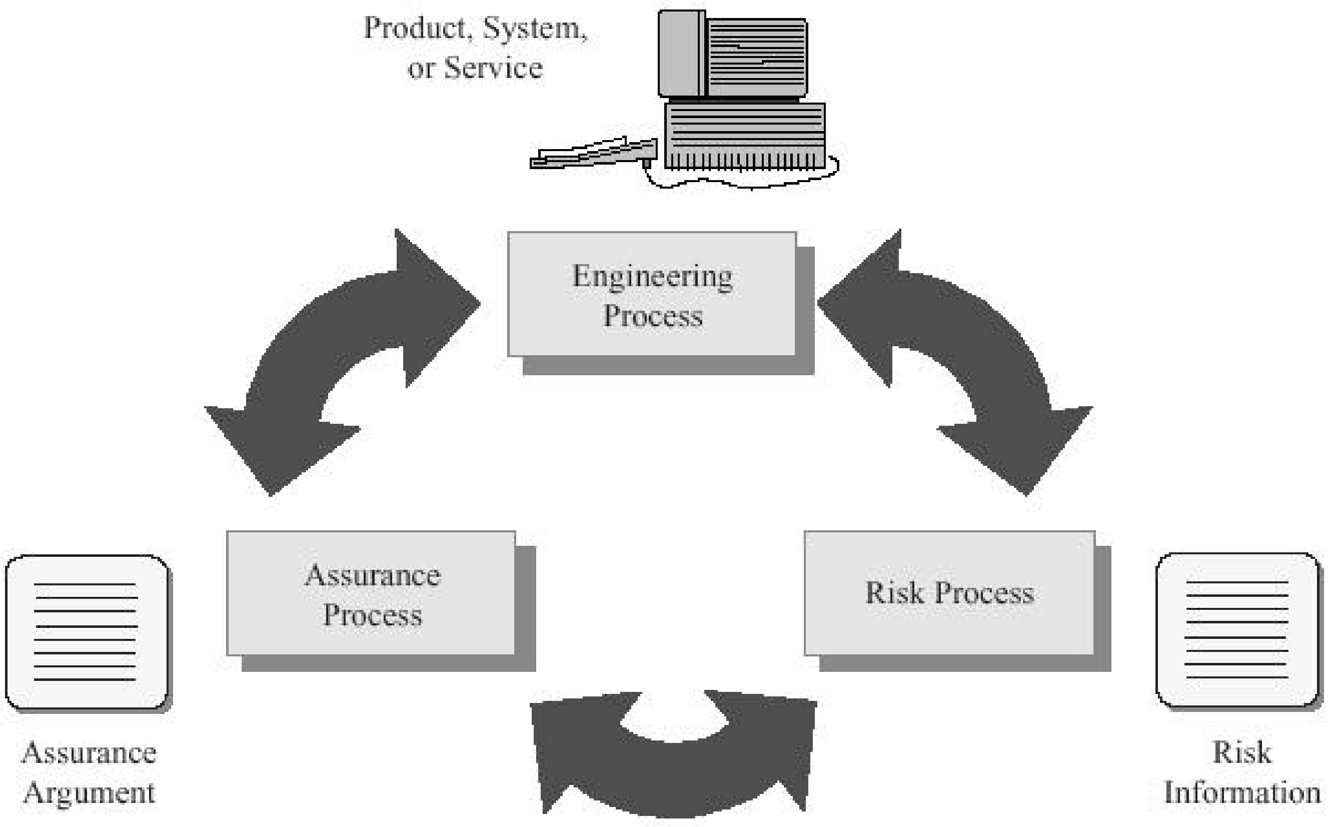
- Assertions
  - Process is an essential element of the assurance argument (more important than product)
  - Process must be organized around specific activities (e.g., system development lifecycle)
  - Process must have measures of evaluation (e.g., key performance parameters)
- Desired Outcome
  - Process with measurable outputs that enables “best of breed” to be identified and widely adopted

Process Capability: The Imperative

- A single vulnerability can compromise a system as thoroughly as if it had no benefit of security engineering
- Process capability is a defense-in-depth mechanism to combat this ubiquitous threat
  - Prevent ("Protect")
  - Identify ("Detect")
  - Remedy ("React")
- Process capability determines and sustains the robustness of an enterprise's security posture
  - Assessment-type activities (e.g., penetration testing, security test and evaluation) are only point-in-time snapshots

SSE-CMM Overview

- SSE-CMM Security Engineering Process Elements



Model Architecture

- Security Engineering Base Practices
  - Represent best practices
  - Iterative, and not ordered by lifecycle phase
- Project and Organizational Base Practices
  - Adapted from Systems Engineering CMM
  - Reference materials for interpreting generic practices
- Capability Levels (Generic Practices)
  - Management, measurement and institutionalization aspects
  - Assess and improve organization’s process capability
  - Rank ordered according to maturity

Security Engineering Base Practices

- Base practices are grouped into 11 process areas:
  - PA01 Administer Security Controls
  - PA02 Assess Impact
  - PA03 Assess Security Risk
  - PA04 Assess Threat
  - PA05 Assess Vulnerability
  - PA06 Build Assurance Argument
  - PA07 Coordinate Security
  - PA08 Monitor Security Posture
  - PA09 Provide Security Input
  - PA10 Specify Security Needs
  - PA11 Verify and Validate Security

Project and Organizational Base Practices

- Base practices are grouped into 11 process areas:
  - PA12 Ensure Quality
  - PA13 Manage Configuration
  - PA14 Manage Project Risk
  - PA15 Monitor and Control Technical Effort
  - PA16 Plan Technical Effort
  - PA17 Define Organization’s Systems Eng Process
  - PA18 Improve Organization’s Sys Eng Process
  - PA19 Manage Product Line Evolution
  - PA20 Manage Sys Eng Support Environment
  - PA21 Provide Ongoing Skills and Knowledge
  - PA22 Coordinate with Suppliers

Security Engineering Base Practices Taxonomy

PA01 – Process Area Title (in verb-noun form)

Summary Description – An overview of the process area

Goals – A list indicating the desired results of implementing this process area

Base Practices List – A list showing the number and name of each base practice

Process Area Notes – Any other notes about this process area

BP.01.01 – Base Practice Title (in verb-noun form)

Descriptive Name – A sentence describing the base practice

Description – An overview of this base practice

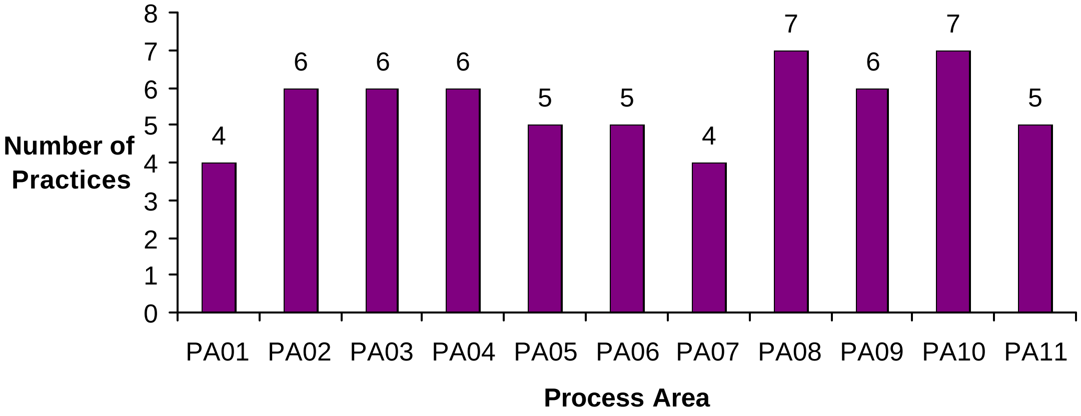
Example Work Products – A list of examples illustrating some possible output

Notes – Any other notes about this base practice

BP.01.02…

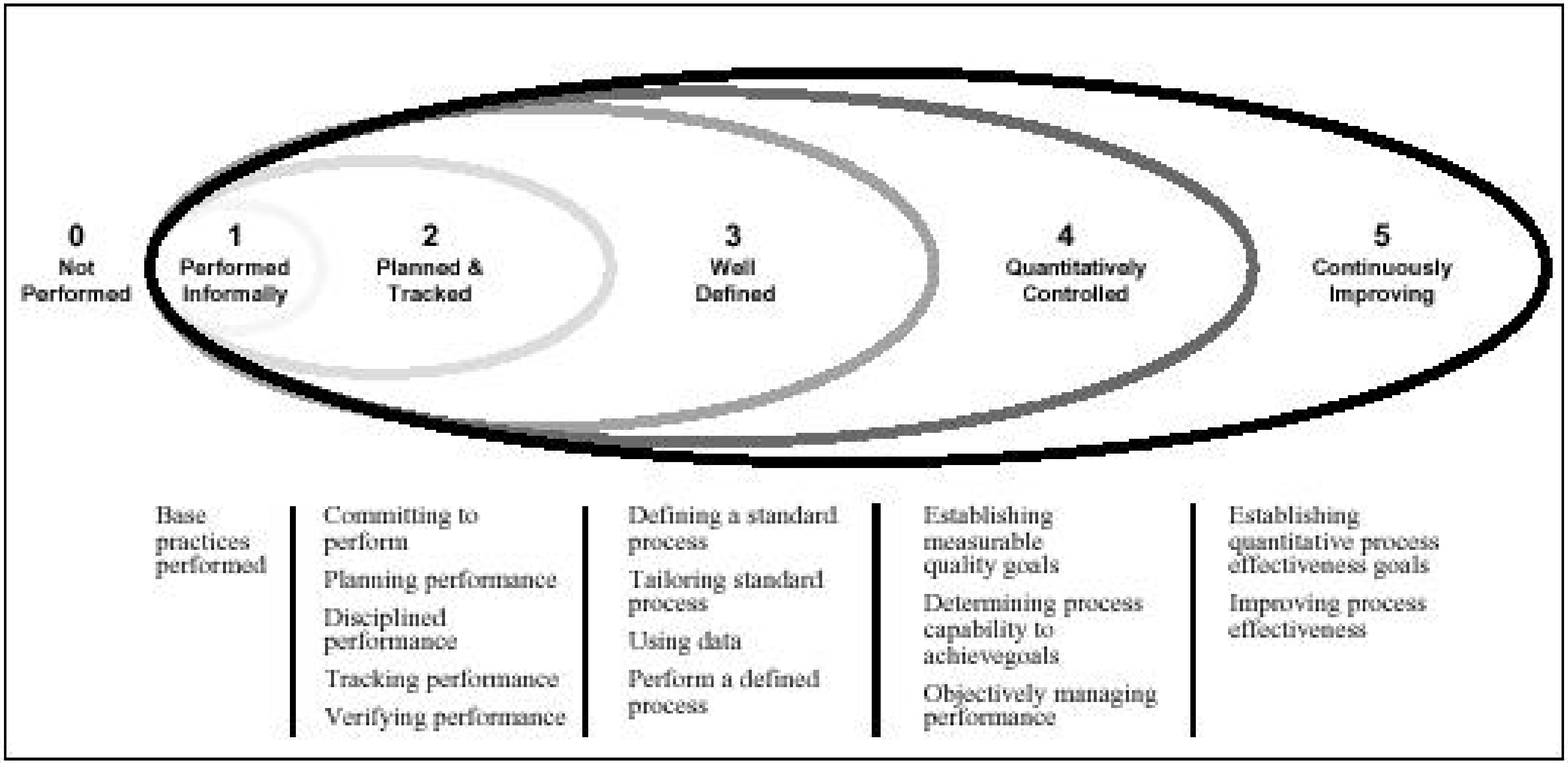
BP.01.03…

Security Engineering Base Practices



Capability Levels

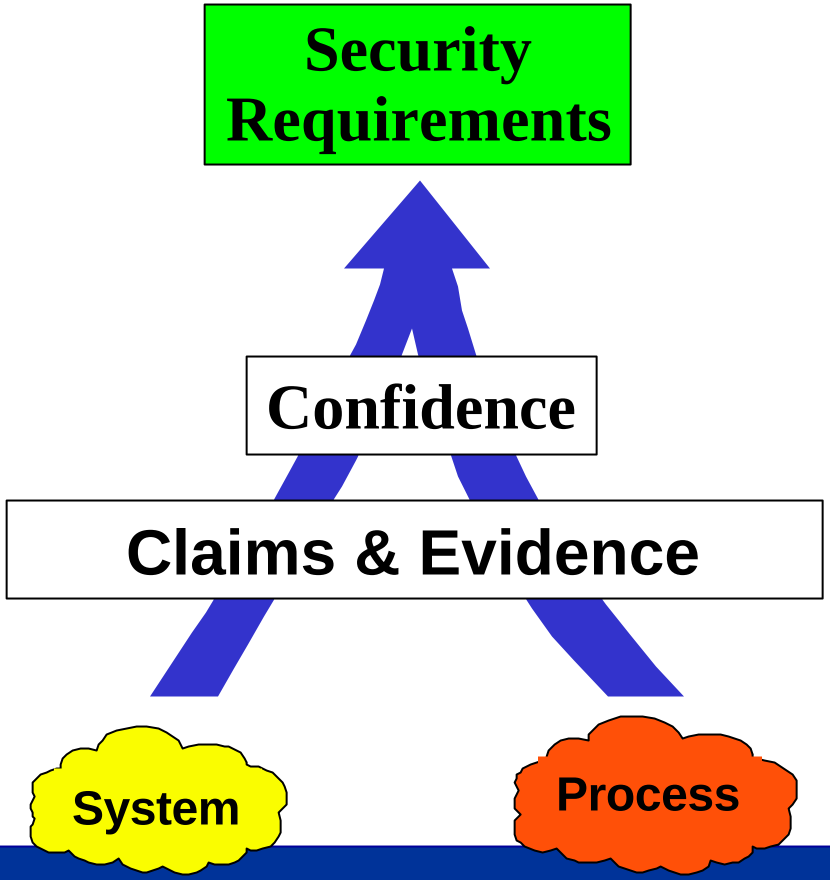
- **Represent the maturity of the security engineering organization**



Base practices performed	Committing to perform Planning performance Disciplined performance Tracking performance Verifying performance	Defining a standard process Tailoring standard process Using data Perform a defined process	Establishing measurable quality goals Determining process capability to achievegoals Objectively managing performance	Establishing quantitative process effectiveness goals Improving process effectiveness

Capability-Based Assurance

- Assurance mechanisms provide confidence that security requirements have been satisfied

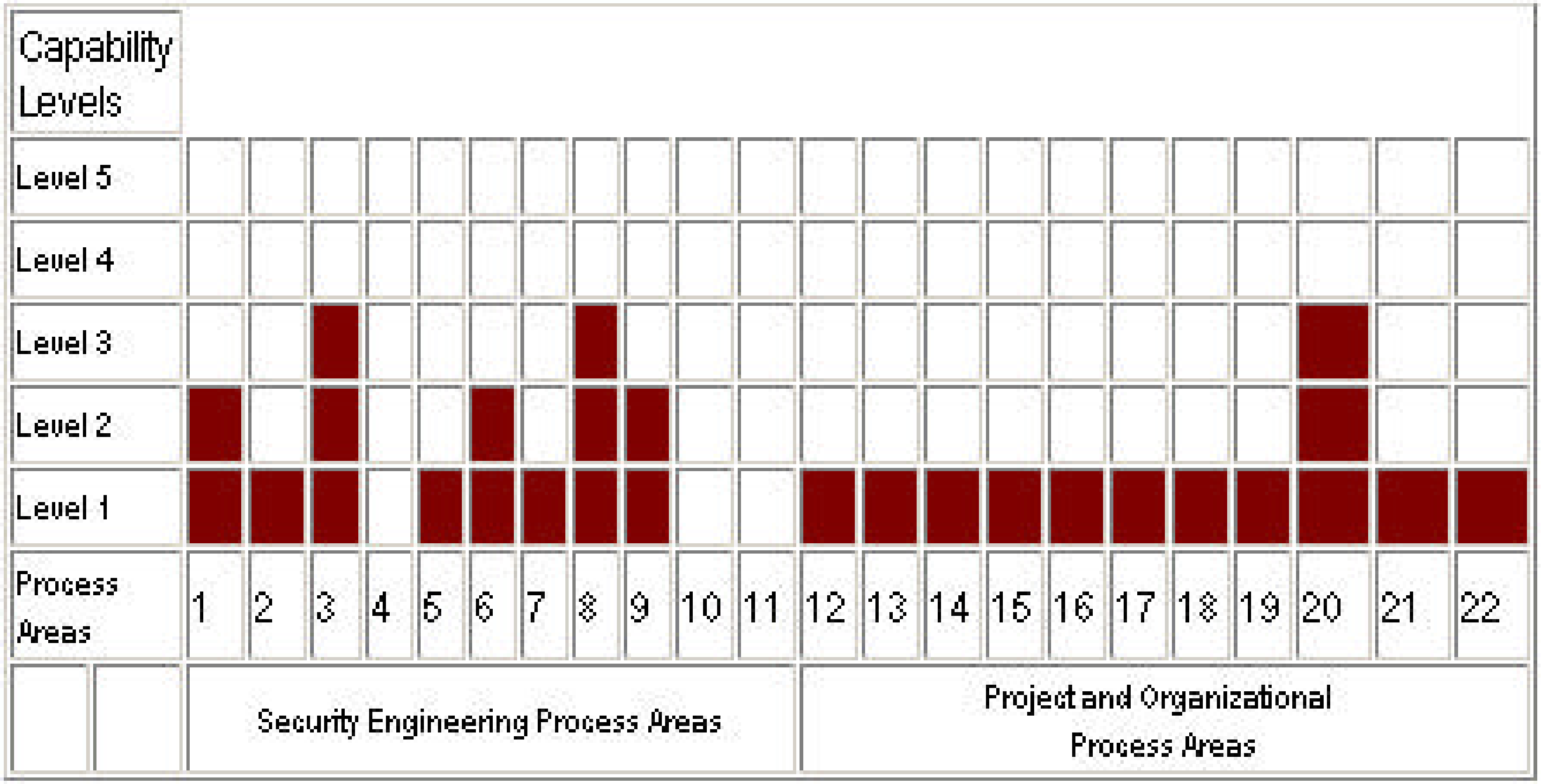


Security Requirements

Confidence

Claims & Evidence

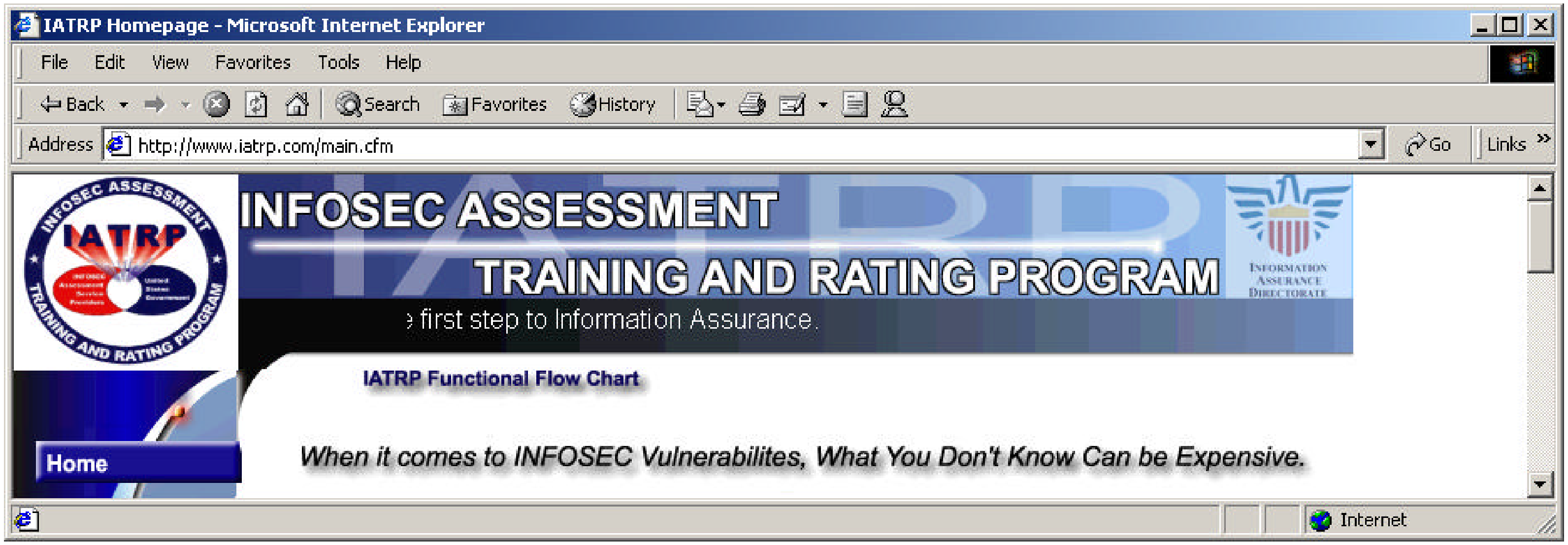
Determining Organizational Capability



Capability Levels																						
Level 5																						
Level 4																						
Level 3			■					■												■		
Level 2	■		■			■		■	■											■		
Level 1	■	■	■		■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■
Process Areas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
	Security Engineering Process Areas											Project and Organizational Process Areas										

Process Capability Evaluations

- The National Security Agency has developed an INFOSEC Assessment Training and Rating Program
  - INFOSEC Assessment CMM based upon SSE-CMM
  - Provides standard evaluation of vendors' INFOSEC vulnerability assessment capabilities
  - 7 firms have had appraisal


IATRP Homepage - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Links
INFOSEC ASSESSMENT TRAINING AND RATING PROGRAM
IATRP
Information Assurance Directorate
Home
Internet

http://www.iatrp.com/main.cfm

INFOSEC ASSESSMENT

TRAINING AND RATING PROGRAM

e first step to Information Assurance.

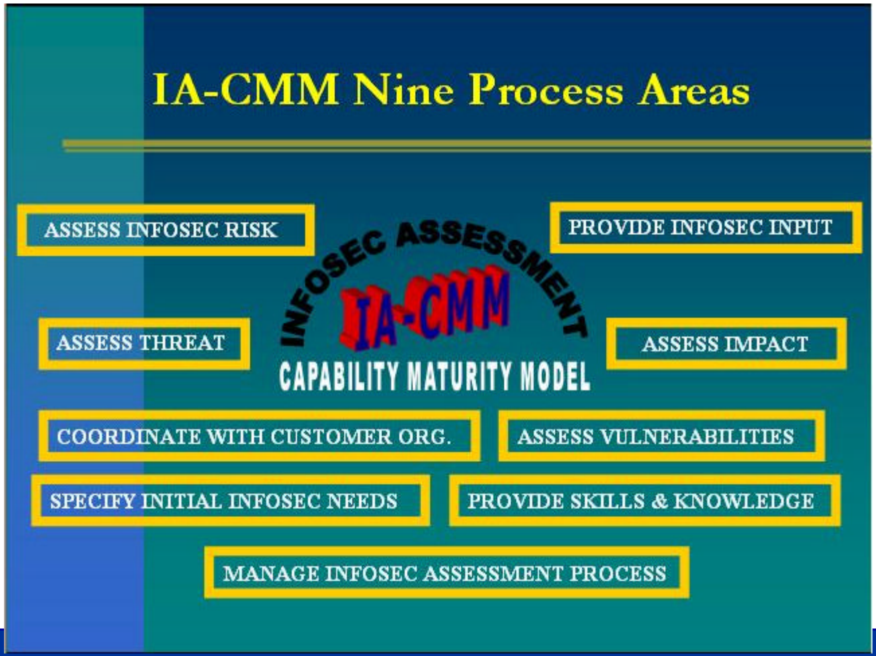
IATRP Functional Flow Chart

When it comes to INFOSEC Vulnerabilites, What You Don't Know Can be Expensive.

http://www.iatrp.com/main.cfm

Process Capability Evaluations (2)

- IA-CMM has 9 process areas
  - Focuses on the processes that produce products (e.g., identified vulnerabilities, countermeasures and threats)
  - Uses standard CMM capability levels to rate maturity



IA-CMM Nine Process Areas

- ASSESS INFOSEC RISK
- PROVIDE INFOSEC INPUT
- ASSESS THREAT
- ASSESS IMPACT
- COORDINATE WITH CUSTOMER ORG.
- ASSESS VULNERABILITIES
- SPECIFY INITIAL INFOSEC NEEDS
- PROVIDE SKILLS & KNOWLEDGE
- MANAGE INFOSEC ASSESSMENT PROCESS

Limitations of the SSE-CMM for Process Capability

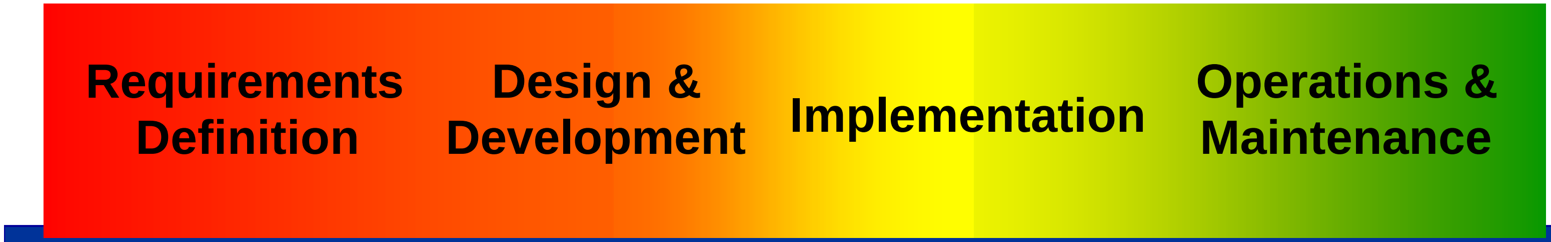
- **Model is not prescriptive**
  - **Emphasizes "what to do", not "how to do"**
  - **Specifically avoids defining sequence for activities**
- **Model definition of risk is simplistic**
  - **Threat → Vulnerability → Impact**
- **Model does not appear to be widely used**
  - **A de facto standard would promote common terminology, definition of problem space/solutions**

A Significant Advancement for Process Capability

- Information Assurance Technical Framework Forum
  - NSA-sponsored IATF document (Release 3.1, Sep 2002)
    - ➢ Information Systems Security Engineering process consisting of 6 activities
      - ✓ Discover Information Protection Needs
      - ✓ Define System Security Requirements
      - ✓ Define System Security Architecture
      - ✓ Develop Detailed Security Design
      - ✓ Implement System Security
      - ✓ Assess Information Protection Effectiveness
    - ➢ Master Activity and Task List to decomposes ISSE process activities into tasks and subtasks
      - ✓ Two program management activities are included
    - ➢ ISSE Process is related to Systems Engineering Process
    - ➢ ISSE Process is related to DoD's certification and accreditation process (DITSCAP)

Essential Elements of Security Engineering Process

- Proposed 10 elements:
  - Security Policy and Requirements
  - Certification and Accreditation Plan
  - Security Architecture and Implementation Plan
  - Security Configuration Baseline Development
  - Security Documentation
  - Security Test and Evaluation
  - Vulnerability Identification and Patch Process
  - Host and Network Intrusion Detection Plan
  - Security Monitoring
  - Periodic Evaluation of Countermeasures



System Development Lifecycle

Security Policy and Requirements

- Assigns roles and responsibilities
  - Who’s in charge?
  - Organizational structure to accomplish policy
- Defines what is to be protected (and possibly how)
  - Scope and applicability
  - Exceptions and adjudication
- Defines reporting requirements to evaluate progress
  - Frequency
  - Success criteria

“Measurement Improves Performance”

Requirements Definition

Security Policy and Requirements (2)

- **Policy can be at organizational and/or system level**
  - **Example: DoD's Information Assurance Policy (DoDD 8500.1: http://www.dtic.mil/whs/directives/)**
- **Requirements, at system level, support assurance argument for system certification and accreditation**
  - **System requirements**
  - **Process requirements**
- **Standard requirements promote understanding**
  - **Example: Common Criteria requirements catalog ***
    - **Protection Profiles specify product-based requirements**
      - ✓ **Example: Protection Profiles at http://www.radium.ncsc.mil/tpep/library/protection_profiles/**

Requirements Definition

* http://www.commoncriteria.org

Certification and Accreditation Plan

- Certification and accreditation is a risk management process for approval and operation of a system
  - Defines activities and milestones for security engineering process to support accreditation
- DoD process ("DITSCAP") is formally defined at policy and implementation levels
  - Policy: DoDI 5200.40 *
  - Implementation: DoD 8510.1-M *
- Assessment of risk, and assumption of residual risk, remain subjective decisions within DoD
  - Success criteria/timelines should be explicitly defined
  - Implication for community risk

Requirements Definition

* http://www.dtic.mil/whs/directives/

Certification and Accreditation Plan (2)

Phase I	Phase II	Phase III	Phase IV	
Definition	**Verification**	**Validation**	**Post-Accreditation**	**DITSCAP Phases**
Analyze or Develop Mission Needs Develop SSAA Registration Negotiation	Analyze - System Architecture - Software Design - Network Connection - Product Integrity - Life Cycle Management Assess Vulnerability Assess Analysis Results	Certification - ST&E - Penetration Test - TEMPEST & Red/Black - COMSEC Compliance - Sys Mgmt Analysis - Site Accred. Survey - Contingency Plan - Risk Management Certifier's Recommend. Accreditation Decision	**Accreditation Decision** Maintain Accreditation Ongoing Maintenance System Operation Change Management Compliance Validation	
Requirements Definition	**Design & Development**	**Implementation**	**Operations & Maintenance**	**System Development Lifecycle**

Requirements Definition

Security Architecture and Implementation Plan

- Security architecture is dependent upon system arch.
  - Functional architecture may initially suffice
  - Ultimately technical architecture is needed
  - Functional decomposition to define technical architecture
- Security architecture may be dictated by regulatory environment/system type
  - Health care systems: Health Insurance Portability and Accountability Act security provisions
  - DoD classified system: DoDI 8500.2, IA Implementation
  - Federal IA-related products: NSTISSP No. 11 *
- Operating environment/characteristics
  - Information Assurance Technical Framework (http://www.iatf.net/framework_docs/version-3_1/index.cfm)

Requirements Definition

* http://niap.nist.gov/niap/library/nstissp_11.pdf

Security Architecture and Implementation Plan (2)

- System connections/interfaces and data flows
  - Reliance upon external systems (e.g., PKI)
- Security architecture requirements traceability
  - Technical requirements
    - ➢ Configuration (e.g., OS, application server)
      - ✓ NSA security recommendation guides *
    - ➢ Security products/tools
  - Process requirements
    - Developer/IAO (ISSO)/user
  - Documentation requirements
    - Developer guidance, IAO (ISSO)/user documents
- System security roles and responsibilities
  - Security monitoring: IAO (ISSO)

Requirements Definition

* http://www.nsa.gov/snac/index.html

Security Configuration Baseline Development

- Informally described as the “lockdown”
- Hardware components
  - Security products (e.g., firewalls)
  - Security appliances (e.g, VPN)
- Software components
  - Security tools (e.g., anti-virus)
- Software configuration
  - Security and non-security related (OS and applications)

Design & Development

Security Documentation

- Product of integration testing of security lockdown
- Lockdown invariably involves functional trade-offs
- Security configuration baseline document
  - Captures functional trade-offs/waivers
  - Details hardware/software/configuration settings
    - Often several hundred pages
  - CM, version-controlled document
- IAO (ISSO)/user documentation
  - Examples: Security CONOPS/TFM, SFUG, training docs

Implementation

Security Test and Evaluation

- Configuration management is prerequisite of ST&E and maintenance of system security posture
- Functional testing of security services
  - Prior agreement regarding success criteria (e.g., no priority 1 findings for IATO/ATO) and timelines
  - Traceability to requirements
- Execution of back-up and recovery procedures
  - Off-site storage of back-up media
- Review of security documentation
- Evaluation of residual risk

Implementation

Security Test and Evaluation (2)

Priority	IEEE Std 1044	COE Priority Logic	Security Priority Logic:
1	a) Prevent the accomplishment of an essential capability. b) Jeopardize safety, security, or other requirement designated “critical”.	Unable to perform required operational capability (vital software core dumps), Y2K execution issue that requires more than exiting and restarting application.	a) Exploit affects a large number of hosts in their standard configuration or the underlying infrastructure. b) Exploit is executable from a remote location. c) Exploit has significant impact (e.g., denial of service, root compromise). d) Exploit code is available and currently being used to exploit systems.
2	a) Adversely affect the accomplishment of an essential capability and no work-around solution is known. b) Adversely affect technical, cost, schedule risks to the project or to the life cycle support of the system, and no work-around solution is known.	Required operational capability is adversely affected and no work-around is available (vital software doesn’t work and there is no work-around); Y2K display issue or execution issue that can be fixed by exiting and restarting application.	a) Exploit affects a large number of hosts in their standard configuration or the underlying infrastructure. b) Exploit has significant impact (e.g., denial of service, root compromise).
3	a) Adversely affect the accomplishment of an essential capability but a work-around solution is known. b) Adversely affect technical, cost, schedule risks to the project or to the life cycle support of the system, but a work-around solution is known.	Required operational capability is adversely affected and work-around available (vital software doesn’t work and there is work-around); KPC test procedure issue that reveals a major problem in operational software, support capability and there is no work-around available (check compliance).	a) Exploit affects a large number of hosts in their standard configuration or the underlying infrastructure. b) Exploit adversely affects the accomplishment of an essential capability (e.g., unauthorized ability to modify data).
4	a) Result in user/operator inconvenience or annoyance but does not affect a required operational or mission-essential capability. b) Result in inconvenience or annoyance for development or maintenance personnel but does not prevent the accomplishment of the responsibilities of those personnel.	Operator or user inconvenience; compliance and documentation issues that affect users or administrators; KPC test procedure issue that does not reveal a major problem in operational software, support capability and there is work-around (check compliance)	N/A
5	Any other effect.	Compliance and documentation issues that do not affect users or administrators	N/A

Implementation

Vulnerabilities Are Prioritized According to System Impact

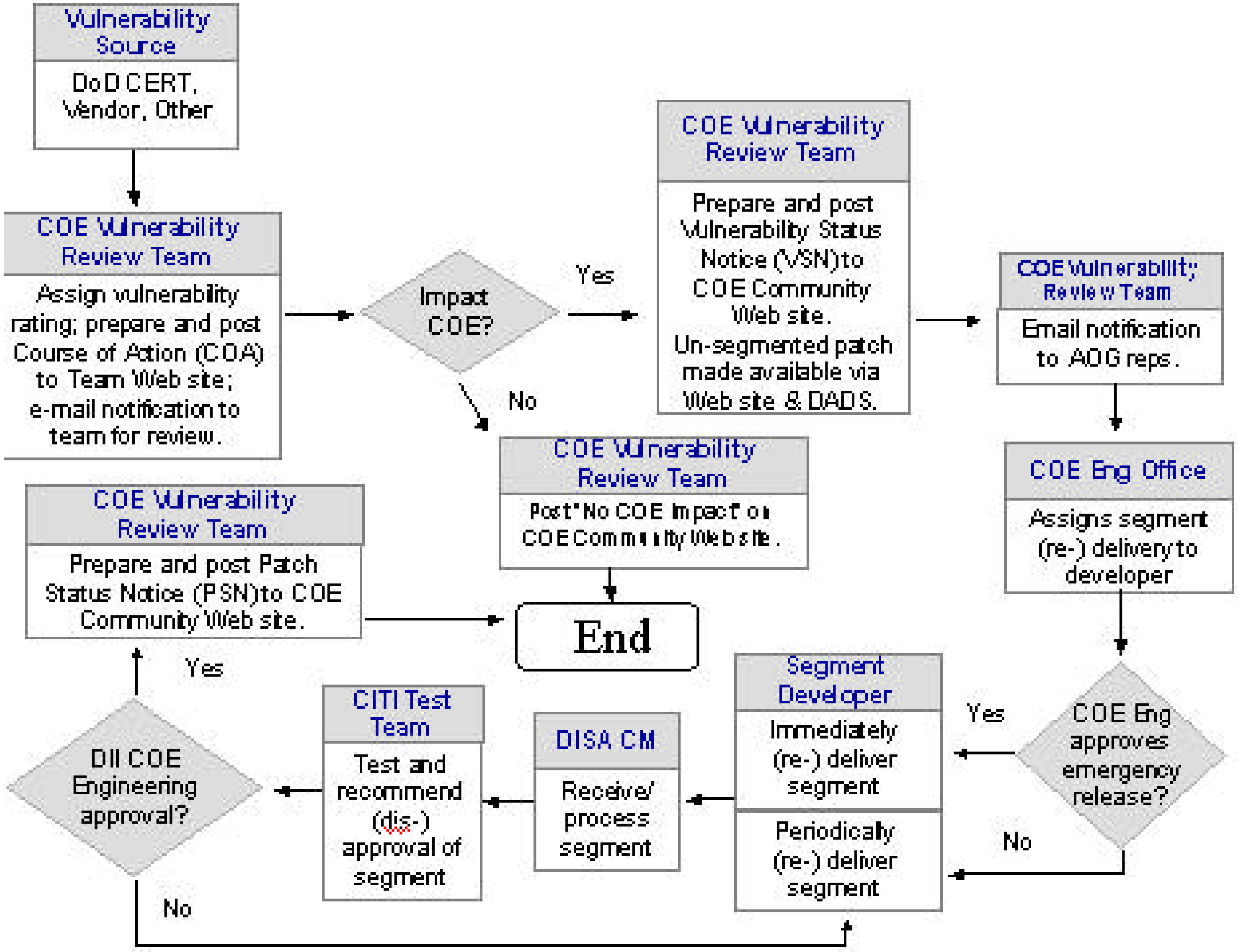
Host and Network Intrusion Detection Plan

- System design phase will select and cost host and network intrusion detection products/tools
- Intrusion detection products/tools/processes are intended to protect against and respond to penetrations (i.e., defense-in-depth capability)
- Host-based products/tools may include malicious code protection (e.g., anti-virus) and integrity-checking tools (e.g., Tripwire)
- Patch process is essential element for O&M
  - Example: NIAP Assurance Maintenance Program *

Implementation

* http://www.niap.nist.gov/cc-scheme/Pub6_v1.pdf

Host and Network Intrusion Detection Plan (2)



Vulnerability Source
DoD CERT, Vendor, Other

COE Vulnerability Review Team
Assign vulnerability rating; prepare and post Course of Action (COA) to Team Web site; e-mail notification to team for review.

Impact COE?

Yes

No

COE Vulnerability Review Team
Prepare and post Vulnerability Status Notice (VSN) to COE Community Web site.
Un-segmented patch made available via Web site & DADS.

COE Vulnerability Review Team
Email notification to AOG reps.

COE Vulnerability Review Team
Post "No COE Impact" on COE Community Web site.

End

COE Eng Office
Assigns segment (re-) delivery to developer

COE Eng approves emergency release?

Yes

No

Segment Developer
Immediately (re-) deliver segment
Periodically (re-) deliver segment

DISA CM
Receive/ process segment

CITI Test Team
Test and recommend (dis-) approval of segment

DII COE Engineering approval?

Yes

No

COE Vulnerability Review Team
Prepare and post Patch Status Notice (PSN) to COE Community Web site.

Security Monitoring

- Security monitoring
  - Ensures compliance with security requirements
    - Including process requirements
  - Provides assurance regarding security posture
- Conduct audit/process reviews, respond to incident reports and release security patches
- Security monitoring is ideal for process metrics collection and evaluation
  - Initial: binary—performed/not performed
  - Interim: process efficiency and problem/trend analysis
  - Final: increase robustness in problem areas (product or process)

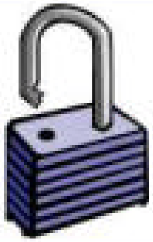
Operations & Maintenance

Security Monitoring (2)

- Security requirements are designed to address three principal types of vulnerabilities:
  - Inherent (e.g., remote login service—no authentication)
  - Strength-of-mechanism (e.g., password construction)
  - Defective engineering (e.g., buffer overflow condition)
- Defective engineering vulnerabilities are addressed throughout system operation
  - Commercial-off-the-shelf operating systems and apps.
  - Custom/proprietary applications

Inherent

Strength-of-Mechanism



Defective Engineering

Operations & Maintenance

Security Monitoring (3)

Vulnerability Patch Process Metrics
December 2002

Initial Response Time

- Elapsed calendar days from receipt of DoD IAVA to issuance of Course of Action (COA) report
- Target time is 2 calendar days
- Metric is only applicable to DoD-generated IAVAs (vice COE-generated vulnerability notices)
- Priority Code (Pri): R = Routine, P = Priority, C = Critical

COE#	Pri	IAVA Receipt	COA Issue	Calendar Days
coe02-096	C	12/04/02	11/20/02	-14
coe02-103	C	12/13/02	12/11/02	-2
coe02-079	P	12/16/02	12/5/02	-11
coe02-108	R	12/19/02	12/20/02	1

Operations & Maintenance

Periodic Evaluation of Countermeasures

- Review of system architecture/operation
- Review of security incident reports
- Review of security vulnerabilities identified through patch process
- Review of security products/tools
- Review of process metrics

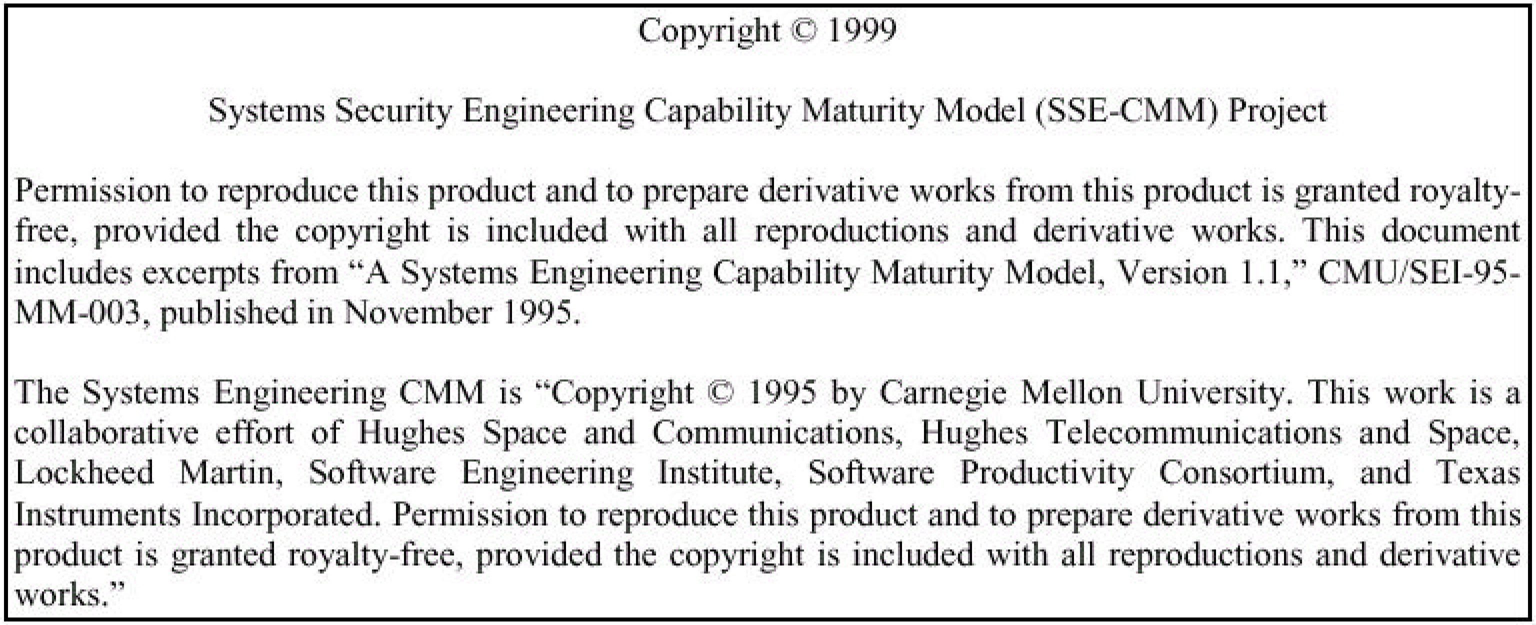
Operations & Maintenance

Summary

- IA process capability is a defense-in-depth mechanism to sustain an enterprise's security posture
- Process elements continue to be refined to reflect
  - System development/systems engineering activities
  - Operational environment/characteristics (e.g., DoD)
  - Process maturity: "The maturity of the discipline is defined by the robustness of its processes"
- Security engineering practices are becoming sufficiently robust to collect and evaluate metrics
  - Robustness is a topic of considerable interest *
- Identification and collection of "best of breed" practices will enable widespread adoption

* See Chapter 4 of IATF Document

Questions?



Back-up Slides

Capability Dimension Overview

Capability Level 1 – Performed Informally

- ***Common Feature 1.1 – Base Practices Are Performed***

Capability Level 2 – Planned and Tracked

- ***Common Feature 2.1 – Planning Performance***
- ***Common Feature 2.2 – Disciplined Performance***
- ***Common Feature 2.3 – Verifying Performance***
- ***Common Feature 2.4 – Tracking Performance***

Capability Level 3 – Well Defined

- ***Common Feature 3.1 – Defining a Standard Process***
- ***Common Feature 3.2 – Perform the Defined Process***
- ***Common Feature 3.3 – Coordinate Practices***

Capability Dimension Overview (2)

Capability Level 4 – Quantitatively Controlled

Common Feature 4.1 – Establishing Measurable Quality Goals
Common Feature 4.2 – Objectively Managing Performance

Capability Level 5 – Continuously Improving

Common Feature 5.1 – Improving Organizational Capability
Common Feature 5.2 – Improving Process Effectiveness

PA01: Administer Security Controls

Goal 1 Security controls are properly configured and used.

BP.01.01 Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.

BP.01.02 Manage the configuration of system security controls.

BP.01.03 Manage security awareness, training, and education programs for all users and administrators.

BP.01.04 Manage periodic maintenance and administration of security services and control mechanisms.

PA02: Assess Impact

Goal 1 The security impacts of risks to the system are identified and characterized.

BP.02.01 Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system.

BP.02.02 Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system.

BP.02.03 Select the impact metric to be used for this assessment.

BP.02.04 Identify the relationship between the selected metrics for this assessment and metric conversion factors if required.

BP.02.05 Identify and characterize impacts.

BP.02.06 Monitor ongoing changes in the impacts.

PA03: Assess Security Risk

Goal 1 An understanding of the security risk associated with operating the system within a defined environment is achieved.

Goal 2 Risks are prioritized according to a defined methodology.

BP.03.01 Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analyzed, assessed, and compared.

BP.03.02 Identify threat/vulnerability/impact triples (exposures).

BP.03.03 Assess the risk associated with the occurrence of an exposure.

BP.03.04 Assess the total uncertainty associated with the risk for the exposure.

BP.03.05 Order risks by priority.

BP.03.06 Monitor ongoing changes in the risk spectrum and changes to their characteristics.

PA04: Assess Threat

Goal 1 Threats to the security of the system are identified and characterized.

BP.04.01 Identify applicable threats arising from a natural source.

BP.04.02 Identify applicable threats arising from man-made sources, either accidental or deliberate.

BP.04.03 Identify appropriate units of measure, and applicable ranges, in a specified environment.

BP.04.04 Assess capability and motivation of threat agent for threats arising from man-made sources.

BP.04.05 Assess the likelihood of an occurrence of a threat event.

BP.04.06 Monitor ongoing changes in the threat spectrum and changes to their characteristics.

PA05: Assess Vulnerability

Goal 1 An understanding of system security vulnerabilities within a defined environment is achieved.

BP.05.01 Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized.

BP.05.02 Identify system security vulnerabilities.

BP.05.03 Gather data related to the properties of the vulnerabilities.

BP.05.04 Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities.

BP.05.05 Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics.

PA06: Build Assurance Argument

Goal 1 The work products and processes clearly provide the evidence that the customer's security needs have been met.

BP.06.01 Identify the security assurance objectives.

BP.06.02 Define a security assurance strategy to address all assurance objectives.

BP.06.03 Identify and control security assurance evidence.

BP.06.04 Perform analysis of security assurance evidence.

BP.06.05 Provide a security assurance argument that demonstrates the customer's security needs are met.

PA07: Coordinate Security

Goal 1 All members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions.

Goal 2 Decisions and recommendations related to security are communicated and coordinated.

BP.07.01 Define security engineering coordination objectives and relationships.

BP.07.02 Identify coordination mechanisms for security engineering.

BP.07.03 Facilitate security engineering coordination.

BP.07.04 Use the identified mechanisms to coordinate decisions and recommendations related to security.

PA08: Monitor Security Posture

Goal 1 Both internal and external security related events are detected and tracked.
Goal 2 Incidents are responded to in accordance with policy.
Goal 3 Changes to the operational security posture are identified and handled in accordance with the security objectives.

BP.08.01 Analyze event records to determine the cause of an event, how it proceeded, and likely future events.
BP.08.02 Monitor changes in threats, vulnerabilities, impacts, risks, and the environment.
BP.08.03 Identify security relevant incidents.
BP.08.04 Monitor the performance and functional effectiveness of security safeguards.
BP.08.05 Review the security posture of the system to identify necessary changes.
BP.08.06 Manage the response to security relevant incidents.
BP.08.07 Ensure that the artifacts related to security monitoring are suitably protected.

PA09: Provide Security Input

Goal 1 All system issues are reviewed for security implications and are resolved in accordance with security goals.
Goal 2 All members of the project team have an understanding of security so they can perform their functions.
Goal 3 The solution reflects the security input provided.

BP.09.01 Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.
BP.09.02 Determine the security constraints and considerations needed to make informed engineering choices.
BP.09.03 Identify alternative solutions to security related engineering problems.
BP.09.04 Analyze and prioritize engineering alternatives using security constraints and considerations.
BP.09.05 Provide security related guidance to the other engineering groups.
BP.09.06 Provide security related guidance to operational system users and administrators.

PA10: Specify Security Needs

Goal 1 A common understanding of security needs is reached between all parties, including the customer.

BP.10.01 Gain an understanding of the customer's security needs.
BP.10.02 Identify the laws, policies, standards, external influences and constraints that govern the system.
BP.10.03 Identify the purpose of the system in order to determine the security context.
BP.10.04 Capture a high-level security oriented view of the system operation.
BP.10.05 Capture high-level goals that define the security of the system.
BP.10.06 Define a consistent set of statements which define the protection to be implemented in the system.
BP.10.07 Obtain agreement that the specified security meets the customer's needs.

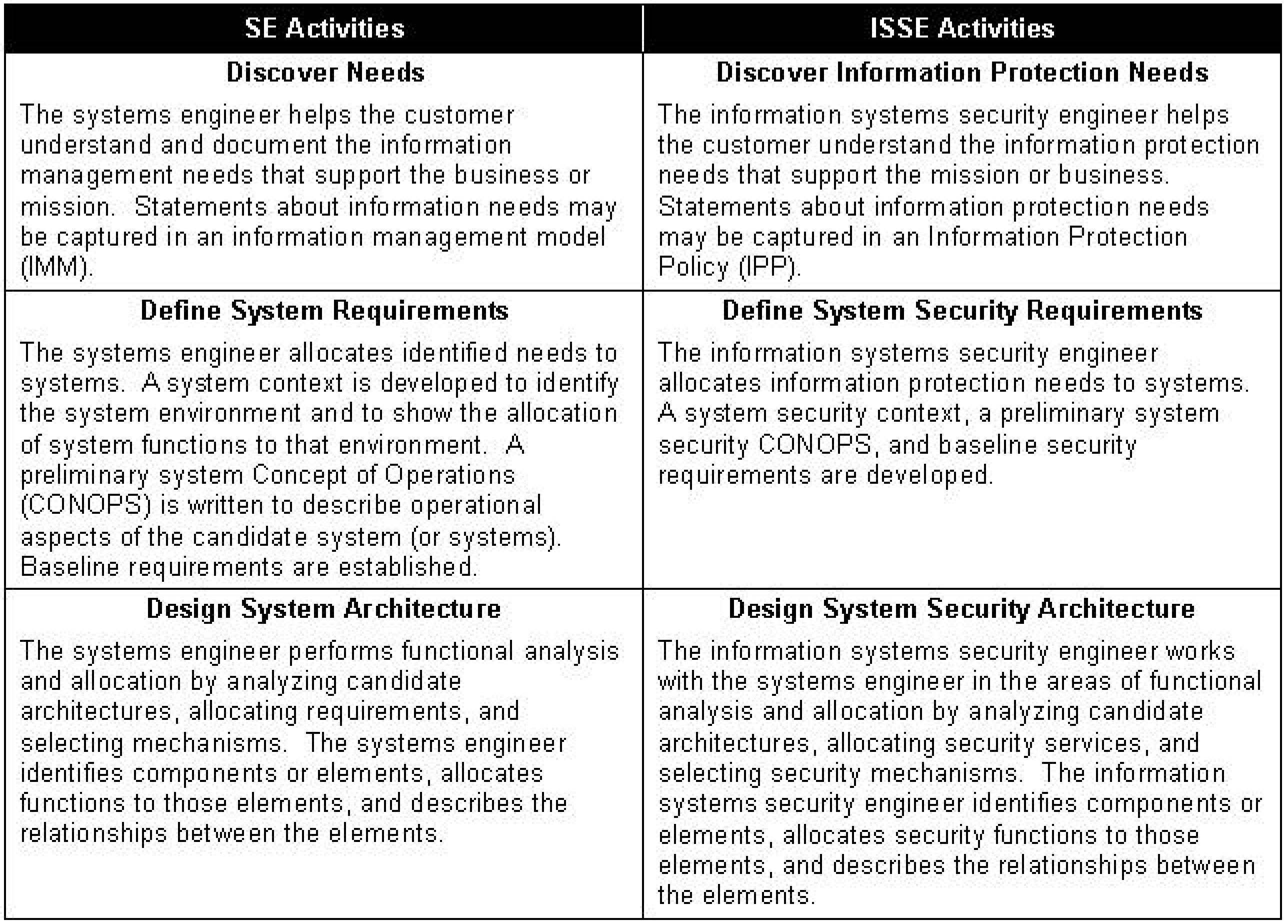
PA11: Verify and Validate Security

Goal 1 Solutions meet security requirements.
Goal 2 Solutions meet the customer’s operational security needs.

BP.11.01 Identify the solution to be verified and validated.
BP.11.02 Define the approach and level of rigor for verifying and validating each solution.
BP.11.03 Verify that the solution implements the requirements associated with the previous level of abstraction.
BP.11.04 Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer’s operational security needs.
BP.11.05 Capture the verification and validation results for the other engineering groups.

IATF's ISSE Process

- ISSE process activities are related to SE Process activities

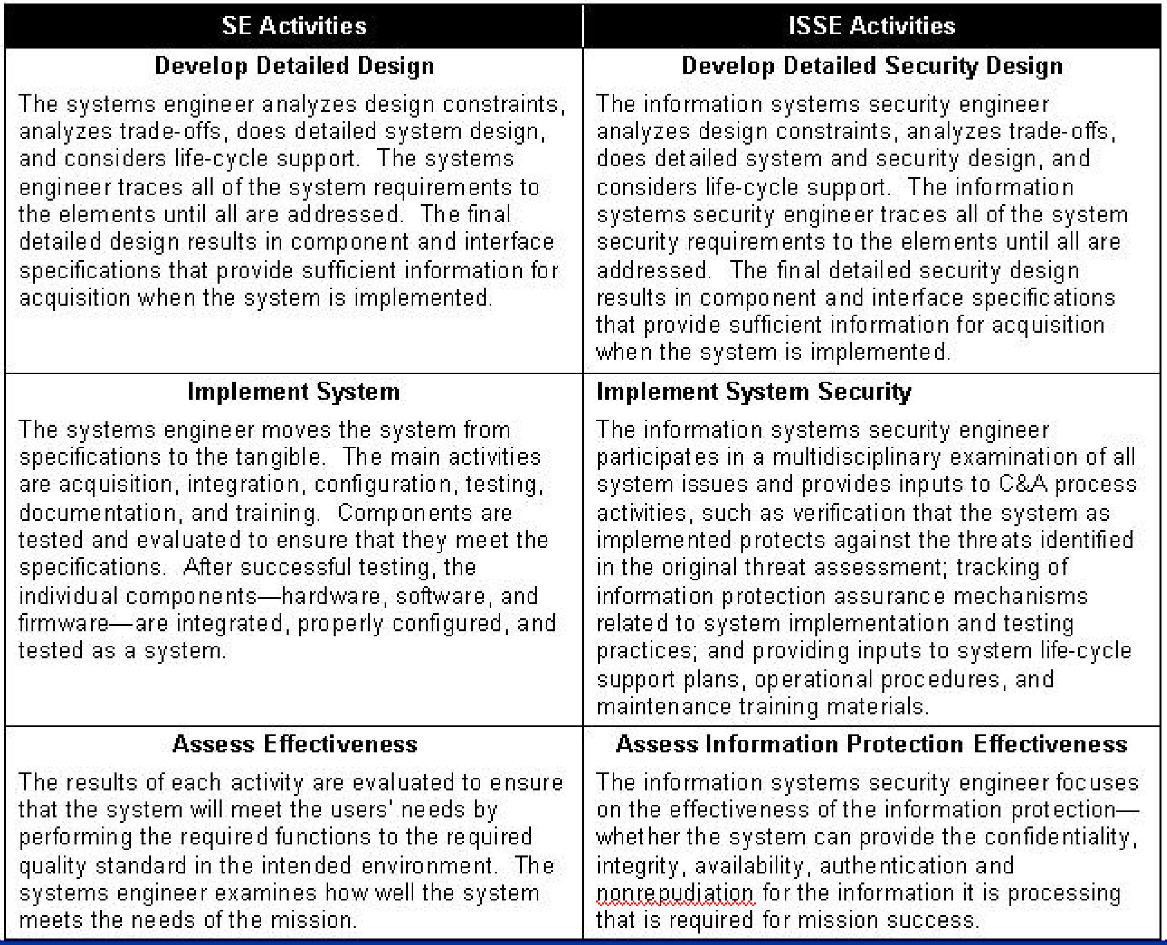


SE Activities	ISSE Activities
Discover Needs The systems engineer helps the customer understand and document the information management needs that support the business or mission. Statements about information needs may be captured in an information management model (IMM).	**Discover Information Protection Needs** The information systems security engineer helps the customer understand the information protection needs that support the mission or business. Statements about information protection needs may be captured in an Information Protection Policy (IPP).
Define System Requirements The systems engineer allocates identified needs to systems. A system context is developed to identify the system environment and to show the allocation of system functions to that environment. A preliminary system Concept of Operations (CONOPS) is written to describe operational aspects of the candidate system (or systems). Baseline requirements are established.	**Define System Security Requirements** The information systems security engineer allocates information protection needs to systems. A system security context, a preliminary system security CONOPS, and baseline security requirements are developed.
Design System Architecture The systems engineer performs functional analysis and allocation by analyzing candidate architectures, allocating requirements, and selecting mechanisms. The systems engineer identifies components or elements, allocates functions to those elements, and describes the relationships between the elements.	**Design System Security Architecture** The information systems security engineer works with the systems engineer in the areas of functional analysis and allocation by analyzing candidate architectures, allocating security services, and selecting security mechanisms. The information systems security engineer identifies components or elements, allocates security functions to those elements, and describes the relationships between the elements.

IATF Document, Chapter 3, pp. 3-3 & 3-4

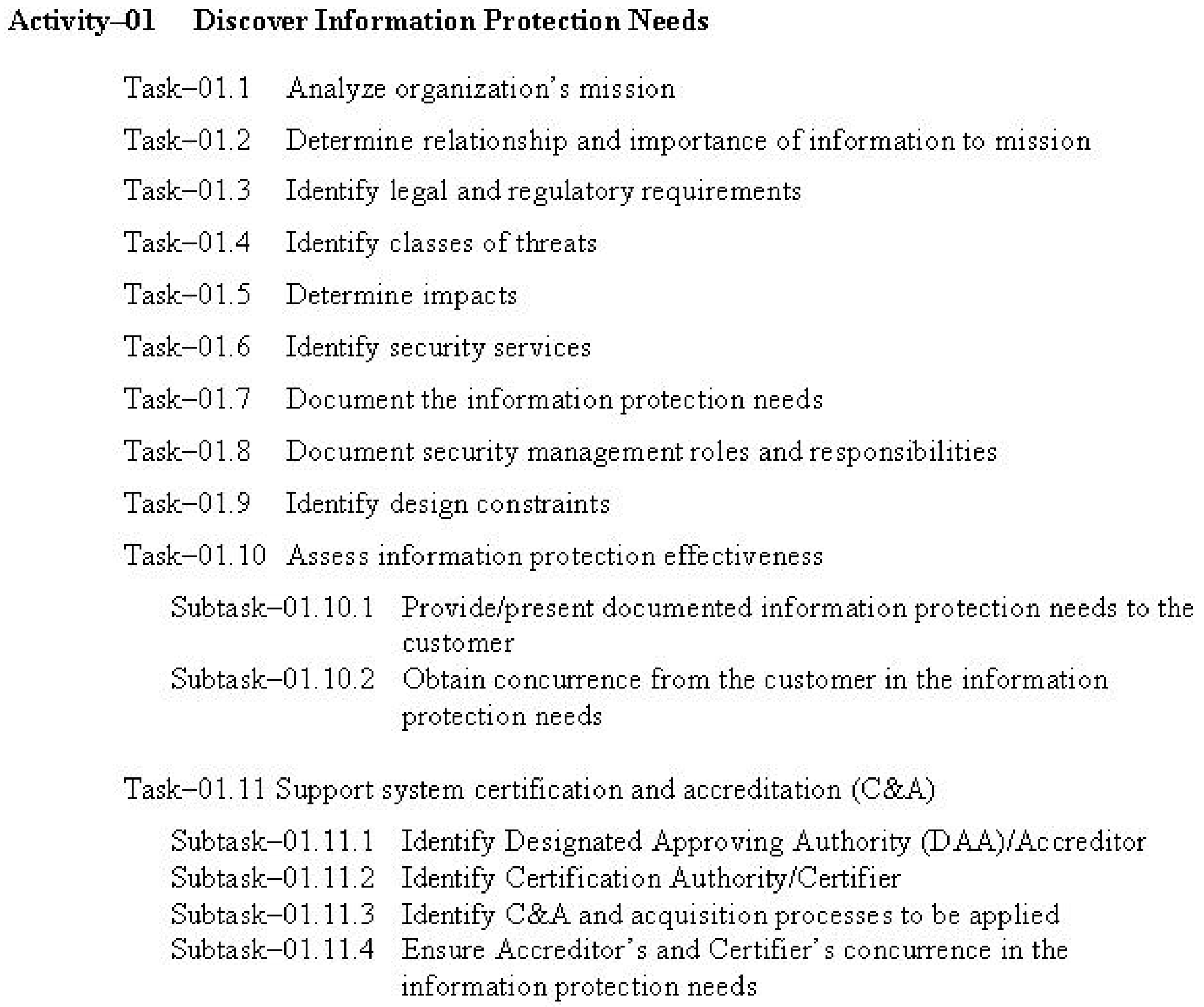
IATF's ISSE Process (2)

- **ISSE process activities are related to SE Process activities (2)**



SE Activities	ISSE Activities
Develop Detailed Design The systems engineer analyzes design constraints, analyzes trade-offs, does detailed system design, and considers life-cycle support. The systems engineer traces all of the system requirements to the elements until all are addressed. The final detailed design results in component and interface specifications that provide sufficient information for acquisition when the system is implemented.	**Develop Detailed Security Design** The information systems security engineer analyzes design constraints, analyzes trade-offs, does detailed system and security design, and considers life-cycle support. The information systems security engineer traces all of the system security requirements to the elements until all are addressed. The final detailed security design results in component and interface specifications that provide sufficient information for acquisition when the system is implemented.
Implement System The systems engineer moves the system from specifications to the tangible. The main activities are acquisition, integration, configuration, testing, documentation, and training. Components are tested and evaluated to ensure that they meet the specifications. After successful testing, the individual components—hardware, software, and firmware—are integrated, properly configured, and tested as a system.	**Implement System Security** The information systems security engineer participates in a multidisciplinary examination of all system issues and provides inputs to C&A process activities, such as verification that the system as implemented protects against the threats identified in the original threat assessment; tracking of information protection assurance mechanisms related to system implementation and testing practices; and providing inputs to system life-cycle support plans, operational procedures, and maintenance training materials.
Assess Effectiveness The results of each activity are evaluated to ensure that the system will meet the users' needs by performing the required functions to the required quality standard in the intended environment. The systems engineer examines how well the system meets the needs of the mission.	**Assess Information Protection Effectiveness** The information systems security engineer focuses on the effectiveness of the information protection—whether the system can provide the confidentiality, integrity, availability, authentication and nonrepudiation for the information it is processing that is required for mission success.

IATF's 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

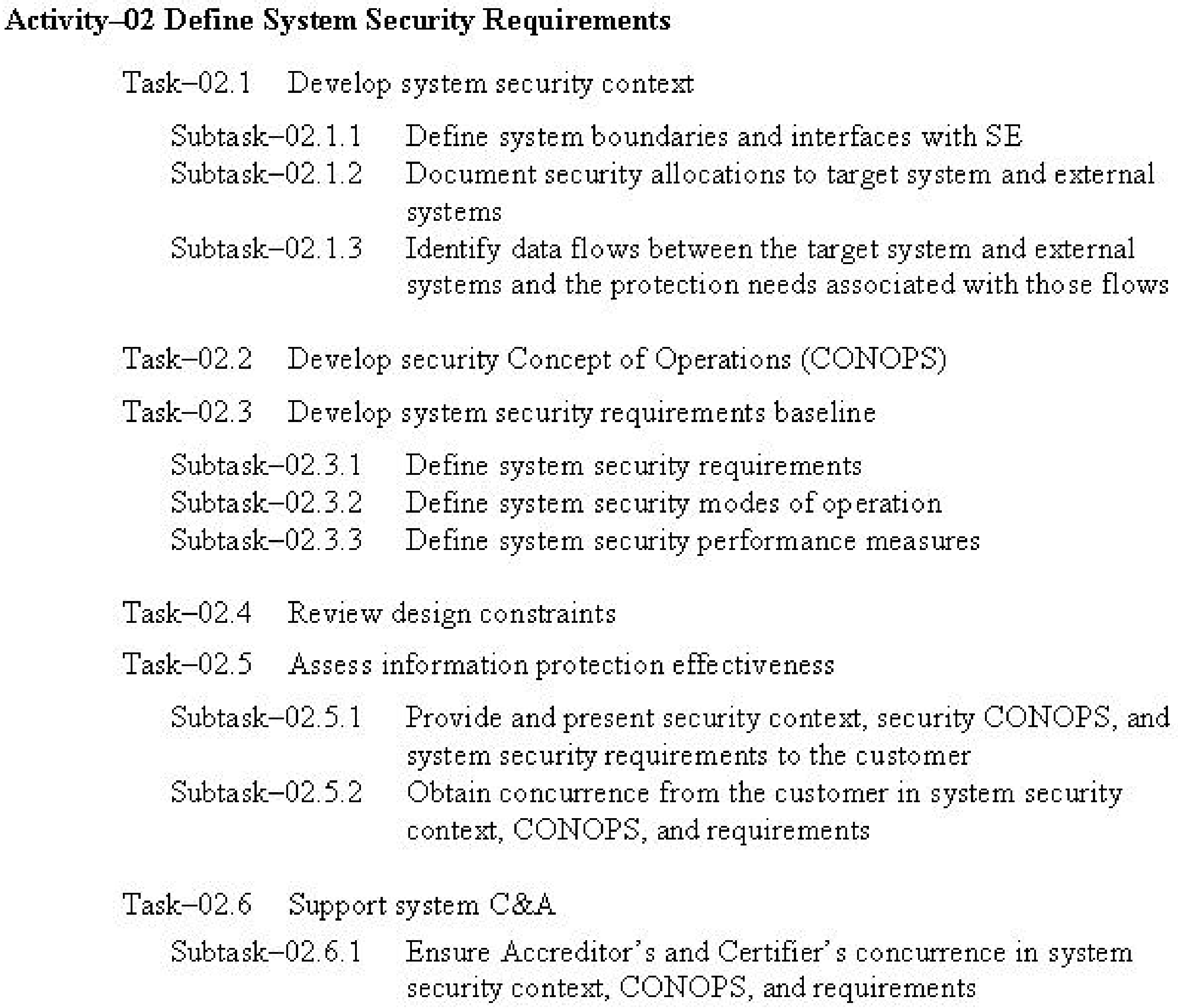
- Subtask–01.10.1 Provide/present documented information protection needs to the customer
- Subtask–01.10.2 Obtain concurrence from the customer in the information protection needs

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 Accreditor's and Certifier's concurrence in the information protection needs

IATF Document, Appendix J, pp. J-1 - J-6

IATF's ISSE Master Activity and Task List (2)



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

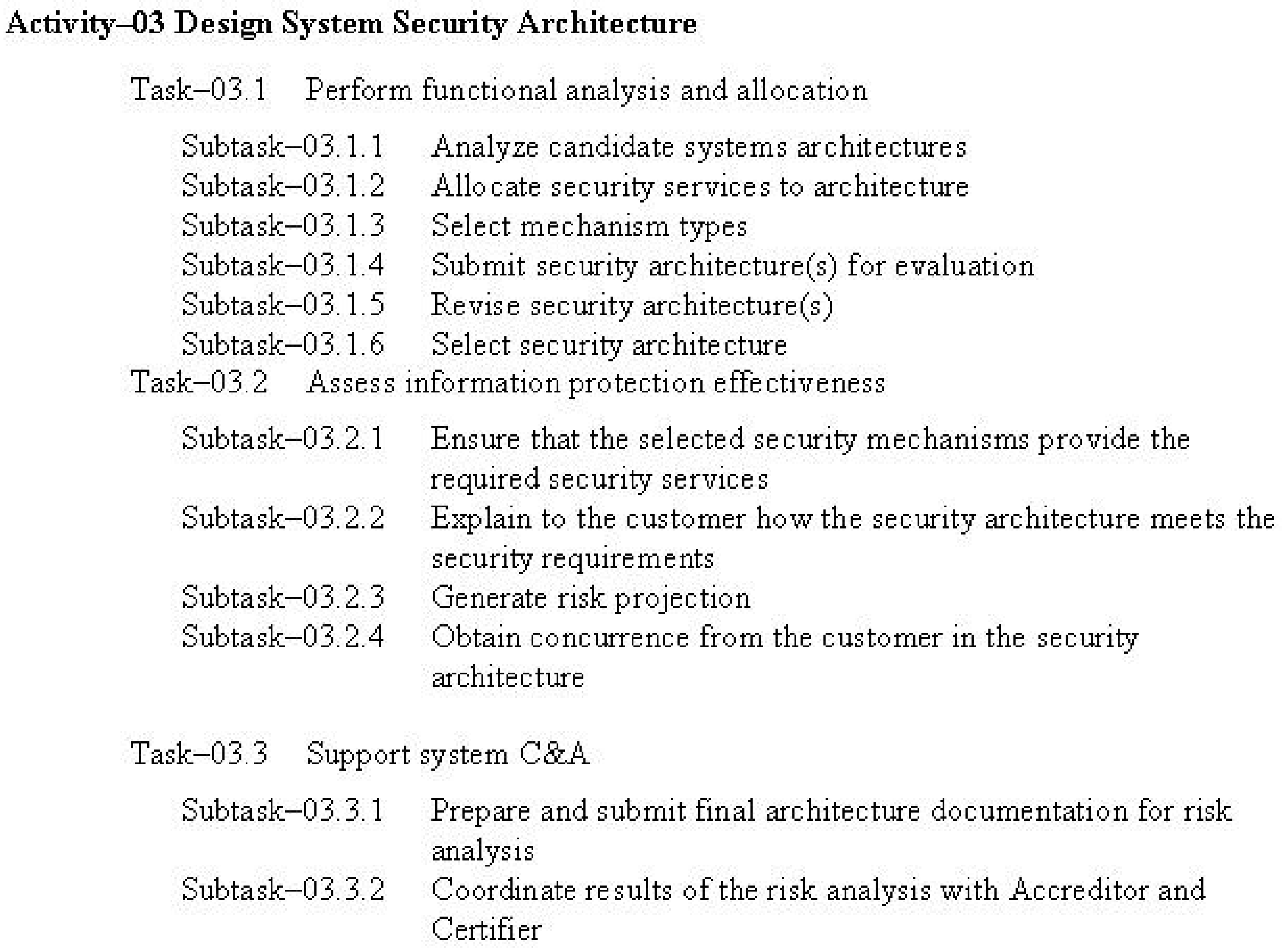
Task–02.5 Assess information protection effectiveness

- 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

IATF’s ISSE Master Activity and Task List (3)



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

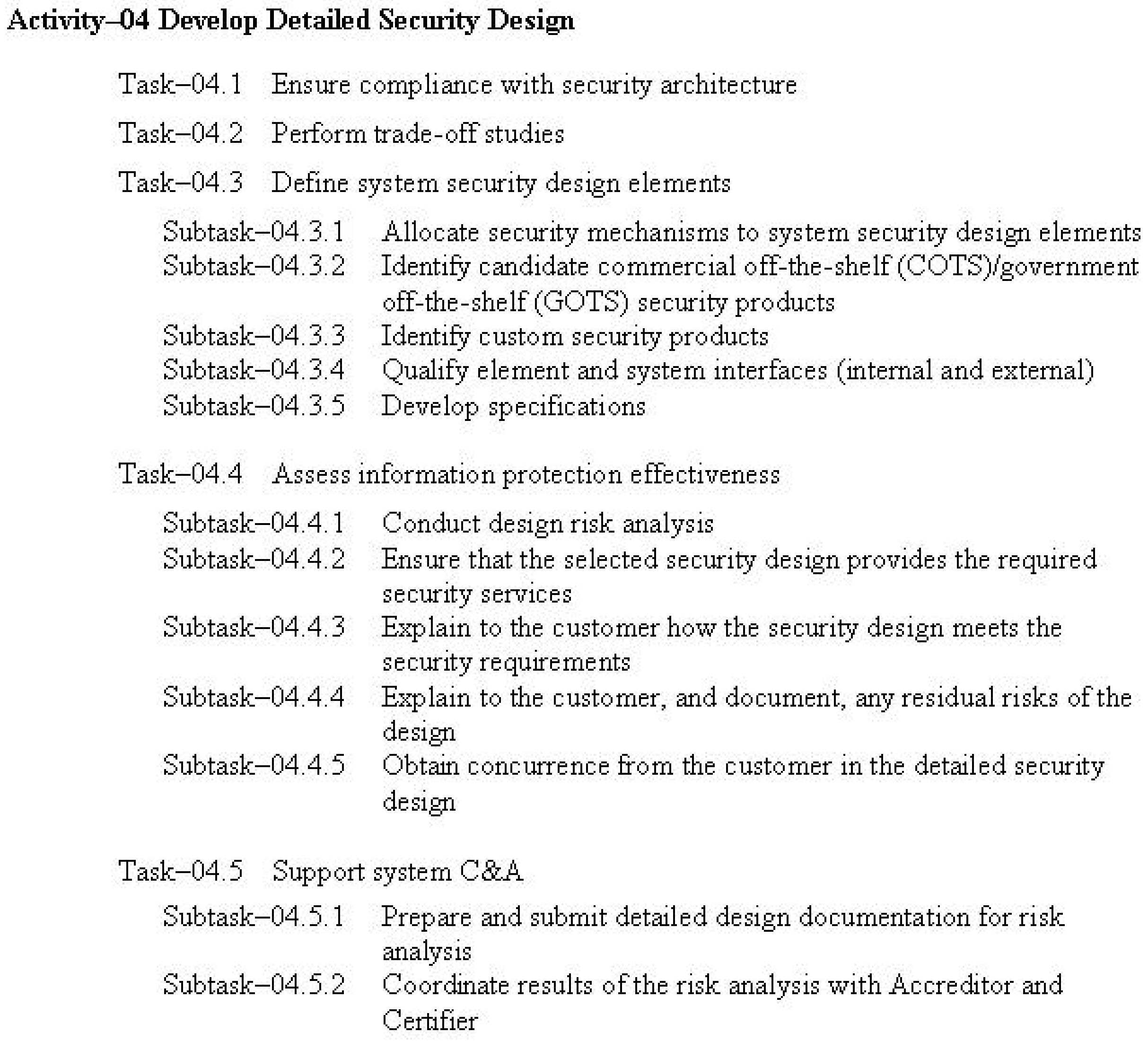
Task–03.2 Assess information protection effectiveness

- 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 Accreditor and Certifier

IATF's ISSE Master Activity and Task List (4)



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

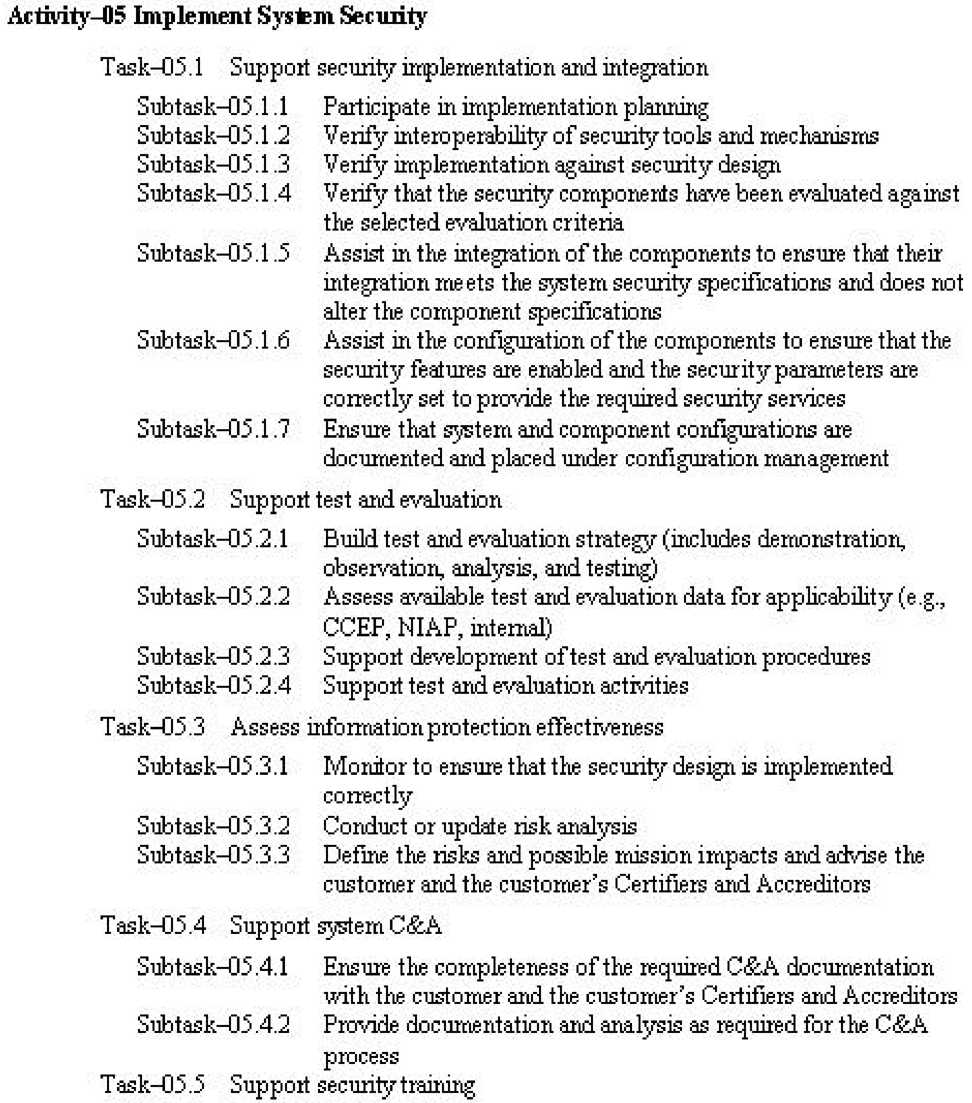
Task–04.4 Assess information protection effectiveness

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

IATF's ISSE Master Activity and Task List (5)



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

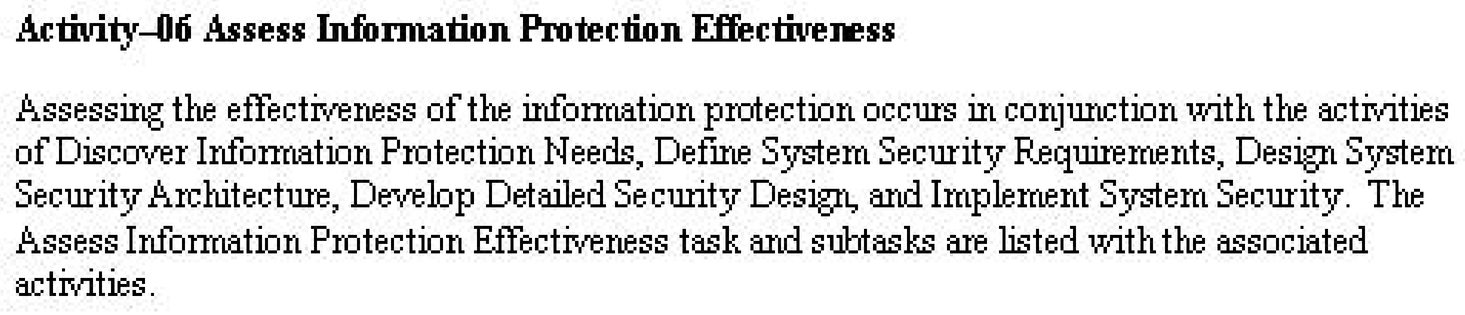
Subtask–05.3.1 Monitor to ensure that the security design is implemented correctly
Subtask–05.3.2 Conduct or update risk analysis
Subtask–05.3.3 Define the risks and possible mission impacts and advise the customer and the customer's Certifiers and Accreditors

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

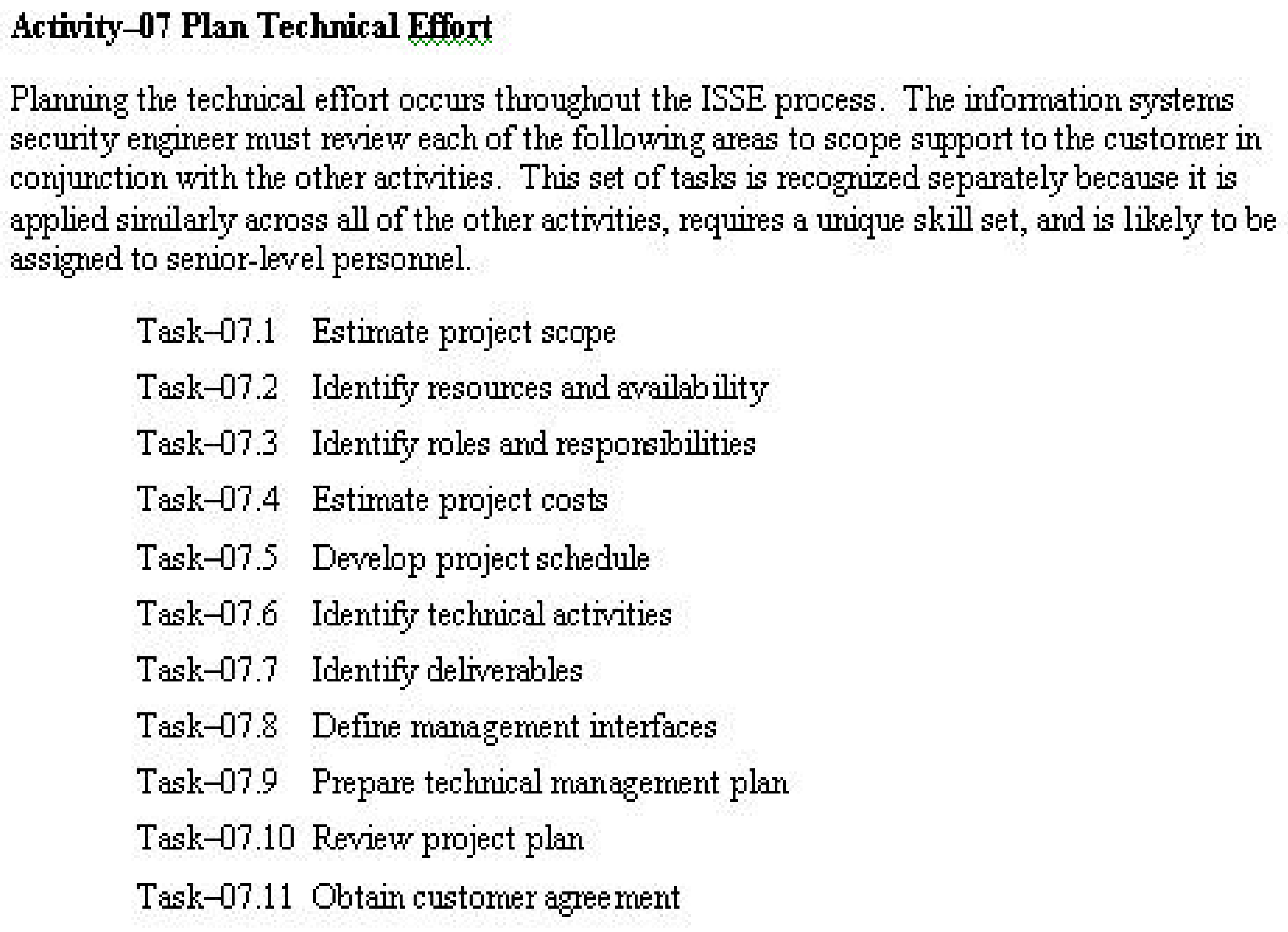
IATF's ISSE Master Activity and Task List (6)



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.

IATF's ISSE Master Activity and Task List (7)

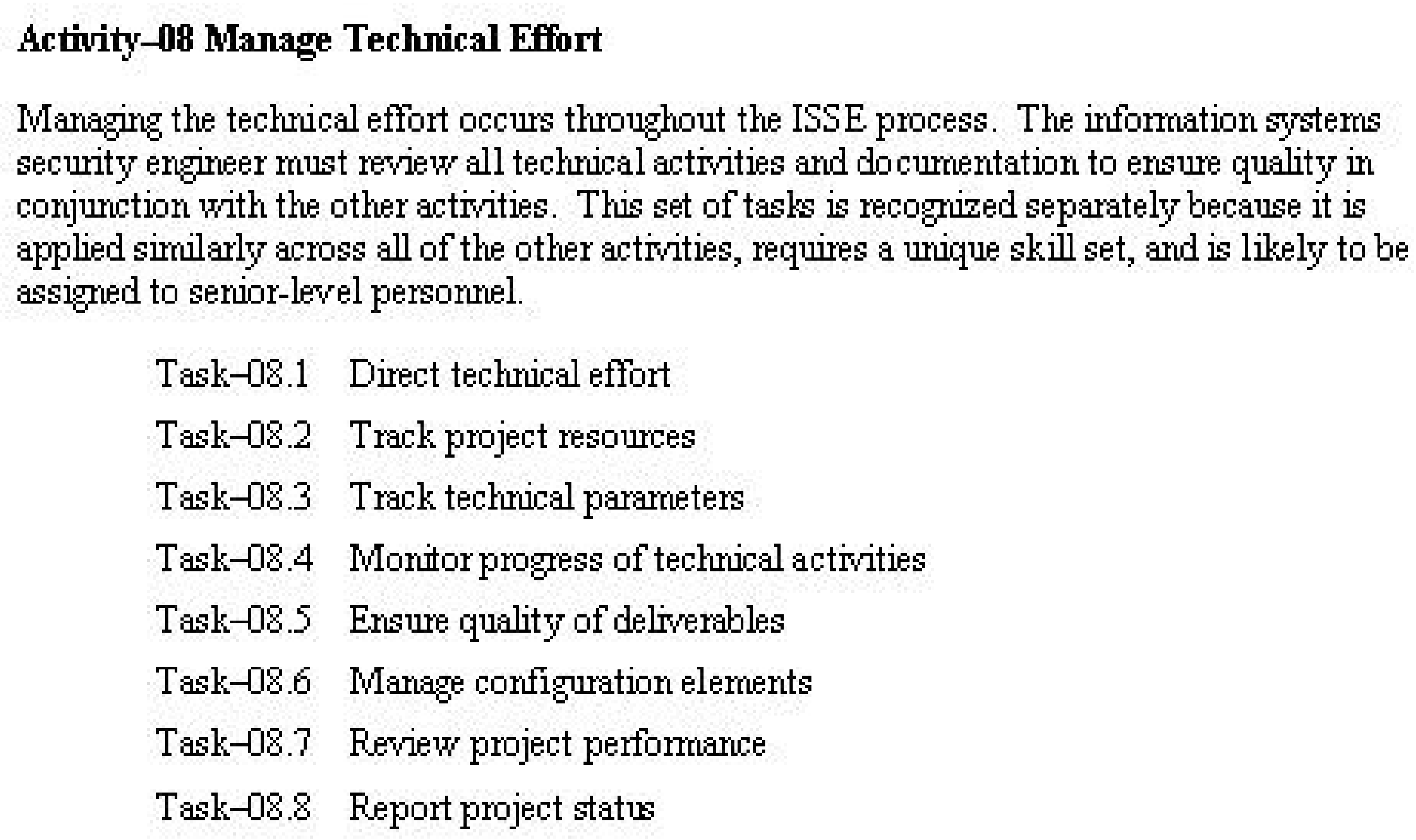


Activity–07 Plan Technical Effort

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

IATF's ISSE Master Activity and Task List (8)



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