Annex D

Summary of the Components, Activities, and Tasks of an Effective Information Security/IA Program

This annex summarizes the components, activities, and tasks of an effective information security/IA program. Exhibit 1 illustrates the interaction between the components of an information security/IA program, as discussed in Chapters 4 through 8. Exhibit 2 defines the inputs, outputs, and dependencies of these components, activities, and tasks.

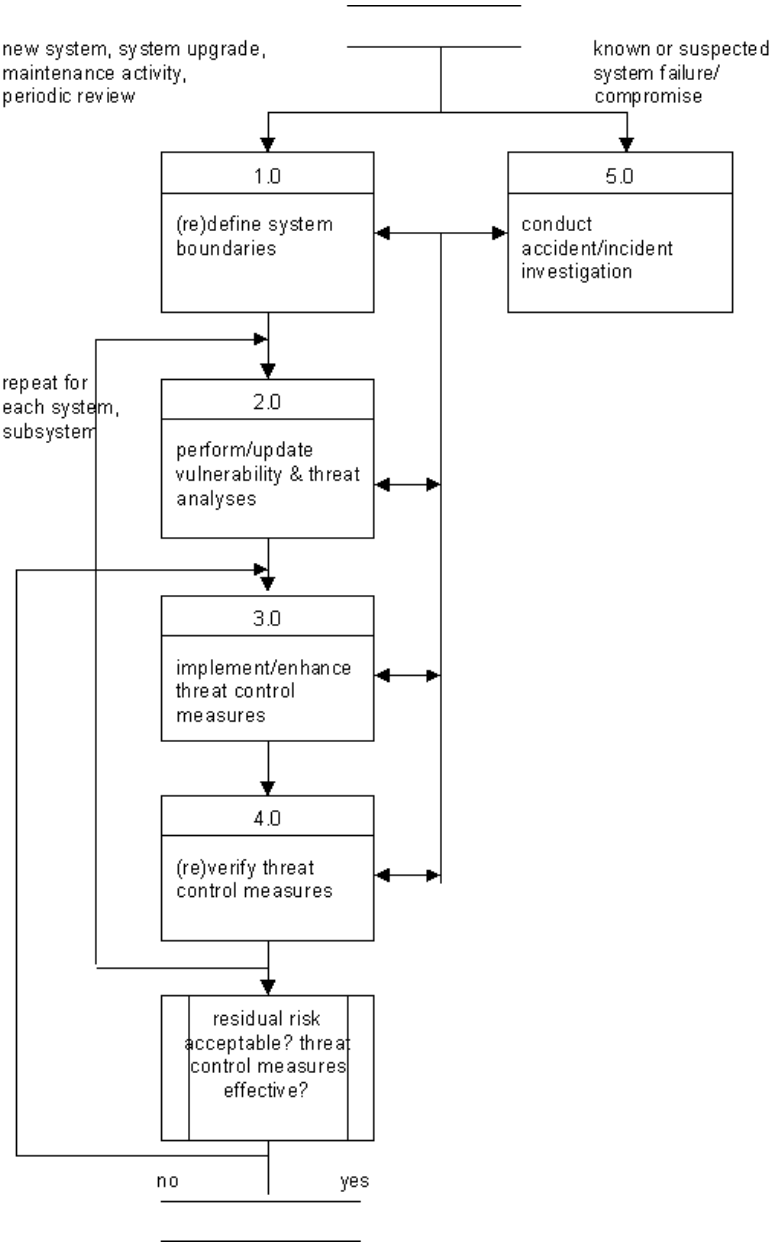

Exhibit 1 Interaction Between Components of an Effective Computer Security/IA Program

Exhibit 2 Summary of the Components, Activities, and Tasks of an Effective Information Security/IA Program

	Component/Activity/Task	*Inputs*	*Outputs*
1.	**Define the System Boundaries**		
1.1	Determine what is being protected and why		IA goals Justification for IA goals
1.2	Identify the system		System definition
1.3	Characterize system operation	System definition	System operation characterization
1.4	Ascertain what you do/do not have control over	System definition	System entity control analysis
2.	**Perform Vulnerability and Threat Analyses**		
2.1	Select and use IA analysis techniques	IA goals	Analysis results
2.2	Identify type, source, and severity of vulnerabilities	Analysis results System definition System entity control analysis	System vulnerability characterization
2.2.1	Identify potential failure/attack points		
2.2.2	Postulate failure/compromise scenarios		
2.2.3	Perform vulnerability analyses		
2.3	Identify type, source, and likelihood of threats	Analysis results System vulnerability characterization System entity control analysis	System threat characterization
2.4	Identify transaction paths	System definition	Transaction paths
2.5	Evaluate transaction paths, critical threat zones, risk exposure	System operation characterization	Initial risk exposure Updated system vulnerability characterization Updated system threat characterization
3.	**Implement Threat Control Measures**		
3.1	Determine how much protection is needed	IA goals Initial risk exposure	IA integrity level
3.1.1	Compare initial risk exposure to target		
3.1.2	Identify IA-critical, IA-related functions, entities		
3.1.3	Specify MWFs, MNWFs		
3.1.4	Reassess entity control analysis		
3.1.5	Evaluate time element		
3.1.6	Reassess privacy issues		
3.1.7	Update/refine estimated level of protection needed		

Exhibit 2 Summary of the Components, Activities, and Tasks of an Effective Information Security/IA Program (continued)

	Component/Activity/Task	*Inputs*	*Outputs*
3.2	Evaluate controllability, operational procedures, in-service considerations	System operation characterization IA integrity level	Updated operational procedures Updated physical security practices
3.2.1	Identify hazard consequences		
3.2.2	Ascertain best and most likely outcomes		
3.2.3	Ascertain worst-case outcome		
3.2.4	Determine severity range		
3.2.5	Update/refine IA integrity level		
3.3	Plan for contingencies, disaster recovery	IA goals IA integrity level System definition System entity control analysis System vulnerability characterization System threat characterization Transaction paths Critical threat zones	Contingency plans
3.3.1	Identify all internal and external system entities		
3.3.2	Identify failure points/modes, loss/compromise scenarios		
3.3.3	Formulate alternative courses of action, identify alternate resources		
3.3.4	Assign responsibility for deploying alternatives		
3.3.5	Define maximum response time interval		
3.3.6	Identify alternate response if maximum time interval is exceeded		
3.3.7	Communicate plan, training, practice drills		
3.3.8	Update, revalidate plan		
3.4	Perception management		
3.5	Select/implement IA design techniques/features	IA integrity level Operational procedures Contingency plans Physical security practices	Threat control measures

Exhibit 2 Summary of the Components, Activities, and Tasks of an Effective Information Security/IA Program (continued)

	Component/Activity/Task	*Inputs*	*Outputs*
4.	**Verify Effectiveness of Threat Control Measures**		
4.1	Select, employ IA verification techniques	System operation characterization System vulnerability characterization System threat characterization Transaction paths Critical threat zones IA integrity level	Results of static and dynamic analyses
4.2	Determine residual risk exposure	IA integrity case	Threat control effectiveness assessment Threat control effectiveness summary
4.3	Monitor ongoing vulnerabilities, threats, and survivability	Changes or additions to operational profile or mission System enhancements System reconfiguration	Updated: System vulnerability characterization System threat characterization Threat control effectiveness assessment Threat control effectiveness summary IA integrity case
5.	**Conduct Accident/Incident Investigations**		
5.1	Analyze failure/compromise	IA integrity case IA accident/incident investigation techniques	Investigation results Updated IA integrity case
5.2	Initiate recovery mechanisms	Investigation results Backups Operational procedures Contingency plans	
5.3	Report accident/incident	Investigation results	Standardized initial and follow-up reports
5.4	Deploy remedial measures	Lessons learned	Updated: System vulnerability characterization System threat characterization Threat control measures IA integrity case Operational procedures Contingency plans, etc.

Exhibit 2 Summary of the Components, Activities, and Tasks of an Effective Information Security/IA Program (continued)

	Component/Activity/Task	*Inputs*	*Outputs*
5.5	Evaluate legal issues	Standardized accident/incident reports Local, national, and international laws	Informed legal action