Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
Schedule and Progress	Measures applicable to monitoring progress and schedule of activities. Two viewpoints are identified: (1) the development of a system or component, by means of a traditional project and SDLC: this is implied in PSM. Activities are planned and scheduled with reference to a linear sequence of gates etc. The state of the product evolves from an initial state to a desired end state. (2) the provision of a service, by means of quasi-continuous processes, usually modelled by PDCA cycle or similar (as in ISO/IEC 27000). Activities are planned and scheduled on a cyclic basis; response times are important. Service state is maintained in the face of change and disturbance. Whether activities are viewed as linear or continuous can depend on viewpoint; for example maintenance activities can be viewed as mini-projects by the maintainer, but as a means to maintain service by a service provider.			
	Work Unit Status	What is the current state of completion of planned security tasks? What is the current progress of assurance evidence development?	Status of planned security process tasks	Progress of activities against Project Plan, current plan. Depends on SDLC and WBS
		Are risk mitigations on schedule?		Refers to particular risk-driven activities
		How much of the system incorporates security features?	Units Secure	
		Have we completed security testing (e.g. attacks, penetration)?	Requirements Tested Procedures Tested	
		Have all identified security issues been resolved? (1)	Action items open/closed	
	Requirements Progress	Have we traced our security requirements? - have all sources been considered (e.g. threats, assets, usability, certification, etc.) - have all stakeholders been considered	Security requirements traced	Include derived rqmts Forward and backward traceability
		Are the security requirements valid? Do they meet user needs? (1)	Requirements validated	
		Are security requirements completed on schedule? - Mitigations	Requirements Tested	
		Have requirements been deliberately tampered with?	Requirements Integrity	
		Are we expressing our security requirements, following the best practices for doing so?	Requirements documented	Need to check against some standard

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
		If I state this security requirement, can I tell if it has been satisfied?	Requirements Testability	
		Security vulnerabilities VS Security Requirements		
	Design Progress	Have we followed security design principles?	# units following security design principles	Prospective measures will be determined by the SDLC: (a) modified standard SDLC – Microsoft SDL (b) formal SDLC – Praxis CbC (c) EAL selected, perceived risk level
		Does the design meet the security requirements placed on it? (is it sufficiently detailed and sufficient) Does each security requirement trace to an appropriate design unit(s)?	Design Traceability	
		Is the design such that it can be analyzed to see whether it meets the security policy? (can I tell – is it verifiable)? (1)	Design Verification	
	Source Code Progress	Has each unit complied with the secure coding practices? (1) Has each reused/COTS/NDI package complied with the secure coding practices?	# Units / packages complying with secure coding practices # units / packages that have been formally verified against a specification	Assumes objective criteria May have a measure for each specific code practice described
	Integration and Test Progress	How broad is the security testing (1) - including tools and people - how many attack patterns are evaluated - are we testing at the unit, subsystem, system-of-system level? - Static or dynamic testing? E.g. privileges, resource exhaustion, regular expressions	# units tested for security (unit level) % of system that has been tested for security (as an entire system)	Penetration test, attack patterns, etc.

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
	User/ Operations Definition Progress	Do we have coverage of security in user aids (help files, manuals, training, etc.)?		
	Maintenance Progress	Has each corrective maintenance action (security-related) been carried out? Tested?	# actions completed, tested for security (unit level)	
	Vulnerability Event Response	What is the progress in responding to a notification of a vulnerability, patch, weakness?		
	Threat Event Response	What is the progress in responding to a threat event, or notification of a potential threat?		
	Risk Mitigation Action status	How badly can I be harmed if my system security is violated? If something happens, how much is lost/ harmed? How valuable is the data? What is the progress in my damage limitation action?	Damage severity	
Resources and Cost	Measures applicable to monitoring the resources and costs consumed in security work, throughout the development and operations/maintenance phases. Security work is that work that achieves acceptable levels of security risks and performance in developed systems and provided services, and acceptable assurance information. (Damage costs are included under Product Quality, below)			
	Security Capability Deployed	Do I have adequate resources to achieve my security level: qualified people, tools, environments? (1)	Training records Personnel capability (security)	Professional Society models Split into separate questions. APIs Libraries
		Do I have qualified tools that support security analysis during development? How effective are the security tools? (goes into buy decision) (2)	# specific code practices evaluated by each tool	

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
		How effectively are they used?	# specific code practices evaluated using each tool compared to total number the tool is capable of evaluating	
		How many (insecure) code practices do these tools identify?	# defects identified	
		Do I have qualified tools that support security analysis during operations?		
	Resources Consumed in development	How much does it cost to implement security aspects?	Costs	Project Plan
		How much time does it take to implement security aspects?	Schedule	Project Plan
	Resources Consumed in operations	How much does it cost to maintain security during operations?	$ per time period, different cost categories	Costs of implementing security policies.
Product Size, Stability, Scope	Measures applicable to assessing the size and volatility of the security-critical aspects of a product system, for purposes of managing, resourcing and monitoring progress. Applicable to the development and maintenance of an engineered system or component. (Service provision covered in following section)			
	Scope - Security (secure system)	How much of the system requires security (at different levels)?	Secure Units Compared to Total Units	Might spend more time on units that definitely have security implications, and less on those that are believed to be not-security related.
		What is the scope of the security-critical functions, system, software? Level of criticality?	Security Requirements	Requirements Tracker
			Security-Critical Functions	System design and threat environment. Scope provides basis for estimating and monitoring progress
			Security-Critical Components	
		Scope of attack surface?	Security-Critical Interfaces	
			Security-Critical Modes	
			Security Enclaves	
		What is the rate of change of security requirements?	Security Change Workload Requirements volatility	Project Plan

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
	Scope - Security - critical Assets	What are the potential losses/ damages?	Value	Priority; level of protection required
			Damage Costs	Damage scenarios
			Security Risk Tolerance	Assurance required
	Security Criticality	What are the potential losses/ damages?	Number of critical functions Number of interfaces	
	Security Controls	Have the security controls of the system and interconnected systems been reviewed?	Percentage of total systems for which security controls have been tested and evaluated in the past year	Reference sources of imported measures
		Does management ensure that corrective actions are effectively implemented?	The average time elapsed between vulnerability or weakness discovery and implementation of corrective action	
Service Stability and Scope	Measures applicable to assessing the size and volatility of a security-critical service, given an engineered system (e.g. IT system) infrastructure, for purposes of managing, resourcing and monitoring compliance/operation. The 'size' of the security task is determined by: (1) Scope of service and systems involved (in provision of core services) (2) Size of assets that have to be protected (3) Volatility in the vulnerability aspects of the given IT systems and security policies (4) Volatility in the threat environment (covered in following section)			
	Scope - Security (secure service)	What parts of the delivered service are security-critical? What is the stability, complexity, distribution of the services?		The ISSEA MWG measures cover this area.
		How many ports?		
		How many Security Policy Requirements?		
		How many security controls?		
		Rates of change in these?		
		Rate of arrival of threat notifications, vulnerability notifications, patches etc?		
	Scope of critical assets	Size, distribution, transaction rate and communication flows related to critical assets?		Size of assets that have to be protected.

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
Environment Properties	Measures applicable to the security aspects of the environment of the system or service, especially the threat environment			
	Security Risk: Threat Agents	What are the external threat agents?	Threat Level	Standard models. Threat agent capability
			ROI for Attacker	Attacker perceived Gain & Attack Cost
		Rate of threat agent notification/ awareness	# / time period	
	External Dependencies	What external systems does this system depend on for security risk mitigation?	Externalized Risk Interfaces?	Security risk borne by external agents, systems
	Insurance	What security risks are covered by financial means?	Insured Risk	Financial risk transferred to insurer, at cost
	Personnel Security	Are duties separated to ensure least privilege and individual accountability?	Percentage of systems compliant with the separation of duties requirement	
		Is appropriate background screening for assigned positions completed prior to granting access?	Percentage of users with special access to systems who have undergone background evaluations	
	Physical and Environmental Protection	Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?	Percentage of information systems libraries that log the deposits and withdrawals of tapes	
		Is data protected from interception?	Percentage of data transmission facilities in the organization that have restricted access to authorized users	
		Are mobile and portable systems protected?	Percentage of laptops with encryption capability for sensitive files	

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
Product Quality	Measures applicable to assessing the security properties of an engineered system or component, at any indenture level or layer in a complex system.. (Service Quality is covered in following section). There are two principal phases: (1) during development: here security has to be viewed mainly in risk terms, because the system product has yet to be deployed. (2) during operations: here security can be viewed also in achieved performance terms, because the system product is being used to support the provision of services. Components may have operational performance or equivalent test data. - During Development Product Quality is assessed throughout the SDLC, with reference to planned achievements, specifications, test plans, analysis etc. Security quality manifests as acceptably low levels of faults, fault effect propagations and predicted service failures, assessed in the context of predicted threats and potential damages. The detailed form of faults, errors and failures will vary, depending on the product architecture and technologies involved. Aggregation of total system security, based on component security, is difficult. The following approach is assumed: (1) At each indenture level, 'layer' or area of the system, quality is achieved by learning from past practices, within the applicable engineering practice ('doing things right'). This is covered in the Process Performance section below. (2) Residual security risks are managed between layers, by means of requirements and provision of assessed residual risks and assurance ('doing the right thing'). Covered in this section. These measures address the 'vertical'/ aggregation aspects of security in complex systems. Quality relates to the products or services delivered between layers or development groups. Measures apply to the particular system under development. The provision of residual risk information has three aspects: (1) estimates of expected likelihoods of failures in provided services and the consequent damages; (2) confidence intervals around these expected values, expressing engineering uncertainty; (3) assurance information that provides evidence for the bases of these assessments, for the purpose of building trust between different parties. The Common Criteria framework provides one model for independent (third party) evaluation of products against defined threat models (protection profiles). - During Operations Achieved security quality manifests as acceptably low levels of faults, fault effect propagations and service failures, assessed in the context of threats and damages sustained. Here, service failures are restricted to those with root causes in the product system.			

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
	Detected Faults or defects	Have we provided sufficient info with defects to allow prioritization and root cause analysis etc – remediation – vulnerabilities?	Faults potentially security-related Latent defects	Categorized by SDLC Phase, when detected, when treated Defect classification for root cause analysis Categorization (RAG) of security relevance Correlate with testing
		Have we created any unintended security consequences with anything else we have done?	Defects traced to security practices	
		How many bad practices exist in the system code? (tools and inspections will identify some of these)		
	Security Risk: Vulnerabilities	How many known vulnerabilities exist in the system? How many have been resolved or accepted at risk, documented and transmitted to customer?	Likelihood of attack/ exploit Likelihood of successful attack	Assessment Penetration Testing Language features Consider have any known vulnerabilities gone thru a risk assmt and been treated appropriate. Theoretical vulns Emergent vulns
		In resolving non-security defects, have we introduced any security issues?		
	Security Risk: Damages/ Impacts		Impact Cost Lives, reputation, infn etc	Damage Assessments Consider infn cat Scope of potential damage
	Security Risk: Security Events		Count of, categorized Undetected events ?	Monitoring Systems (e.g. IDSs) e.g. Microsoft measures new infn cat security posture ? Attractiveness for attackers

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
	Security Risk: Responses	How predictable is the system or component, in terms of security-related faults, in the context of its intended function in providing a security-critical service?	Response success rate	Monitoring Systems Robustness Fail safe
			Risk Management Coverage to CIAA (Confidentiality, Integrity, Availability, and Accountability)	
	Assurance - Security: Test/ Analysis/ Inspections		CC EALs	Common Criteria independent tests
			SW scanning tools vulnerability density	Checks implicit in tools
			Integrated Security Assurance Case	
			Penetration Test Coverage (Exploitation, Insider/Outsider)	
Service Quality	Measures applicable to assessing the security properties of a delivered service. Security quality manifests as acceptably low levels of service failures and consequential losses. Acceptability may be defined in terms of a service level agreement or similar. Total service quality is the quality as perceived by the user, irrespective of root causes of failures. Service failures with root causes in operations (for example, a non-compliance with a policy) may be distinguished from failures due to system and software faults.			
	Performance Outcome: Events/ Incidents	How many events/incidents have occurred?	Number of intrusions Incidents by category 'near misses'	Historical performance in testing or operations
	Performance Outcome: Damages	How much damage was caused by events/incidents?	Damage costs Damage recovery time	Recovery cost monitoring systems To operator and other parties Damage may not be just $ - also loss of privacy, reputation, etc.

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
	Performance Outcome: Residual Risk	How much residual security risk exists in the delivered service? How much confidence is there in this estimate?	Residual security risk	Difficult to directly measure, but as assessed
	Performance Outcome: Effectiveness	Have I realized the benefits of my investment in security? How efficiently has the security investment been used? How efficiently have security risks been mitigated?	Return on investment ROI Response Time	Applicable to operations process
	Compliance: Security Policy	Have we followed the relevant policies?		Operational Policies
	Incident Response Capability	Is there a capability to provide help to users when a security incident occurs in the system?	Percentage of agency components with incident handling and response capability	
		Do program officials understand the risk to systems under their control and determine the acceptable level of risk?	Percentage of systems that have had risk levels reviewed by management	
	Stealth Attacks	How many stealth attacks have successfully accessed our systems? Is there evidence of modular malware in our systems, in a dormant state?		Can only be detected indirectly, perhaps.
	Service Assurance			
Process Performance: System Development	Set of measures applicable to processes that: (1) develop security-critical systems and components; (2) implement changes to systems or components. Effectiveness and efficiency with which component or system specifications, relating to security, are achieved. These measures apply to the practices that are applied to the development of a component or system, at any indenture level. These are 'horizontal' processes and focus on the creation of faults/defects/anomalies and their removal or mitigation. Application of knowledge/templates/checklists etc learnt from previous experience is important. Also effectiveness of basic methods deployed e.g. formal methods in sw devlpt.			

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
	Compliance: Legal	Have we followed the regulatory requirements?	Regulatory certification	Legal requirements
	Capability Maturity	Have we followed the standard process model?	Maturity of security practices	Audit against CMMI/ iCMM extensions, SSE-CMM
	Compliance: Best practice	Have we followed the relevant best practices?	Checklists	DISA Checklists, Security Engineering
	Compliance: Security Policy	Have we followed the relevant policies?		Development policies.
		Have I included security requirements in each out-sourcing supplier selection? (1)		
	Authorize Processing (Certification and Accreditation)	Has the system been certified/ recertified and authorized to process (accredited)?	Percentage of total systems that have been authorized for processing following certification and accreditation	
		Is the system operating on an interim authority to process in accordance with specified authority?	Percentage of systems that are operating under an Interim Authority to Operate (IATO)	
	System Security Plan	Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?	Percentage of systems with approved system security plans	
		Is the plan kept current?	Percentage of current security plans	
	System Development Life Cycle	Has a system development life cycle (SDLC) methodology been developed?	Percentage of systems that have the costs of their security controls integrated into the life cycle of the system	
		Are changes controlled as programs progress through testing to final approval?	Percentage of systems recertified if security controls are added or modified after the system was developed	
	Product Defects or Faults	Numbers of defects introduced at different SDLC stages, when corrected, rates, time intervals, regression testing		Set of metrics Jeremy Epstein – from a software developer

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
	Production, Input/Output Controls	Is there user support?	Percentage of security-related user issues resolved immediately following the initial call	
		Are there media controls?	Percentage of used media sanitized before reuse or disposal	
	Contingency Planning	Have the most critical and sensitive operations and their supporting computer resources been identified?	Percentage of critical data files and operations with an established backup frequency	
		Has a comprehensive contingency plan been developed and documented?	Percentage of systems that have a contingency plan	
		Are tested contingency/disaster recovery plans in place?	Percentage of systems for which contingency plans have been tested in the past year	
	Hardware and Systems Software Maintenance	Is access limited to system software and hardware?	Percentage of systems that impose restrictions on system maintenance personnel	
		Are all new and revised hardware and software authorized, tested, and approved before implementation?	Percentage of software changes documented and approved through change request forms	
		Are systems managed to reduce vulnerabilities?	Percentage of systems with the latest approved patches installed	
	Documentation	Is there sufficient documentation explaining how software/hardware is to be used?	Percentage of in-house applications with documentation on file	
		Are there formal security and operational procedures documented?	Percentage of systems with documented risk assessment reports	
	Security Awareness, Training, and Education	Have employees received adequate training to fulfill their security responsibilities?	Percentage of employees with significant security responsibilities who have received specialized training	

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
	Audit Trails	Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?	Percentage of systems on which audit trails provide a trace of user actions	
	Situation Awareness	Have we identified new potential threats? Have we modified our process to detect new potential threats?	Identified threats Detected potential threats	Moved from another info category - review
	Performance Outcome: Residual Risk	How much residual security risk exists in the operational system? How much confidence is there in this estimate?	Residual security risk	Difficult to directly measure, but as assessed
	Performance Outcome: Effectiveness	Have I realized the benefits of my investment in security? How efficiently has the security investment been used? How efficiently have security risks been mitigated?	Return on investment ROSI Response Time	Applicable to development process
	Performance Outcome: Security Options	Have my choices in security improvements been well timed / well spent / appropriate?	Security options – risk return	
Process Performance: Service Provision	Set of measures applicable to processes that maintain the security of a delivered service, given a system infrastructure (e.g. an IT system) subject to update, changing threat environment, and assets. Applicable to service-providing organizations and service aspects of system development organizations. Effectiveness and efficiency with which Security Policies are enacted, and a Service Level Agreement, or similar relating to security, is met.			
		| or 0 (with slash), 0 with slash = unacceptable	Site Accreditation Survey (SSAA compliance, environment)	E
	Risk Management	Is risk periodically assessed? How predictable is the service, in terms of security-related failures, in the context of a defined threat environment?	Percentage of systems that had formal risk assessments performed and documented Caveat: Aggregation can be trouble	E/SP

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
		Do program officials understand the risk to systems under their control and determine the acceptable level of risk?	Percentage of systems that have had risk levels reviewed by management	E/SP
	Personnel Security	Are duties separated to ensure least privilege and individual accountability?	of systems compliant with the separation of duties requirement	E/SP
		Is appropriate background screening for assigned positions completed prior to granting access?	of users with special access to systems who have undergone background evaluations	E/SP
	Data Integrity	Is virus detection and elimination software installed and activated?	of systems with automatic virus definition updates and automatic virus scanning	E/SP
		Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?	How many systems that perform password policy verification	E/SP
	Identification and Authentication	Are users individually authenticated via passwords, tokens, or other devices?	Percentage of systems without active vendor-supplied passwords	
		Are access controls enforcing segregation of duties?	Percentage of unique user IDs	
	Logical Access Controls	Do the logical access controls restrict users to authorized transactions and functions?	How many of users with access to security software that are not security administrators	
		Are there logical controls over network access?	How Many of systems running restricted protocols	
		If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?	How many of websites with a posted privacy policy	
	Situation Awareness	Have we identified new threats? Have we modified our process to detect new threats?	Identified threats Detected threats	

Comment [Bh2]: Physical access without account access?

Deleted: Percentage

Comment [Bh1]: The actual number is more important than the percentage

Deleted: Percentage

Deleted: Percentage

Deleted: Percentage of

Comment [Bh3]: INSERT: Is there a dedicated log server with write once media?

Comment [Bh4]: How many facto (?) authenticate?

Comment [Bh5]: Number of default passwords by account?

Deleted: Percentage

Deleted: Percentage

Deleted: Percentage

Comment [Bh6]: # of penetration not detected by IDS

Also

False positive rate changes between multiple IDs in defense in depth

Information Categories	Measurable Concepts	Questions Addressed	Prospective Measures	Notes
Technology Effectiveness	Set of measures applicable to the assessment of completed components and systems, independently of their development.			
	Security performance of a component or system that delivers a security-related function (e.g. firewall)	How effective is the system or component in providing security risk mitigation, protection, as assessed against a defined protection profile?	# systems, components assessed at a defined EAL, compared with defined security requirements.	Common Criteria
	Security performance of a component or system that delivers a function for which security is a property (data storage/ retrieval)	Is COTS and NDI software secure (including open source)?	# packages that have been formally verified against a specification.	
Customer Satisfaction AND User satistaction	Set of measures applicable to assessing security properties of a service or system, as experienced by users. E/SP			
	Customer Trust	Are my customers satisfied with achieved product security?	# events / incidents Damages incurred (cost, schedule) SURVEY	Security achieved up to the present time.
		Are my customers satisfied with predicted product security?	Assessed future security (likelihood and damage level per failure, confidence intervals for these, plus acceptability of assurance evidence)	Confidence in the level of security in the future. Confidence in the assessment of this.

Comment [Bh7]: Need a clean sheet approach

Comment [Bh8]: Need a clean sheet approach