

# Software Assurance (SwA) Checklist for Software Supply Chain Risk Management

### SwA Forum Processes and Practices Working Group December 14, 2010



- Organizations that are ready to improve their assurance capabilities may not be aware of how to begin an organized security initiative.
- Several maturity models are publicly available, but:
  - Learning curves may inhibit adoption
  - Finding the right model(s) can be time consuming
  - Selecting model components can be complicated
  - Each model has a different approach and level of granularity



- Performed a model-agnostic analysis of several publicly available maturity models
- Created a consolidated view of current software assurance goals and best practices in the context of an organized SwA initiative
- This consolidated view evolved into the SwA Checklist for Software Supply Chain Risk Management



- The crosswalk includes mappings between the SwA Checklist practices and practices identified in existing SwA maturity models and related capability maturity models.
- The maturity models mapped within the framework include:
  - Building Security In Maturity Model (BSIMM)
  - Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI) for Acquisitions
  - OWASP Open Software Assurance Maturity Model (SAMM)
  - SwA Forum Processes and Practices Working Group Assurance Process Reference Model (PRM)
  - CERT Resilience Management Model (RMM)



### SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN BSIMM

- Scientific observationbased descriptive model
- Uniquely qualified to be used as a measuring stick for software security
- Based upon analysis of the software security initiatives of 30+ organizations www.bsimm.com





- CMMI-ACQ provides guidance to acquisition organizations for initiating and managing the acquisition of products and services
- Used to guide process improvement initiatives across a project, a division, or an entire organization.

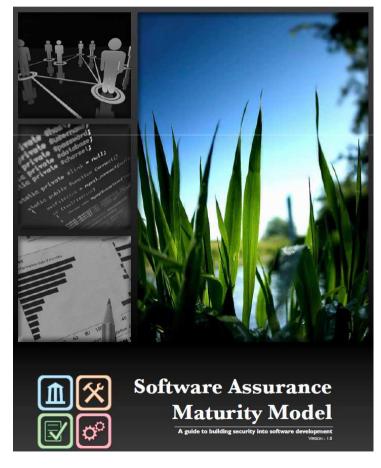
www.sei.cmu.edu/cmmi/



www.sei.cmu.edu/cmmi/



### SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN OpenSAMM



- Open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.
- Can be applied organization-wide, for a single line-of-business, or individual projects.
  www.opensamm.org



# SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN Assurance PRM

- SwA Forum Processes & Practices Working Group synthesized from the contributions of leading government and industry experts.
- Assurance for CMMI® defines the Assurance Thread for Implementation and Improvement of Assurance Practices that are assumed when using the CMMI-DEV.

#### BUILDING SECURITY IN



https://buildsecurityin.us-cert.gov/swa/proself\_assm.html



- The Assurance PRM Self-Assessment provides an assessment framework of the implementation of assurance practices
- Incorporates the Assurance PRM goals and practices
- Contains mappings to other freely available maturity models

https://buildsecurityin.us-cert.gov/swa/proself\_assm.html



SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN CERTRMM

- Process improvement model
- Addresses the convergence of security, business continuity, and IT operations



- Focus on managing operational risk and establish operational resilience
- Supplies a process improvement approach through the definition and application of a capability level scale

www.cert.org/resilience/rmm.html

### SOFTWARE ASSURANCE FORUM

#### BUILDING SECURITY IN

							Contraction of the local division of the loc	And in the second	the second second	and the second second				A DE LA CARACIÓN DE L	1 J 2 2 3 4 4
		Governance			Knowledge		1	Verification			Deploymen	t	Supp	lier Manage	ment
	Strategy	Policy	Training		Security				Risk-Based		Vulnerability		Agreement	Evaluation	Agreement
		-	-	Threat		Secure	Architecture	Code		Penetration	-	Environmen	-		-
	&	&	&	Assessment	Requirement	Design	Analysis	Analysis	Security	Testina	Managemen	t Hardening	Requirement	&	Managemen
	Metrics	Compliance	Guidance		S	beerg.			Testing		t		S	Selection	t
						Develops list of				Performs			Identifies and		
	Establishes					preferred		Develops list of		external	Identifies point		prioritizes supplier		
	Security Plan;	Identifies and		Builds and	Documents,	frameworks and		top bugs and	Performs edge /	penetration	of contact for	Maintains	dependencies;	Establishes,	Formalizes
Practices:	communicates	monitors relevant	Conducts security	maintains list of	analyzes, and	security features;	Reviews design	creates review	boundary value	testing on	incident	operational	identifies,	reviews, and	supplier
	and provides	compliance	awareness	application-	manages	explicitly applies	against security	checklists from	condition	production	response;	environment	assesses, and	distributes	relationships and
	training for the	drivers	training regularly	specific attack	functional security	security	requirements	security	testing in QA	software with	creates incident	specification	mitigates risks	solicitation	executes supplier
	plan	divers		models	requirements	principles to		requirements	process	latest	response team	specification	associated with	package	agreement
	pian					design		requiremento		techniques and	response team		supplier		
						-				mitigates			dependencies		
BSIMM	SM1.1	CP1.1	T1.1	AM1.1	SR1.1	SFD1.1	AA1.1 - AA1.3	CR1.1	ST1.1 - ST1.2	PT1.1 - PT1.2	CMVM2.1	SE1.1	SR3.1		
	-	CP1.2	T3.4	AM1.4	•	SFD1.2	SFD3.1					SE1.2			•
CMMI-	PP SG2 - SG3	OPF SG1	OT SG2	RSKM SG1- SG2	ARD SG1, SG3	ATM SG2	ATM SG1	AVER SG3	AVER SG3	AVER SG3	CAR SG1	CM SG2 - SG3	RSKM SG2-SG3	SSAD SG1	AM SG1
ACQ				-	REQM SG1	AVAL SG2	AVAL SG1- SG2			CAR SG1- SG2	OPD SG1		PP SG1		SSAD SG3
OSAMM	SM1B	PC1A	EG1A	TA1A	SR1A	SA1A	DR1B	CR1A	ST2B	ST1B	VM1A	EH1A		-	-
USAMM	-	PC1B			SR2B	SA1B		-	-		VM1B	-		-	
0014	SG 2.1	SG 3.1	SG 1.3	SG 3.2	SG 3.1	SG 3.2	SG 3.4	SG 3.4	SG 3.4	SG 3.4	SG 4.3	SG 4.3	SG 2.3	SG 2.3	SG 2.3
PRM	SG 1.3												SG 3.1		
	RTSE:SG2 - SG3	COMP:SG2	OTA:SG1-SG2	RISK:SG1-SG4	RRD:SG1-SG3	RTSE:SG1-SG2		VAR:SG2	RTSE:SG3	RTSE:SG3	VAR:SG1	ADM:SG3	EXD:SG1-SG2	EXD:SG3	EXD:SG3
RMM	MON:SG1	MON:SG1-SG2		KIM:SG6	RRM:SG1	KIM:SG2, SG6		KIM:SG6			MON:SG1	KIM:SG5	RISK:SG3 - SG6		
	THOR.COM	Establishes		Tell Placeto	TH NYLOON			Uses			inioid.com	Tal 4.0000			
		policies and			Documents,	Builds secure		automated	Integrates black		Develops	Monitors	Establishes		
	Collects and	procedures for	Conducts role-	Identifies	analyzes, and	frameworks,	Makes design	code analysis	box security	Performs	consistent	baseline	enterprise and	Evaluates	Monitors and
Practices:	tracks security	compliance with	based advanced	potential attacker	manages non-	security	reviews available	tools; requires	testing tools	periodic internal	incident	environment	assurance	solicitation	corrects supplier
	plan metrics	security plan and	application	profiles	functional security	services, and	for projects	code analysis	into QA of	white box pen	response	configuration	requirements for	responses	processes and
	based upon risk	other compliance	security training		requirements	security design		as part of	software	testing	process	changes	supplier	·	performance
		requirements				patterns		development	releases			_	agreement		
BSIMM	SM1.5	CP1.3	T2.1	AM1.3	SR1.3	SFD2.1	AA2.1	CR1.4	ST2.1	PT2.1-PT2.3	CMVM1.1	SE1.1	SR2.1, SR2.5		-
DOIMIM	SM2.1	CP3.2	-	-	-	SFD2.3	AA2.3	CR2.3	-	-	-	-	-	-	-
CMMI-	MA SG1-SG2	OPF SG2 - SG3	OT SG2	RSKM SG1- SG2	ARD SG1, SG3	ATM SG2	AVAL SG1	AVER SG3	AVER SG3	AVER SG3	CAR SG1	CM SG2 - SG3	REQM SG1	SSAD SG2	AM SG1
ACQ	PMC SG1				REQM SG1	AVAL SG2	PMC SG1-SG2				OPD SG1		ARD SG2		REQM SG1
	SM1B	PC2A	EG2A	TA1B	SR1B	SA2A	DR2A	CB2A	ST1B	ST1A	VM2A	EH2B	SR3A	-	
OSAMM	-		EG3B			SA2B	DR2B	CR2B		ST1B					
	SG 1.1	SG 1.2	SG 1.3	SG 3.2	SG 3.1	SG 3.2	SG 3.4	SG 3.4	SG 3.4	SG 3.4	SG 4.3	SG 4.3	SG 3.1	SG 2.3	SG 2.3
PRM	SG 2.2		-		-			-	-	-	-	-	-	-	SG 3.5
	MA:SG2	RTSE:SG2	OTA:SG3-SG4	RISK:SG1-SG4	COMP:SG2	RTSE:SG3		RTSE:SG3	RTSE:SG3	RTSE:SG3	VAR:SG1	ADM:SG3	EXD:SG3	EXD:SG3	EXD:SG4
RMM	MON:SG2	COMP:SG1	017/303-304	KIM:SG6	RRM:SG1	hiot:ouo	•		niae:aua	nioc:ouo	MON:SG1	KIM:SG5	BRD:SG2 - SG3	EAD:503	RRM:SG1
	MUN:SG2	COMPISI		KIIVI:SG6	BRIVI:SUI	•	•	•	- Fereleus si-h	- Derferenc	MON:SG1	KIIVI:SG5	nmD:502-503	•	HRIVI:SU1
	Drives hudgets				Duilde repository	Pequireques of		Tailors code	Employs risk- driven	Performs	Conducts root	Identifies and			
	Drives budgets based upon	Measures project	Provides security	Builds and	Builds repository of well written	Requires use of approved	Builds standard	analysis for	automated	extensive penetration	cause analysis	deploys relevant	Establishes		Evaluates and
Practices:	analysis from	compliance at	resources for	maintains abuse	testable and	security	architectural	application-	security and	testing	for incidents,	operations and	supplier	Negotiates and	accepts supplier
Flactices.	metrics	specific	coaching ł	cases and attack	reusable security	platforms and	patterns from	specific	regression	customized with	fixes all	protection tools;	agreement	selects supplier	work products
	collections	checkpoints	learning	patterns	requirements	architectures	lessons learned	concerns	testing in QA	organizational	occurrences of	performs code	agreement		work produces
	conections				requirements	aroniceotares		concerns	process	knowledge	bugs	signing			
	SM1.5	CP2.3	T1.3 - T1.4	AM2.1	SR1.2	SFD3.2	AA3.2	CB3.1	ST3.1	PT3.1-PT3.2	CMVM3.1-3.2	SE2.3	CP2.4		
BSIMM											-		CP3.2		-
	-	CP3.3	T2.4 - T2.5	AM 2.2	SR2.3										
	-		T2.4 - T2.5 OT SG2		SR2.3	CM SG1	AVAL SG2	AVEB SG3	AVEB SG3	AVEB SG3	CAR SG1-SG2	OID SG1 - SG2	SSAD SG3	SSAD SG2	AM SG1
CMMI-	PMC SG2	CP3.3 OPP SG1	T2.4 - T2.5 OT SG2	AM 2.2 RSKM SG2		CM SG1	AVAL SG2	AVER SG3	AVER SG3	AVER SG3	CAR SG1-SG2	OID SG1 - SG2	SSAD SG3	SSAD SG2	AM SG1 PPQA SG1
CMMI- ACQ	- PMC SG2 -	OPP SG1	OT SG2	RSKM SG2	-					-	-		1	SSAD SG2	AM SG1 PPQA SG1
CMMI-	PMC SG2	OPP SG1 - PC3A	OT SG2 - EG1B - EG2B	RSKM SG2 - TA2A	- - SR2A	SA3A	- DR3A	CR3A	ST1A	ST1B	VM3A	EH3A	-		PPQA SG1
CMMI- ACQ	PMC SG2 SM3A SM3B	OPP SG1 - PC3A -	OT SG2 - EG1B - EG2B EG3A	RSKM SG2 TA2A	- - SR2A -	- SA3A SA3B	- DR3A -	- CR3A -	STIA ST2A	ST1B	VM3A -	EH3A OE3B		- - -	PPQA SG1 -
CMMI- ACQ	PMC SG2	OPP SG1 - PC3A	OT SG2 - EG1B - EG2B	RSKM SG2 - TA2A	- - SR2A	SA3A	- DR3A	CR3A	ST1A	ST1B	- VM3A - SG 4.2	EH3A	-		PPQA SG1
CMMI- ACQ OSAMM	PMC SG2 SM3A SM3B SG 3.1	OPP SG1 PC3A SG 4.1	OT SG2 - EG1B - EG2B EG3A SG 1.3 -	RSKM SG2 TA2A SG 3.1	- SR2A - -	SA3A SA3B SG 3.2	DR3A -  	CR3A - 	ST1A ST2A SG 3.4	ST1B - SG3.4	- VM3A - SG 4.2 SG 3.5	EH3A OE3B SG 4.3 -	- - - - SG 2.3 -	- - 	PPQA SG1 - - - - - - - - - - - - -
CMMI- ACQ OSAMM	PMC SG2 SM3A SM3B	OPP SG1 - PC3A -	OT SG2 - EG1B - EG2B EG3A	RSKM SG2 TA2A	- - SR2A -	- SA3A SA3B	- DR3A -	- CR3A -	ST1A ST2A	ST1B	- VM3A - SG 4.2	EH3A OE3B		- - -	PPQA SG1 -



- Useful to any organization that is currently or will soon be acquiring or developing software
- Organizations can use the SwA Checklist to:
  - Guide their own development
  - Evaluate vendor capabilities
- Organizations can establish an assurance baseline using the SwA Checklist
- Learn more about current software assurance best practices
- Guide the selection of the most appropriate model components



- Currently implemented as a "hot linked" Microsoft Excel spreadsheet
- Provides a cross-reference of SwA goals and practices with side-by-side mappings to several freely available maturity models
- The consolidated format simplifies identification of the model components best suited for use



	Software Assurance Checklist for Software Supply Chain Risk management														
Domains:	s: Governance		Knowledge			Verification			Deployment			Supplier Management			
Categorie s:	Strategy Ł Metrics	Policy & Compliance	Training & Guidance	Threat Assessment	Security Requirements	Secure Design	Architecture Analysis	Code Analysis	Risk-Based Security Testing	Penetration Testing	Yulaerability Management	Environment Hardening	Agreement Requirements	Evaluation & Selection	Agreement Management
Goals:	Establishes and executes plan for ensuring software is secured throughout the supply chain	Enforces and tracks compliance with security plan policies and other compliance requirements	Fosters training and awareness programs to ensure staff can properly maintain a secure software supply chain	Performs threat modeling and maintains knowledgebase of threats to secure software supply chain	Develops and enforces security requirements that will ensure a secure software supply chain	Builds security into the software design	Reviews software designs to ensure they meet the documented assurance requirements	Analyzes code to mitigate bugs before advancing to production	Performs automated testing as part of QA process to identify flaws	Conducts penetration testing to test software from a hacker's perspective	Establishes robust processes to identify, prioritize, and fix software vulnerabilities	Protects, monitors, and manages the software environment	Manages supplier risk and documents supplier security requirements	Reviews and selects supplier(s) demonstrating sufficient risk management controls and processes to meet security requirements	Enforces, monitors, manages, and analyzes supplier performance against documented supplier security requirements
Practices:	Ertablisher Socurity Plan: communicator and eravider training for the plan	Identifier and monitorr relevant compliance driverr	<u>Conductrrecurity</u> auarener trainina reaularly	Builds and maintains list of application: specific attack models	Decuments, analyzes, and manages functional security requirements	Develoer list of preferred frameworks and rocurity features: <u>explicitly applies</u> <u>recurity principles to</u> <u>design</u>	Roviour derian against recurity requirements	Develoer list of too buar and creater revieu checkliste from recurity requiremente	Performe edae f boundary value condition tertina in CA process	Perform external constration terting on production rol tures with latert techniquer and mitigater defects	Identifier paint of contact for incident reregnere: creater incident reregnere team	Maintainr aperational environment recoification	Identifier and prioritizer rubblier dependencier: identifier, arrerer, and mitiaater rickr arreciated with	Ertablisher, review, and distributer sulisitation paskage	Enrmalizerzuselier relationzhier and executerzuselier garcementz
Statur:															
Practices:	<u>Collectr and trackr</u> Security Planmetricr <u>bareduconrick</u>	Ertablisher onlisier and pracedurer far compliance with resurity plan and other compliance requirements	<u>Conductrale-based</u> advanced application recurity training	ldentifier extential attacker ersfiler	Documents, analyzes, and manages non: functional security requirements	Builderecure frameuarke.recurity rervicer.andrecurity derianeatterne	Maker derian revieur available for eroiestr	Urer automated code analyzir tools: reauirer code analyzir ar part of development process	Integrater black box recurity terting took into QA of roftware releaser	<u>Performe ceriodic</u> internal unite box cen tertina	Develoer consistent incident resource process	Manitarr bareline environment configuration changer	Ertablishes entererise and azzurance reauisements for supplies aareements	Evaluater relicitation researcer	Manitary and correcty rupplier processor and performance
Statur:															
Practices:	Driver budgetr bared usen analyzis from metrics collections	<u>Measures espiest</u> sameliance atspecific <u>sheckepints</u>	Provider recurity recourses for coaching flearning	Buildr and maintainr abure carer and attack eatternr	Buildr knowle daebare of well-written rewrable, tertable recurity requirements	<u>Beauirer ure of</u> approved recurity elatforme and architecturer	Buildretandard architectural patterne fram legenne learned	<u>Tailorr code analyrir</u> <u>for application:</u> reesific concerne	Employerisk-driven automatedrecurity and reasonin tortina in QA process	Perform extensive senetration tertina curtomized with prognizational knowledge	<u>Conductr root caure</u> analyzir for incidentr. fixer all occurrencer of <u>buar</u>	Identifier and dealawr relevant acerationr and crotection taolr: cerfarmr caderianing	Ertablishersupelier gareements	<u>Neantiater and relectr</u> runnlier	Evaluator and acceptr rupplicrum/kornductr
Statur:															
Intro	SwA Ch	necklist 🏑	Sources 🏑	BSIMM	CMMI-ACQ	OSAMM	PRM	RMM							

- All fields are hyperlinked to specifically related areas in other tabs in the spreadsheet
- This linking allows the user to read how different models address similar assurance goals and practices



• There is a "Status" cell under each practice in which to select an implementation status.

Status:	
Practices:	Unknown Not Applicable Not Started Partially Implemented Internal Partially Implemented by Supp Partially Implemented Internal Fully Implemented Internally Fully Implemented by Supplier

• The aggregation of the status of each practice helps organizations understand their ability to execute on software assurance activities.



### SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN Baseline Summary

- After establishing a baseline, a summary displays at the bottom
- This system provides an easy-to-view dashboard for an organization's overall implementation of assurance practices

Summary:	
Not Applicable:	0
Unknown or	
Not Started:	9
Partially	
Implemented:	19
Fully	
Implemented:	17



 The SwA Checklist is available on the DHS SwA Community Resources and Information Clearinghouse website alongside the Assurance PRM Self-Assessment:

https://buildsecurityin.us-cert.gov/swa/proself\_assm.html

 The Processes and Practices Working Group welcomes feedback on your experiences using the SwA Checklist in the field.



- The SwA Forum Processes & Practices Working Group plans to add mappings to additional models and update the SwA Checklist as newer versions of mapped models are released.
- CrossTalk journal article on the SwA Checklist in March



### SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN Contacts

### Ed Wotring

Information Security Solutions, LLC ed.wotring@informationsecuritysolutionsllc.com



Sammy Migues Cigital, Inc smigues@cigital.com

