Members of the Software Assurance (SwA) Processes and Practices (P&P) Working Group (WG) performed a model-agnostic analysis to determine how the maturity models listed below help organizations address assurance goals and practices and to determine where the models converge and diverge. This analysis of the mappings between the models revealed a high degree of agreement. This analysis evolved into the SwA Checklist for Software Supply Chain Risk Management. Organizations can use the SwA Checklist to determine process improvement opportunities and establish a baseline from which to benchmark their capabilities.

Building Security In Maturity Model (BSIMM2), version 2
www.bsimm.com
It's possible to build a software security maturity model theoretically by waxing philosophic on what others should do. Or one could build a maturity model by documenting what a set of motivated organizations have already done successfully. The latter approach is both scientific and grounded in the real world, and it is the one followed to build BSIMM.

The Building Security In Maturity Model (BSIMM2 <http://bsimm2.com>, pronounced "bee simm") is an observation-based scientific model directly describing the collective software security activities of thirty software security initiatives listed in *Table 1 – Security Initiatives Included in the BSIMM2* (below).

Adobe	AON	Bank of America	Capital One	The Depository Trust & Clearing Corporation (DTCC)
EMC	Google	Intel	Intuit	Microsoft
Nokia	QUALCOMM	Sallie Mae	Standard Life	SWIFT
Symantec	Telecom Italia	Thomson Reuters	VMware	Wells Fargo

Table 1 – Security Initiatives Included in the BSIMM2

Three experienced software security experts created BSIMM2: Dr. Brian Chess, Chief Scientist and co-founder of Fortify Software; Dr. Gary McGraw, Chief Technology Officer of Cigital; and Sammy Migues, Principal and Director of Knowledge Management at Cigital (and co-author of this article).

BSIMM2 is uniquely qualified to be used as a measuring stick for software security. As such, it is useful for comparing software security activities observed in a target firm to those activities observed among the thirty firms (or various subsets of the thirty firms) in the model. A direct comparison using the BSIMM2 is an excellent tool for devising software security strategy.

In contrast with prescriptive approaches to software security, the BSIMM2 is directly descriptive. That is, it does not tell you what you should do; instead, it tells you what other organizations are actually doing. As a descriptive model built with data from 30 software security initiatives, BSIMM2 accumulated a number of observed facts shared below.

BSIMM2 describes the work of 635 people whose firms have a collective 130 years of experience working on software security. On average, the target organizations have practiced software security for four years and five months (with the newest initiative being three months old and the oldest initiative being fourteen years old in September 2009). All thirty agree that the success of their program hinges on having an internal group devoted to software security—the Software Security Group (SSG). SSG size on average is 21.9 people (smallest 0.5, largest 100, median 13) with a "satellite" of others (developers, architects and people in the organization directly engaged in and promoting software security) of 39.7 people (smallest 0, largest 300, median 11). The average number of developers among our targets was 5061 people (smallest 40, largest 30,000, median 3000), yielding an average percentage of SSG to development of just over 1%.

Carnegie Mellon University (CMU)/Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI) for Acquisitions, version 1.2
www.sei.cmu.edu/cmmi/index.cfm
"The CMMI Product Suite was developed by the CMMI Product Team, a team of process improvement experts from the government, industry, and the SEI, to improve on the existing Software Capability Maturity Model (SW-CMM) released in 1991. The CMMI Steering Group, leaders of the CMMI Product Team, realized that the best practices outlined for software development could be merged into a single framework that organizations could use for enterprise-wide process improvement initiatives. In 2000, the team published the original CMMI model, training, and appraisal method, which incorporated software and systems engineering. The model was also designed to support the future integration of other disciplines."[i]

"CMMI is a process improvement approach that provides organizations with the essential elements of effective processes that ultimately improve their performance. CMMI can be used to guide process improvement across a project, a division, or an entire organization. It helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes."[ii]

"CMMI for Acquisition (CMMI-ACQ) is based on the CMMI Framework. CMMI for Acquisition (CMMI-ACQ) provides guidance to acquisition organizations for initiating and managing the acquisition of products and services. The model focuses on acquirer processes and integrates bodies of knowledge that are essential for successful acquisitions."[iii]

Open Web Application Security Project (OWASP) Open Software Assurance Maturity Model (SAMM), version 1.0
www.opensamm.org
"The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.

SAMM was defined with flexibility in mind such that it can be utilized by small, medium, and large organizations using any style of development. Additionally, this model can be applied organization-wide, for a single line-of-business, or even for an individual project.

As an open project, SAMM content shall always remain vendor-neutral and freely available for all to use."[iv]

Software Assurance (SwA) Forum Processes and Practices (P&P) Working Group (WG) Assurance Process Reference Model, September 2010
https://buildsecurityin.us-cert.gov/swa/downloads/20100922_PRM_Practice_List.pdf
The Assurance Process Reference Model contains a set of assurance goals and supporting practices that the SwA Forum P&P WG synthesized from the contributions of leading government and industry experts.[v] The Process Reference Model goals and practices align with the CMMI framework.

Carnegie Mellon University/CERT Resiliency Management Model, version 1.0
www.cert.org/resilience/rmm.html
The development of the CERT® Resiliency Management Model began during CERT's development and deployment of the OCTAVE® methodology, which was focused on improving an organization's involvement in managing information security risks. CERT realized that organizations often view security as a technical specialty not usually associated with other activities such as business continuity and IT operations management—all of which are focused on managing operational risk and sustaining operational resiliency. Absent this important business driver, it is difficult to position security (or business continuity planning) as an enabler of an organization's strategy, much less an activity that is worthy of the investment of limited resources such as capital and people.

CERT codified a draft process definition for operational resiliency management processes called the Resiliency Engineering Framework (REF). The framework described the range of processes that characterize the organizational capabilities necessary to actively direct, control, and manage operational resiliency. This framework has been used by Financial Services Technology Consortium organizations to benchmark their performance against the framework to characterize industry performance, validate the framework, and begin process improvement efforts. Along with this benchmarking activity, CERT began developing an appraisal method based on the SCAMPI appraisal method known as the RMM CAM (capability appraisal method).

The CERT Resiliency Management Model is a capability model for operational resiliency management. It is a process improvement model that addresses the convergence of security, business continuity, and IT operations to manage operational risk and establish operational resiliency. The RMM supplies a process improvement approach to operational resiliency management through the definition and application of a capability level scale that expresses increasing levels of process improvement.

[i] Software Engineering Institute | Carnegie Mellon University. (2010).*CMMI: A Short History.* Available: http://www.sei.cmu.edu/library/abstracts/brochures/cmmihistory.cfm. Last accessed 25th Oct 2010.

[ii] Software Engineering Institute | Carnegie Mellon University. (2010).*CMMI Overview.* Available: http://www.sei.cmu.edu/cmmi/. Last accessed 25th Oct 2010.

[iii] Software Engineering Institute | Carnegie Mellon University. (2010).*CMMI for Acquisition.* Available: http://www.sei.cmu.edu/cmmi/tools/acq/index.cfm. Last accessed 25th

[iv] OWASP. (2010). *OpenSAMM.* Available: http://www.opensamm.org/. Last accessed 25th Oct 2010.

[v] Software Assurance Community. (2010). Software Assurance (SwA) Self-Assessment. Available: https://buildsecurityin.us-cert.gov/swa/proself_assm.html. Last accessed 25th Oct 2010.