Ensuring Your Development Processes Meet Today's Cyber Challenges

Mary Beth Chrissis, Carnegie Mellon University
Mike Konrad, Carnegie Mellon University
Michele Moss, Booz Allen Hamilton

Abstract. While security in the physical world can be addressed using controls such as guns, gates, and guards, the virtual world requires other mechanisms to ensure the confidentiality, availability, and integrity of products and services. Much of what today's products, services, infrastructures, and institutions do is automated by software, thereby increasing our dependence on how safety and security are addressed in the virtual world. As software continues to evolve and we find new ways to leverage the virtual world in our day–to-day activities, the volume of and our reliance on software grows exponentially. Therefore, it is increasingly important to have confidence that products operate as intended and only as intended to ensure the resilience and reliability of the functions they support. Much of software is acquired forcing consideration of these critical qualities into the supply chain. Achieving such confidence ultimately relies on good system and software engineering knowledge, processes, and technology. Fortunately, many resources are available. This article provides a brief survey of some of these resources, such as process capability frameworks, secure lifecycle practices, and implementation approaches.

Introduction

Global markets, funding, and shareholder commitments often drive companies to get their products and services out to the market quickly. However, ignorance of vulnerabilities, heuristics, and biases [1] result in exploitable weaknesses that may affect the safety and security as well as the reputation of products. It is the market demand for newer, faster, and cooler that drives the pace of technology. However, software developers make it happen. We find a gap in security and safety in the products today because of the lack of both market requirements and developer skills. Much of software is acquired forcing consideration of these critical qualities into the supply chain.

Today consumers expect products to have safety and security built in. They take such quality attributes[1] for granted. However, over half of the 240 companies surveyed in a recent Forrester study reported at least one web application security incident since last year. The most frequently cited causes were misused default password accounts, SQL injection-related vulnerabilities, and security misconfigurations [2]. This is particularly challenging since many organizations acquire software products and must ensure their expectations are met through acquisition where requirements and design expectations must be clearly conveyed.

Developers initially tend to focus exclusively on product functionality, treating safety and security as something to test at the end of product development. In other words, they miss the opportunity to identify and mitigate vulnerabilities early in the development lifecycle. If problems are not detected and addressed early, they frequently are too expensive to fix when discovered later in the lifecycle.

The Threat Landscape

According to the October 2011 report from the Office of the National Counterintelligence Executive to Congress on Foreign Economic and Industrial Espionage, "Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect U.S. technological and economic information will continue at a high level and will represent a growing and persistent threat to U.S. economic security. The nature of the cyber threat will evolve with continuing technological advances in the global information environment [3]."

The report further identified specific technology areas (i.e., information and communications technology, military technologies, clean technologies, advanced materials and manufacturing techniques, healthcare, pharmaceuticals, and agricultural technology) and types of business information (i.e., energy and other natural resources, business deals, and macroeconomic information) as targets of foreign attack.

For the past five years, Verizon has published its annual Data Breach Investigations Report. In these reports, Verizon analyzes the causes of breaches and provides recommendations for how they could have been prevented. These studies provide valuable insight into the level of complexity in today's attacks as well as organizational behaviors that either enable or hinder attacks.

	2011 Verizon Data Breach Investigations Report [4]	2012 Verizon Data Breach Investigations Report [5]
What commonalities exist?	▪ 83% of victims were targets of opportunity ▪ 92% of attacks were not highly difficult ▪ 86% of incidents were discovered by a third party ▪ 96% of breaches were avoidable through simple or intermediate controls	▪ 79% of victims were targets of opportunity (-4%) ▪ 96% of attacks were not highly difficult (+4%) ▪ 92% of incidents were discovered by a third party (+6%) ▪ 97% of breaches were avoidable through simple or intermediate controls (+1%)
How do breaches occur?	▪ 50% utilized some form of hacking ▪ 49% incorporated malware *(lower percentages included physical attacks, privilege misuse, and social tactics)*	▪ 81% utilized some form of hacking (+31% increase) ▪ 69% incorporated malware (+20% increase) *(lower percentages included physical attacks, privilege misuse, and social tactics)*

Table 1. Data from Verizon Data Breach Investigations Report

Good Development Practice

To assure safe and secure products and services, good development practice must be used from the beginning. Safety and security should be viewed as enablers, not constraints because they impact an organization's goals and reputation. One general principle that facilitates stakeholders to focus on safety and security throughout the software lifecycle is to use iterative, continuous, and evolutionary approaches to direct product acquisition, development, and delivery. Such approaches provide developmental agility, which is helpful to effectively address high uncertainty and to respond to unanticipated change.

Good development practice that is specific to safety and security includes:

• Provide early and careful consideration to quality attributes. Experience shows that safety and security cannot be added at the end of the development lifecycle [6]. Rather, products need

to be developed with safety and security in mind from inception through disposal.

- Provide early and careful attention to an architecture that effectively addresses tradeoffs among quality attributes and product functionality.
- "Step to the left." Most human error can be best detected shortly after it is committed (and it is more cost-effective to remove). Organizations need to make the most of this principle when detecting errors in individual, team, and organizational processes.
- Use processes that encourage careful consideration of how errors may be introduced, detected, removed, and prevented. For example, explicit task kickoff and inspection checklists can be incorporated at multiple points in the software development lifecycle (SDLC) to sustain attention on common error patterns affecting quality. Also, requirements elicitation, architecture, risk management, and decision analysis processes (and thus software development teams) should encourage explicit attention to safety and security (as well as other critical quality attributes).
- View safety and security as an enabler of the organization's core mission and objectives and not as a constraint on creativity and innovation. Make sure these attributes are commonplace in the development of all products and services.
- Use reviews and code analysis tools to reduce code-induced vulnerabilities hereby developing higher quality code.
- Be informed; what you do not know can kill you. A team's overconfidence is an attacker's best friend. Most exploitable errors are not the result of a lack of creativity or motivation but the lack of knowledge about vulnerabilities and human oversights. Better knowledge, processes, and technology can help overcome these weaknesses and the limits of our self-awareness [1]. Learn to think like an attacker.

Changing Technology

Opportunities and challenges arise with our ever-increasing reliance on technology. Digital thievery and espionage are concerns that organizations have to think about for their employees. The nature of cyber threats is changing at an alarming rate. You must commit to knowing as much about security as the attackers know to hope to stay ahead of them. Learn what resources are available and weave it into your learning and business processes. Your development practices must consider security issues as they relate to technology as well as to what others have learned and are sharing about safety and security.

According to a Forrester study, "ROI was greater for those who employed a coordinated, prescriptive approach [7]."

Unfortunately, many organizations are unable to communicate the return on investment effectively enough to gain management support in driving the adoption of more secure practices. Lack of management support and resistance to change is a barrier to the adoption of secure development methodologies.

In a more recent Forrester study, challenges contributing to the volume of insecure software included [2]:

- Developers being unable to keep pace with the volume of code they produce.
- Struggles to build the business case for additional funding.
- The lack of adequate tools.

Diversity of Resources

Do not limit yourself to the perspectives offered by only one process improvement model. As George Box is famous for saying, "All models are wrong but some are useful [8]." Models often become more useful when used in aggregate. Process improvement can and should incorporate knowledge of superior practice and vulnerabilities. Process measurement can help to determine the effects of particular development practices, making both cause and effect more salient, and elevating the state of software programming from ad-hoc practices toward evidence-based software development.

The DHS, NIST and the DoD are tackling this problem with their Software Assurance (SwA) working groups and forums, which seek to engage multiple communities working together to develop solutions and guidelines that reduce software vulnerabilities, minimize exploitation, and improve the routine development and deployment of trustworthy software products. Together, these activities will enable more secure and reliable software that supports mission requirements across enterprises and the critical infrastructure.

It is important to be aware of activities associated with safety and security and to ensure your organization has the capability to achieve your software assurance goals. To help with this awareness, the DHS SwA Processes and Practices Working Group has synthesized the contributions of leading government and industry experts into the set of high-level goals and supporting practices shown in Figure 1. Using these practices, organizations can identify their assurance practices implementation baseline.

The Assurance Process Reference Model [9] addresses assurance in the organization from executive to developer. It can be used to help organizations conduct a gap analysis of their existing practices versus industry recognized security practices. The results of the gap analysis can then be used to prioritize and track SwA implementation efforts.

What CMMI Says About Security

CMMI® models reflect what leading organizations do to acquire, develop, and sustain software-intensive products and services. It is not surprising that safety and security are addressed implicitly (and sometimes, explicitly) in CMMI models.

Safety and security are regarded as quality attributes in CMMI models. This term is mentioned extensively in the Acquisition Engineering process areas of the CMMI for Acquisition model [10], the Engineering process areas of the CMMI for Development model [11], and the Service System Development process area of the CMMI for Services model [12]. In particular, CMMI for Development includes coverage of quality attribute requirements (and thus safety and security requirements).

Safety and security are addressed at an abstract level. Such coverage makes sense in a CMMI model because it is rare that products need to be only safe or secure. Instead, desired quality attributes are addressed through careful architecture evaluation and tradeoffs. This more holistic treatment of quality attributes is essential to effective product design and is addressed in the 2011 SEI Webinar Capability Maturity Model Integration V1.3 and Architecture-Centric Engineering [6].

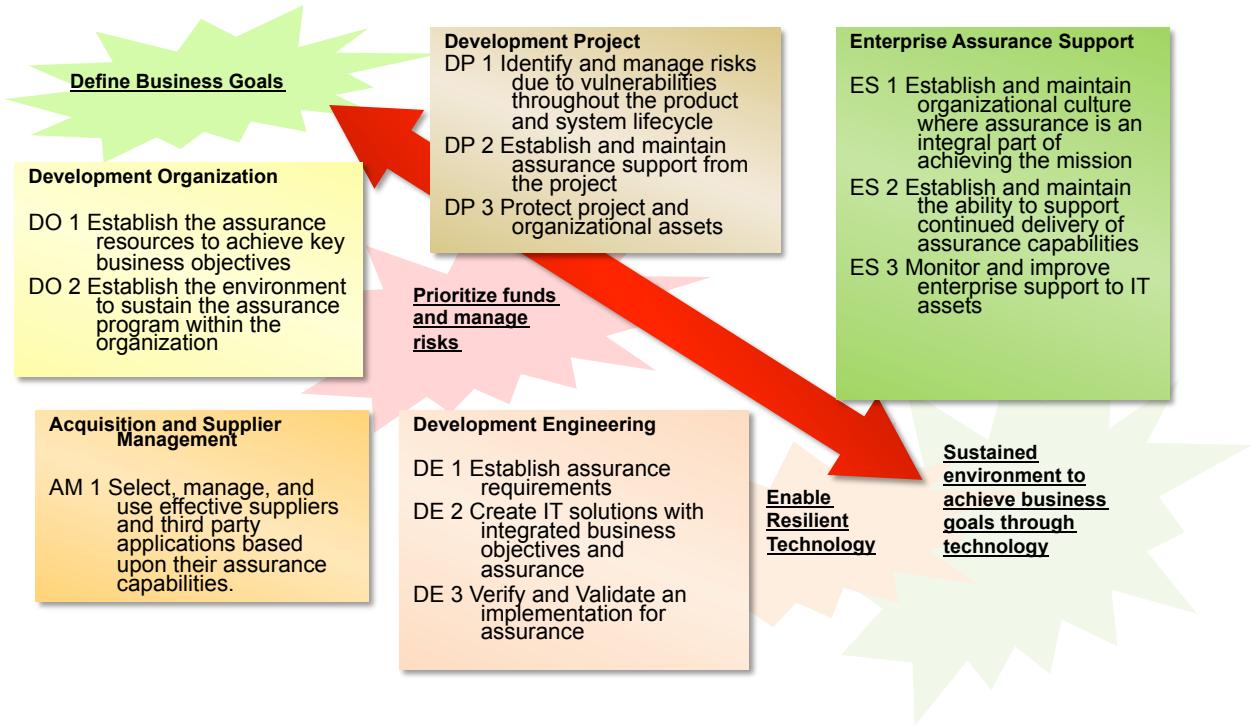

Figure 1. The Assurance Process Reference Model

Security (and sometimes safety) is explicitly covered in CMMI in the following:

- Example standards that are applicable to the organizational processes as listed in the Organizational Process Focus process area.
- A special section of the References that addresses Information Assurance/Information Security Related Sources.
- A discussion of information system vulnerabilities that appears in the Measurement and Analysis process area.
- Work environment standards in the Organizational Process Definition and Integrated Project Management process areas.
- Example quality attributes in the Engineering process areas.
- As a strategic consideration in the Project Planning and Work Planning process areas.
- Requirements and procedures that are considered as part of data management practices.

What Does This Imply?

CMMI addresses the critical broader (system) view of product and service scope, functionality, and quality attributes and how attention to all of these are necessary to make appropriate decisions and tradeoffs as the product or service is engineered and developed. However, CMMI does not provide specific guidance about individual quality attributes or information about their relationships. Safety and Security are addressed in an informative, not normative, manner. You must look elsewhere for explicit guidance about what to do in your organizational, team, or individual processes about safety and security because CMMI is relatively silent when your focus shifts from the overall balance of quality attributes to individual quality attributes.

What Additional Practices Help to Build Safe and Secure Products?

In recent years, multiple frameworks were developed that explicitly focus on practices and guidance for addressing safety and security. These frameworks can be grouped into three categories:

- Process capability frameworks.
- Secure lifecycle practices.
- Implementation approaches.

Process capability frameworks include:

- Resilience Management Model–a model that addresses converging security, business continuity, and IT operations in support of operational risk management [13].
- Assurance Process Reference Model–a model that synthesizes the contributions of leading government and industry experts into a set of high-level goals and practices to address software assurance (Figure 1) [9].
- Assurance for CMMI–a thread of assurance practices that can be overlaid on an existing CMMI implementation.[2]
- +Safe and +Secure[3]–white papers that extend CMMI models by providing a set of process areas specific to safety and security [14].

References for secure lifecycle practices include:

- Microsoft Security Development Lifecycle–a software development security assurance process consisting of security practices grouped into 7 phases: training, requirements, design, implementation, verification, release, and response [15].
- SAFECode–a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware, and services[4]

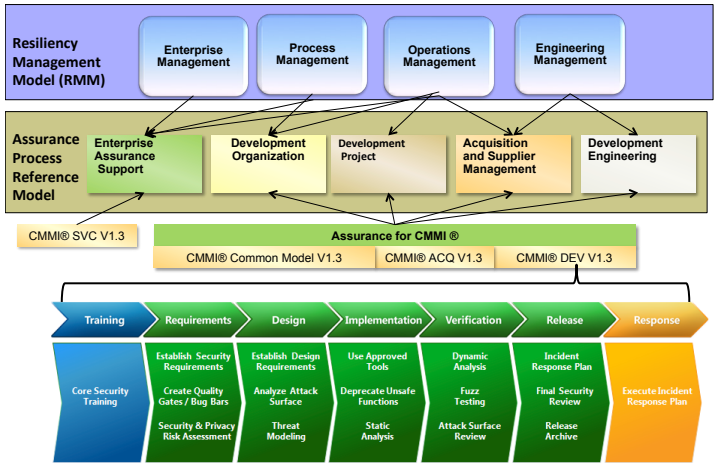

Figure 2. Configuration of Resources Addressing Process Improvement, Quality, and Security

Implementation approaches include.

- Open Software Assurance Maturity Model–an open framework that helps organizations to formulate and implement a strategy for software security that is tailored to the specific risks facing the organization [15].
- Building Security In Maturity Model–a descriptive model that describes the specific activities that organizations can engage in to improve and mature their software security posture [16].
- TSP Secure–an extension of the SEI Team Software Process (TSP) methodology that achieves the development of secure software systems by incorporating the planning, process, quality, measurement, and tracking frameworks of TSP and generating the practices and artifacts required to satisfy a maturity level 3 appraisal [17, 18].
- CERT Secure Coding Standards–a wiki-based website that supports a broad-based community of more than 500 contributors, including security researchers, language experts, and software developers [19].
- Open Web Application Security Project–an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted as well as to provide tools, documents, forums, and chapters free to anyone interested in improving application security [15].
- Build Security In–a collaborative effort that provides practices, tools, guidelines, rules, principles, and other resources that software developers, architects, and security practitioners can use to build security into software during every phase of its development [20].
- Strengthening Ties between Process and Security–a summary of key accomplishments in linking security, the SDLC, and process improvement, including an industry-led initiative to harmonize security practices with CMMI, the use of assurance cases, and NIST security considerations in the SDLC [21].
- Security Quality Requirements Engineering–a process model that provides a means for eliciting, categorizing, and prioritizing security requirements for information technology systems and applications [22].
- Correctness by Construction–a method of building software with demonstrable integrity for security- and safety-critical applications by combining formal methods and Agile development [23].

The challenge that many organizations face is defining their business goals and objectives with respect to safety and security. These goals and objectives, along with organizational policies and processes, are critical to identifying the regulations, standards, and best practices that are needed to enable organizations to build safe and secure products. It is important to tailor one or more frameworks, such as CMMI, to provide both a foundation and the flexibility for organizations to respond to internally or externally driven changes in business goals and objectives. Figure 2 illustrates how existing resources fit together to address process improvement, product quality, and security.

Summary

With the ever-increasing reliance on safety and security in products and services, CMMI provides a needed starting point, but it is not sufficient. A learning, knowledgeable, and resource-aware mindset is also required. A variety of approaches and tools are available to help you be successful. Very little of these approaches and tools are rocket science but their use requires a commitment by the organization. For a software product acquired through a supply chain, the acquisition mechanisms need to incorporate effective supply chain risk management to ensure the supplying organization is performing critical processes and practices.

As a starting point, identify the policies, standards, and business objectives that will drive excellence in your organization. CMMI and other lifecycle standards (e.g., ISO/IEEE 15288) provide the foundation and flexibility to build safety and security into an organization's lifecycle processes. You can then identify which of the available resources will best drive development of safe and secure products and services in your organization.

Process and product assessments are valuable to understanding potential vulnerabilities and risks. Organizations need to explicitly link their objectives to the assessments to use them effectively. The assessment results can help in the evaluation of resources that help in developing better products and services. There are many different approaches for addressing safety and security; no single approach addresses the needs of all audiences and organizations. The challenge for you is to pick the approaches that work best in your respective environments. This article provides an overview of some of the resources available because today most organizations are not taking advantage of the guidance that is freely available.

Acknowledgements:

We wish to thank Joe Jarzombek of the DHS; Don Davidson of the DoD; and Carol Woody of SEI, Carnegie Mellon University for encouraging us to write this article and for their helpful suggestions. Also, thanks to Winfried Russwurm and Peter Panholzer of Siemens AG for their work with +SECURE, and Stephanie Shankles of Booz Allen Hamilton for her review. Finally, thank you to Sandy Shrum, our editor, for improving our prose to say what we wanted more eloquently.

Disclaimer:

CMMI® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

NOTES

1. The term quality attributes is defined in CMMI models as "A property of a product or service by which its quality will be judged by relevant stakeholders. Quality attributes are characterizable by some appropriate measure. Quality attributes are non-functional, such as timeliness, throughput, responsiveness, security, modifiability, reliability, and usability. They have a significant influence on the architecture."
2. A pilot version of Assurance for CMMI was released in March 2009. Assurance for CMMI V1.3 has not yet been published.
3. Siemens AG, Corporate Technology released a draft report entitled +SECURE, V1.3, A Security Extension to CMMI-DEV, V1.3 in March 2012.
4. SAFECode, whose members include Adobe, EMC Corporation, Juniper Networks, Inc., Microsoft Corporation, Nokia, SAP AG, Siemens AG, and Symantec Corporation, displays its work on their website, <http://www.safecode.org>.

REFERENCES

1. Kahneman, Daniel. Thinking, Fast and Slow. New York: Farrar, Straus and Giroux 2011.
2. Forrester Research, Inc. Half of Companies Surveyed Report Web Application Security Problems. <http://www.networkworld.com/news/2012/091812-web-application-security-262520.html> (2012).
3. Office of the National Counterintelligence Executive (ONCIX). ONCIX Reports to Congress: Foreign Economic and Industrial Espionage.
4. Verizon, 2011 Data Breach Investigations Report, A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit, <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf> (2011)
5. Verizon, 2012 Data Breach Investigations Report, A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service, <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf> (2012)
6. Jones, Lawrence G. & Konrad, Michael D. Capability Maturity Model Integration V1.3 and Architecture-Centric Engineering.
7. Forrester Research, Inc. State of Application Security. <http://www.microsoft.com/en-us/download/details.aspx?id=2629> (2011).
8. Box, George E. P. & Draper, Norman Richard. Empirical Model-Building and Response Surfaces.
9. Department of Homeland Security, Assurance Process Reference Model (PRM), <https://buildsecurityin.us-cert.gov/swa/proself_assm.html> (2010)
10. Gallagher, Brian; Phillips, Mike; Richter, Karen; & Shrum, Sandy. CMMI-ACQ: Guidelines for Improving the Acquisition of Products and Services, 2nd Edition. Boston: Addison-Wesley, 2011.
11. Chrissis, Mary Beth; Konrad, Mike; & Shrum, Sandy. CMMI: Guidelines for Process Integration and Product Improvement, Third Edition. Boston: Addison-Wesley, 2011.
12. Forrester, Eileen; Buteau, Brandon; & Shrum, Sandy. CMMI for Services: Guidelines for Superior Service, 2nd Edition. Boston: Addison-Wesley, 2011.
13. Caralli, Richard A.; Allen, Julia H.; Curtis, Pamela D.; White, David W.; & Young, Lisa R. CERT Resilience Management Model, Version 1.0.
14. Defense Materiel Organization, Australian Department of Defense. +SAFE, V1.2: A Safety Extension to CMMI-DEV, V1.2
15. The Open Web Application Security Project. <https://www.owasp.org/> (2012).
16. McGraw, Gary et al. Building Security In Maturity Model. <http://www.bsimm.com/> (2012).
17. CERT. TSP-Secure. <http://www.cert.org/secure-coding/secure.html> (2010). [Davis 2009]
18. Davis, Noopur; Miller, Phillip L.; Nichols, William R.; & Seacord, Robert C. TSP Secure. <http://www.sei.cmu.edu/tspsymposium/2009/2009/DAY%203%20315%20PM%20TSP%20Secure.pdf> (2009).

ABOUT THE AUTHORS

Mary Beth Chrissis of the Software Engineering Institute (SEI), Carnegie Mellon University, is working with VA Health Systems to create a knowledge management system. She developed capability maturity models and training and co-authored multiple books and papers on process improvement. Chrissis chaired the CMMI Configuration Control Board, managed the CMMI Training Team, and instructs SEI courses. She received her BS from Carnegie Mellon University and pursued a MS in Computer Science from Johns Hopkins University.

SEI, Carnegie Mellon University
Phone: 412-268-5757
E-mail: mb@sei.cmu.edu

Dr. Mike Konrad of the Software Engineering Institute at Carnegie Mellon University leads two research efforts: one characterizing the economics of preventing vulnerabilities and the other orchestrating early software lifecycle activities across stakeholders. Previously, Mike served as the manager of SEI's CMMI Modeling Team (1994-2012) and as the CMMI chief architect. Mike has also worked with several software companies and universities. Mike obtained his Ph.D. in Mathematics in 1978 from Ohio University.

SEI, Carnegie Mellon University
Phone: 412-268-5813
E-mail: mb@sei.cmu.edu

Michele Moss of Booz Allen Hamilton, is a recognized thought leader in the integration and benchmarking of assurance practices. She is co-chair of the Department of Homeland Security (DHS) Software Assurance Working Group on Processes & Practices. She represents Booz Allen within the U.S. International Committee for Information Technology Standards Cyber Security 1 (CS1) technical committee and the U.S. Technical Advisory Group (TAG) for ISO/IEC JTC1/SC7. She is the liaison from SC7 TAG to CS1.

Booz Allen Hamilton
Phone: 703-377-1254
E-mail: moss_michele@bah.com

REFERENCES (continued)

19. CERT. CERT Secure Coding Standards. <https://www.securecoding.cert.org/confluence/display/seccode/CERT+Secure+Coding+Standards> (2012).
20. Department of Homeland Security. Build Security In: Setting a Higher Standard for Software Assurance. <https://buildsecurityin.us-cert.gov/bsi/home.html> (2012).
21. Woody, Carol. Strengthening Ties Between Process and Security. <https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/sdlc/1049-BSI.html> (2008).
22. Mead, Nancy R.; Hough, Eric; & Stehney II, Ted. Security Quality Requirements Engineering. <http://www.sei.cmu.edu/library/abstracts/reports/05tr009.cfm> (2005).
23. Amey, Peter. Correctness by Construction. <https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/sdlc/613-BSI.html> (2006).