Deriving Software Security Measures from Information Security Standards of Practice

Julia Allen
Christopher Alberts
Robert Stoddard

February 2012

This material is based upon work funded and supported by the United States Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

This report was prepared for the

Contracting Officer
ESC/CAA
20 Shilling Circle
Building 1305, 3rd Floor
Hanscom AFB, MA 01731-2125

Table of Contents

Introduction

This white paper describes an approach for deriving measures of software security from well-established and commonly used standard practices for information security. This work was performed as part of the Software Engineering Institute's Software Security Measurement and Analysis (SSMA) project. It is an initial demonstration of how SSMA-defined software security drivers (refer to *Risk-Based Measurement and Analysis: Application to Software Security)* can be used in concert with practices and standards to derive meaningful measures of software security [Alberts 2012]. Drivers are critical factors that have a strong influence on the outcome or the result, in this case, the security of software. Measures that have been derived based on software security drivers can then be used within the Integrated Measurement and Analysis Framework (IMAF) for Software Security to determine the extent to which specific practices contribute to the development and acquisition of more secure software. The Framework is described in *Integrated Measurement and Analysis Framework for Software Security, Security Measurement and Analysis,* and *Risk-Based Measurement and Analysis: Application to Software Security* [Alberts 2010; Alberts 2011; Alberts 2012].

The information security practice standard that is used to demonstrate this approach is the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53 *Recommended Security Controls for Federal Information Systems and Organizations* [NIST 2010]. This standard was selected due to its broad applicability and use within U.S. federal government agencies and their supporting contractor community and software supply chain. The SSMA Project team also used a similar approach to determine measures for selected software security practices in ISO 27002 [ISO 2005].

This work has been performed within the context of the IMAF documented in *Risk-Based Measurement and Analysis: Application to Software Security* [Alberts 2012]. To gain a fuller understanding of this white paper's potential value and use, the authors highly recommend that readers become familiar with the Framework, particularly the discussion of software security drivers and how they are used (Section 4 and the Appendix).

Approach

NIST 800-53 has 18 families of controls, which are grouped into three classes as shown in Table 1. Each family has between 4 and 34 individual controls. For the purposes of this research, the authors selected the System and Services Acquisition (SA) and System and Information Integrity (SI) control families as the most relevant when addressing software security. The SA controls are shown in Table 2, and the SI controls are shown in Table 3. The 14 SA controls and the 13 SI controls were analyzed to derive software security measures that are applicable to the SA and SI control families.

Identifier	Family	Class	Number of Controls
CA	Security Assessment and Authorization	Management	6
PL	Planning	Management	5
PM	Program Management	Management	11
RA	Risk Assessment	Management	4
SA	System and Services Acquisition	Management	14
AT	Awareness and Training	Operational	5
CM	Configuration Management	Operational	9
CP	Contingency Planning	Operational	9
IR	Incident Response	Operational	8
MA	Maintenance	Operational	6
MP	Media Protection	Operational	6
PE	Physical and Environmental Protection	Operational	19
PS	Personnel Security	Operational	8
SI	System and Information Integrity	Operational	13
AC	Access Control	Technical	19
AU	Audit and Accountability	Technical	14
IA	Identification and Authentication	Technical	8
SC	System and Communications Protection	Technical	34

Table 1: NIST 800-53 Control Families and Classes

SA-1	System and Services Acquisition Policy and Procedures
SA-2	Allocation of Resources
SA-3	Life Cycle Support
SA-4	Acquisitions
SA-5	Information System Documentation
SA-6	Software Usage Restrictions
SA-7	User-installed Software
SA-8	Security Engineering Principles
SA-9	External Information System Services
SA-10	Developer Configuration Management
SA-11	Developer Security Testing
SA-12	Supply Chain Protection
SA-13	Trustworthiness
SA-14	Critical Information System Components

Table 2: NIST 800-53 System and Services Acquisition Controls

SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-4	Information System Monitoring
SI-5	Security Alerts, Advisories, and Directives
SI-6	Security Functionality Verification
SI-7	Software and Information Integrity
SI-8	Spam Protection
SI-9	Information Input Restrictions
SI-10	Information Input Validation
SI-11	Error Handling
SI-12	Information Output Handling and Retention
SI-13	Predictable Failure Prevention

Table 3: NIST 800-53 System and Information Integrity Controls

The approach used to derive measures of software security from SA and SI controls comprised the following steps. Below we use SA-2 Allocation of Resources as an example to illustrate how each step is performed. The results of this approach for all SA and all SI controls appear as a series of tables in the Appendix.

1. Using NIST 800-53 Revision 3 and its online database, review and fully analyze each SA and SI control description, supplemental guidance, and control enhancements. Review cited references as required.

   SA-2 Allocation of Resources states the following:

   The organization

   a) Includes a determination of information security requirements for the information system in mission/business process planning

b) *Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process*

c) *Establishes a discrete line item for information security in organizational programming and budgeting documentation.*

2. Keeping in mind that the focus for this research is software security (not information or information system security), make an initial determination of the software security drivers that are most relevant for software component aspects of the control. The 17 software security drivers used for this research are summarized in Table 4 and described more fully in *Risk-Based Measurement and Analysis: Application to Software Security* [Alberts 2012].

Driver Number	Driver Title	Driver Question
Programmatic		
1	Program Security Objectives	Are the program's security objectives realistic and achievable?
2	Security Plan	Does the plan for developing and deploying the system sufficiently address security?
3	Contracts	Do contract mechanisms with partners, collaborators, subcontractors, and suppliers sufficiently address security?
4	Security Process	Does the process being used to develop and deploy the system sufficiently address security?
5	Security Task Execution	Are security-related tasks and activities performed effectively and efficiently?
6	Security Coordination	Are security activities within the program coordinated appropriately?
7	External Interfaces	Do work products from partners, collaborators, subcontractors, or suppliers meet security requirements?
8	Organizational and External Conditions	Are organizational and external conditions facilitating completion of security tasks and activities?
9	Event Management	Is the program able to identify and manage potential events and changing circumstances that affect its ability to meet its software security objectives?
Product		
10	Security Requirements	Do requirements sufficiently address security?
11	Security Architecture and Design	Do the architecture and design sufficiently address security?
12	Code Security	Does the code sufficiently address security?
13	Integrated System Security	Does the integrated system sufficiently address security?
14	Adoption Barriers	Have barriers to customer/user adoption of the system's security features been managed appropriately?
15	Operational Security	Will the system comply with applicable security policies, laws,

Driver Number	Driver Title	Driver Question
	Compliance	standards, and regulations?
16	Operational Security Preparedness	Are people prepared to maintain the system's security over time?
17	Product Security Risk Management	Is the approach for managing product security risk sufficient?

Table 4: Software Security Drivers

For SA-2, the applicable software security drivers are

- *(1) Program Security Objectives*
- *(2) Security Plan*
- *(10) Security Requirements*

3. Informed by the drivers (and their detailed considerations), develop one or more statements of software security practice that reflect the intent of the control.

   Statements of practice for SA-2 that are relevant for software components that reside within information systems include the following:

   - *Software components have specified security requirements.*
   - *Adequate resources are allocated to ensure that software components satisfy their security requirements.*
   - *Budget to ensure that software components satisfy their security requirements is committed and documented in program plans.*

   Occasionally, formulating software security practices results in a change to the related drivers. In some cases, updates to the drivers are also identified.

4. Based on the statements of practice, derive measures that demonstrate whether or not the practice is being performed and, in some cases, the extent to which it is performed.

   Software security measures for SA-2 include the following:

   - *percentage of software components with/without specified security requirements*
   - *percentage of software components with/without adequate resources to satisfy security requirements*
   - *percentage of software components with/without committed, documented budgets for satisfying security requirements*

   We include both the presence of ("with") and the absence of ("without") as options to consider. Software development and acquisition managers are often more interested in what is missing than what is present. Identifying gaps and developing action plans to address them is one of the outcomes of having meaningful measures.

We believe this method for deriving measures of software security can be effectively applied to other relevant standards and guidelines such as

- Building Security In Maturity Model (BSIMM2) v3.0, http://www.bsi-mm.com/

- Open Web Applications Security Project (OWASP) Software Assurance Maturity Model (SAMM) v1.0, https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model
- Microsoft's Security Development Lifecycle, Version 5.1, http://www.microsoft.com/security/sdl/
- Department of Homeland Security Assurance for CMMI Process Reference Model, https://buildsecurityin.us-cert.gov/swa/procwg.html

Using Software Security Measures

The software security measures of System and Services Acquisition (SA) and System and Information Integrity (SI) controls can be used to support relevant decision-making activities as described in *Risk-Based Measurement and Analysis: Application to Software Security*, Section 5.1 “Using IMAF to Direct Measurement, Analysis, and Reporting Activities”, for a specific software acquisition or development program.

In the following statements, we continue to use SA-2 as our example. In terms of security requirements, the three SA-2 measures could be used to

- evaluate if software components of interest (internal or externally provided) are satisfying their stated security requirements, and are reviewed and measured during all lifecycle phases
- evaluate if software components are not satisfying their requirements, is this due to lack of staff resources or lack of budget (if this is of sufficiently high priority, resources and budget can be reallocated to correct the issue)
- aid in predicting the likelihood that software might fail in production due to unsatisfied security requirements through various forms of architecture risk analysis, code analysis, and testing
- establish a relationship between SA-2 and corresponding SI controls such as SI-2 Flaw Remediation and SI-3 Malicious Code Protection. For example, if a security requirement is not satisfied, this might lead to a software flaw that is a root cause for a security incident or leaves the software vulnerable to specific types of malware. The earlier in the lifecycle a software flaw is detected and corrected, the less expensive it is.
- support compliance reviews against required standards

Readers are encouraged to review *Risk-Based Measurement and Analysis: Application to Software Security*, Section 5.0, for additional applications of this work and Sections 6.0 and 7.0 for a discussion of additional research tasks and next steps.

Appendix

This appendix describes candidate measures that have been derived for the 14 controls within the System and Service Acquisition (SA) control family (Tables SA-1 through SA-14) and the 13 controls within the System and Information Integrity (SI) control family (Tables SI-1 through SI-13).

Clarifications and interpretations required to arrive at software security measures when a control is targeted to information systems are captured as footnotes. One example is footnote 1 in the SA-1 Policy and Procedures, which states the following [NIST 2010]:

> *The definition or profile of a software component includes the information system(s) on which they reside. Similarly the definition or profile of an information system includes the software components that are part of the information system configuration.*

Another example is footnote 8 in SI-3 Malicious Code Protection, which states [NIST 2010]:

> *Given that measures are intended to be software-component-centric (vs. information system centric), the phrase "information systems of interest" is used to designate those information systems where software components that are the subject of measurement reside/execute.*

Derivation of Software Security Measures for NIST 800-53: System and Service Acquisition Controls

SA-1	System and Services Acquisition Policy and Procedures
SA-2	Allocation of Resources
SA-3	Life Cycle Support
SA-4	Acquisitions
SA-5	Information System Documentation
SA-6	Software Usage Restrictions
SA-7	User-installed Software
SA-8	Security Engineering Principles
SA-9	External Information System Services
SA-10	Developer Configuration Management
SA-11	Developer Security Testing
SA-12	Supply Chain Protection
SA-13	Trustworthiness
SA-14	Critical Information System Components

SA-1 System and Services Acquisition Policy and Procedures Measures

Family and Class		Control			Related Controls
SA	Family: System and Service Acquisition Class: Management	SA-1	Policy and Procedures	The organization develops, disseminates, and reviews/updates a. a formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; b. formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	PM-9

Related Drivers	Practices	Measures
15. Operational Security Compliance 17. Product Security Risk Management	Software components[1] comply with applicable security policies and procedures Software components comply with applicable laws and regulations Software components comply with applicable standards of care Security policies and procedures reflect the organization's risk management strategy including an expression of an acceptable (or unacceptable) level of risk	• percentage of software components that comply/do not comply with applicable security policies and procedures • percentage of software components that comply/do not comply with applicable laws and regulations • percentage of software components that comply/do not comply with applicable standards of care • percentage of software component risks that exceed acceptable tolerances (see also control RA). Exceeding acceptable tolerances results in non-compliance with security policies and procedures

[1] The definition or profile of a software component includes the information system(s) on which they reside. Similarly the definition or profile of an information system includes the software components that are part of the information system configuration.

SA-2 Allocation of Resources

Family and Class	Control	Related Controls
SA Family: System and Service Acquisition Class: Management	SA-2 Allocation of Resources The organization a. includes a determination of information security requirements for the information system in mission/business process planning b. determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process c. establishes a discrete line item for information security in organizational programming and budgeting documentation	none

Related Drivers	Practices	Measures
1. Program Security Objectives 2. Security Plan 10. Security Requirements	Software components have specified security requirements Adequate resources are allocated to ensure that software components satisfy their security requirements Budget to ensure that software components satisfy their security requirements is committed and documented in program plans	• percentage of software components with/without specified security requirements • percentage of software components with/without adequate resources to satisfy security requirements • percentage of software components with/without committed, documented budgets for satisfying security requirements

SA-3 Life Cycle Support

Family and Class	Control	Related Controls
SA Family: System and Service Acquisition Class: Management	SA-3 Life Cycle Support The organization a. manages the information system using a system development life cycle (SDLC) methodology that includes information security considerations b. defines and documents information system security roles and responsibilities throughout the system development life cycle c. identifies individuals having information system security roles and responsibilities.	PM-7

Related Drivers	Practices	Measures
1. Program Security Objectives 2. Security Plan	Software components are developed using a SDLC method that includes security practices at each life cycle phase. Security roles and responsibilities are defined and documented for the entire SDLC. Individuals are identified and assigned to fulfill security roles and responsibilities.	• percentage of software components that are/are not developed using a SDLC that includes security practices o for each life cycle phase • percentage of software components for which individuals with security roles and responsibilities have/have not been o defined o documented o assigned o for each life cycle phase

SA-4 Acquisitions

Family and Class		Control			Related Controls
SA	Family: System and Service Acquisition Class: Management	SA-4	Acquisitions	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. security functional requirements/specifications b. security-related documentation requirements c. developmental and evaluation-related assurance requirements	none

Related Drivers	Practices	Measures
7. External Interfaces 10. Security Requirements 17. Product Security Risk Management	Contracts for acquiring software components include requirements that reflect: a. applicable federal laws, Executive Orders, directives, policies, regulations, and standards b. the results of risk assessment Contracts for acquiring software components include the following requirements (see supplemental guidance): a. Security functional requirements/specifications b. Security-related documentation requirements c. Developmental and evaluation-related assurance requirements	• percentage of acquired software components without contracts • percentage of acquired software components with contracts that do not specify security requirements • percentage of acquired software components with contracts that include requirements that reflect: o applicable federal laws, Executive Orders, directives, policies, regulations, and standards o the results of risk assessment • percentage of acquired software components with contracts that specify the following types of requirements: o security functional requirements o security documentation requirements o developmental (SDLC) assurance requirements o evaluation assurance requirements

SA-5 Information System Documentation

Family and Class		Control			Related Controls
SA	Family: System and Service Acquisition Class: Management	SA-5	Information System Documentation	The organization a. obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes 1. secure configuration, installation, and operation of the information system 2. effective use and maintenance of security features/functions 3. known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions b. obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes 1. user-accessible security features/functions and how to effectively use those security features/functions 2. methods for user interaction with the information system, which enables individuals to use the system in a more secure manner 3. user responsibilities in maintaining the security of the information and information system c. documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent	none

Related Drivers	Practices	Measures
16. Operational Security Preparedness	Each software component includes documentation that addresses the following topics: a. secure configuration, installation, and operation of the software component b. effective use and maintenance of security features/functions c. known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions d. user-accessible security features/functions and how to effectively use those security features/functions e. methods for user interaction with the software component, which enables individuals to use the software in a more secure manner f. user responsibilities in maintaining the security of the software component and any information that it processes, stores, and transmits	• percentage of delivered (deployed; released into production) software components that do/do not include required documentation (including as listed under Practices)

SA-6 Software Usage Restrictions

Family and Class	Control	Related Controls
SA Family: System and Service Acquisition Class: Management	SA-6 Software Usage Restrictions The organization a. uses software and associated documentation in accordance with contract agreements and copyright laws b. employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution c. controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work	none

Related Drivers	Practices	Measures
17. Product Security Risk Management	Software products without accompanying source code from sources with limited or no warranty are assessed for potential security impacts. (from supplemental guidance)	• percentage of software components in binary or machine executable form from sources with limited or no warranty that do not have accompanying source code • percentage of such software components that are used to meet compelling mission/operational requirements where no alternative is available • percentage of such software components that are/are not assessed for potential security impacts

SA-7 User-installed Software

Family and Class	Control	Related Controls
SA Family: System and Service Acquisition Class: Management	SA-7 User-installed Software The organization enforces explicit rules governing the installation of software by users.	CM-2

Related Drivers	Practices	Measures
15. Operational Security Compliance 16. Operational Security Preparedness	All software installed by users complies with explicit, documented rules (installations permitted, installations prohibited).	• none applicable for software security other than perhaps a user’s ability to install security updates and patches.

SA-8 Security Engineering Principles

Family and Class		Control			Related Controls
SA	Family: System and Service Acquisition Class: Management	SA-8	Security Engineering Principles	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. Supplemental guidance: The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of security engineering principles include, i. developing layered protections ii. establishing sound security policy, architecture, and controls as the foundation for design iii. incorporating security into the system development life cycle iv. delineating physical and logical security boundaries v. ensuring system developers and integrators are trained on how to develop secure software vi. tailoring security controls to meet organizational and operational needs vii. reducing risk to acceptable levels, thus enabling informed risk management decisions Security principles are further elaborated in NIST 800-27.	none

Related Drivers	Practices	Measures
1. Program Security Objectives 2. Security Plan 4. Security Process 10. Security Requirements 11. Security Architecture and Design 12. Code Security 16. Operational Security Preparedness 17. Product Security Risk Management	Software components are developed using an SDLC method that includes security practices that reflect security engineering principles at each life cycle phase	• percentage of software components that are/are not developed using a SDLC that includes security practices that reflect security engineering principles ○ for each life cycle phase

SA-9 External Information System Services

Family and Class		Control			Related Controls
SA	Family: System and Service Acquisition Class: Management	SA-9	External Information System Services	The organization a. requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance b. defines and documents government oversight and user roles and responsibilities with regard to external information system services c. monitors security control compliance by external service providers	none

Related Drivers	Practices	Measures
7. External Interfaces	Contracts and agreements with providers of external information system services (EISS) include the following specifications: a. services comply with organizational information security requirements b. services employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance Documentation provided by providers of EISS includes the following: a. security roles and responsibilities for government, service provider, and end users b. service level agreements An organizational risk assessment is conducted prior to the acquisition or outsourcing of EISS EISS providers and systems are regularly monitored for compliance with security controls	None specifically applicable for software security; could consider the following for measuring EISS: • percentage of EISS contracts and agreements that do/do not include specifications to comply with organizational information security requirements • percentage of EISS that do/do not include specifications to employ security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance • percentage of EISS documentation that does/does not include o security roles and responsibilities for government, service provider, and end users o service level agreements • percentage of EISS for which a risk assessment is/is not conducted prior to the acquisition or outsourcing of EISS • percentage of EISS that have/have not been monitored for compliance with security controls in the specified timeframe

SA-10 Developer Configuration Management

Family and Class		Control			Related Controls
SA	Family: System and Service Acquisition Class: Management	SA-10	Developer Configuration Management	The organization requires that information system developers/integrators: a. perform configuration management during information system design, development, implementation, and operation b. manage and control changes to the information system c. implement only organization-approved changes d. document approved changes to the information system e. track security flaws and flaw resolution	CM-3 CM-4 CM-9

Related Drivers	Practices	Measures
9. Event Management 11. Security Architecture and Design 12. Code Security 13. Integrated System Security 16. Operational Security Preparedness	Configuration management is performed for all software components throughout their life cycle Changes to software components are managed and controlled Only organization-approved changes to software components are implemented All approved changes to software components are documented Security flaws are tracked and resolved for all software components	• percentage of software components that are/are not subject to configuration management • for each life cycle phase • percentage of software components for which changes are/are not managed and controlled • percentage of software components for which only organization-approved changes are/are not implemented • percentage of software components for which approved changes are/are not documented • percentage of software components for which security flaws are/are not tracked • percentage of software components for which security flaws are/are not resolved

SA-11 Developer Security Testing

Family and Class		Control			Related Controls
SA	Family: System and Service Acquisition Class: Management	SA-11	Developer Security Testing	The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. create and implement a security test and evaluation plan b. implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process c. document the results of the security testing/evaluation and flaw remediation processes	CA-2 SI-2

Related Drivers	Practices	Measures
12. Code Security 13. Integrated System Security 16. Operational Security Preparedness	Software components are tested and evaluated in accordance with a documented security test and evaluation plan. Software components are analyzed for common flaws and vulnerabilities. Flaws and vulnerabilities found in software components are remediated and remediation is verified. The results of security testing and evaluation and flaw remediation are documented.	• percentage of software components tested and evaluated or not tested and not evaluated in accordance with a documented security test and evaluation plan ○ Supplemental guidance calls for this to be witnessed by an independent verification and validation agent • percentage of software components analyzed/not analyzed for common flaws and vulnerabilities • percentage of software components with remediated/unremediated flaws and vulnerabilities • percentage of software components with/without documented security test and evaluation results • percentage of software components with/without documented remediation results

SA -12 Supply Chain Protection

Family and Class		Control			Related Controls
SA	Family: System and Service Acquisition Class: Management	SA-12	Supply Chain Protection	The organization protects against supply chain threats by employing an organization-defined list of measures to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy. Supplemental guidance: A defense-in-breadth approach helps to protect information systems (including the information technology products that compose those systems) throughout the system development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk (refer to SA-12 control enhancements for specifics).	none

Related Drivers	Practices	Measures
7. External Interfaces	Vulnerabilities in supplier-provided software components are identified, managed, and eliminated at each phase of the life cycle. Supplier-provided software components are subject to complementary, mutually reinforcing strategies to mitigate risk	• percentage of supplier-provided software components for which vulnerabilities are/are not identified, managed, and eliminated o for each life cycle phase • percentage of supplier-provided software components that are/are not subject to risk mitigation strategies (such as the implementation of standard configurations and the use of penetration testing)

SA -13 Trustworthiness

Family and Class		Control			Related Controls
SA	Family: System and Service Acquisition Class: Management	SA-13	Trustworthiness	The organization requires that the information system meets an organization-defined level of trustworthiness. Supplemental guidance: Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of risk despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. (Additional supplemental guidance not included here; refer to NIST web site.)	RA-2 SA-4 SA-8 SC-3

Related Drivers	Practices	Measures
Aspects of all drivers are relevant to this control	Software components meet an organization-defined level of trustworthiness based on actions taken by developers and implementers and actions taken by assessors. (further details in supplemental guidance)	• percentage of software components that do/do not meet an organization-defined level of trustworthiness

SA-14 Critical Information System Components

Family and Class		Control			Related Controls
SA	Family: System and Service Acquisition Class: Management	SA-14	Critical Information System Components	The organization a. determines an organization-defined list of critical information system components that require re-implementation b. re-implements or custom develops such information system components. Supplemental guidance: The underlying assumption is that the list of information technology products defined by the organization cannot be trusted due to threats from the supply chain that the organization finds unacceptable. The organization re-implements or custom develops such components to satisfy requirements for high assurance.	SA-12 SA-13

Related Drivers	Practices	Measures
Refer to controls above	Critical software components that require re-implementation or customization are re-implemented or customized (in accordance with other SA controls for internally developed and externally supplied software components)	• Measures associated with other SA controls are also applicable here for re-implemented or custom-developed software components

Derivation of Software Security Measures for NIST 800-53: System and Information Integrity Controls

SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-4	Information System Monitoring
SI-5	Security Alerts, Advisories, and Directives
SI-6	Security Functionality Verification
SI-7	Software and Information Integrity
SI-8	Spam Protection
SI-9	Information Input Restrictions
SI-10	Information Input Validation
SI-11	Error Handling
SI-12	Information Output Handling and Retention
SI-13	Predictable Failure Prevention

SI-1 System and Information Integrity Policy and Procedures

Family and Class		**Control**			**Related Controls**
SI	Family: System and Information Integrity Class: Operational	SI-1	Policy and Procedures	The organization develops, disseminates, and reviews/updates: a. a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; b. formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	PM-9

Related Drivers	**Practices**	**Measures**
15. Operational Security Compliance 17. Product Security Risk Management	Software components[2] comply with applicable security policies and procedures Software components comply with applicable laws and regulations Software components comply with applicable standards of care Security policies and procedures reflect the organization's risk management strategy including an expression of an acceptable (or unacceptable) level of risk	• percentage of software components that comply/do not comply with applicable security policies and procedures • percentage of software components that comply/do not comply with applicable laws and regulations • percentage of software components that comply/do not comply with applicable standards of care • percentage of software component risks that exceed acceptable tolerances (see also control RA). Exceeding acceptable tolerances results in non-compliance with security policies and procedures.

[2] The definition or profile of a software component includes the information system(s) on which they reside. Similarly the definition or profile of an information system includes the software components that are part of the information system configuration.

SI-2 Flaw Remediation

Family and Class	Control	Related Controls
SI Family: System and Information Integrity Class: Operational	SI-2 Flaw Remediation The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process.	CA-2 CA-7 CM-3 MA-2 IR-4 RA-5 SA-11 SI-11

Related Drivers	Practices	Measures
13. Integrated System Security	Advisories, alerts, and other sources that identify software flaws are monitored and applicable flaws are identified. Software components affected by recently announced software flaws are identified. Software components with potential vulnerabilities that result from recently announced software flaws are identified. Software flaws are reported to designated individuals. Software vulnerabilities are reported to designated individuals.	• elapsed time since sources of software flaws have been monitored (mean, median) • number of applicable software flaws identified by source • percentage of software components affected by software flaws where the elapsed time between when the flaw was announced and affected software components are identified exceeded the organization-defined benchmark • percentage of software components affected by software flaws where corrective action is required[3] • percentage of software components with potential vulnerabilities resulting from software flaws where corrective action is required • percentage of software components affected by software flaws reported to designated individuals[4] • percentage of software components with potential vulnerabilities resulting from software flaws reported to designated individuals
7. External Interfaces 12. Code Security 16. Operational Security Preparedness	Security-relevant software updates[5] are installed[6] for all software components with software flaws and vulnerabilities where corrective action is required. Security-relevant software updates are installed in a timely manner.	• percentage of software components requiring security-relevant software updates • percentage of software components requiring security-relevant software updates where such updates have been installed • percentage of software components

[3] Not all software flaws will require action.

[4] If this percentage is less than the percentage in the measure immediately above, this implies that some judgment call has been made as to which flaws warrant reporting.

[5] “Updates” as used here may also include other mitigating actions that do not involve a change to the software.

[6] NIST 800-53 is silent in this control description on the testing of software updates. The supplemental guidance should state “tests and installs.”

Related Drivers	Practices	Measures
		requiring security-relevant software updates where such updates have been installed in the required timeframe • [from NIST 800-55 Appendix A Measure 19] percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated
9. Event Management 13. Integrated System Security	Updates to software components affected by software flaws discovered as a result of a security assessment are addressed in a timely manner. Updates to software components affected by software flaws discovered as a result of continuous monitoring are addressed in a timely manner. Updates to software components affected by software flaws discovered as a result of a security incident are addressed in a timely manner. Updates to software components affected by software flaws discovered as a result of information system error handling are addressed in a timely manner.	• percentage of software components requiring software updates as a result of any of the activities identified under Practice. • percentage of software components requiring software updates where such updates have been installed • percentage of software components requiring software updates where such updates have been installed in the required timeframe
13. Integrated System Security 15. Operational Security Compliance 16. Operational Security Preparedness	Software flaw remediation is incorporated into the organizational configuration management process. Software flaw remediation actions are tracked and verified.	• percentage of software flaws that are/are not remediated as part of the organizational configuration management process • percentage of software flaws that are/are not tracked to closure • percentage of closed software flaws where the remediation actions are verified against identified sources
13. Integrated System Security 16. Operational Security Preparedness	The software flaw remediation process is managed centrally. Software updates to remediate flaws are installed automatically.	• percentage of software flaws that are/are not remediated as part of a defined remediation process that is managed centrally • percentage of software flaws remediated by software updates where the updates are/are not installed automatically
	The state of software components with regard to flaw remediation (whether or not an identified flaw has been remediated in the required timeframe) is determined automatically. The state of software components with regard to flaw remediation is determined and reported at a frequency determined by the organization.	• percentage of software components with identified flaws where the remediation (or absence of remediation) for each flaw is/is not determined automatically • percentage of software components whose flaw remediation is determined; is reported within the defined frequency
	The time between flaw identification and flaw remediation is measured. The time between flaw identification and flaw remediation is compared to benchmarks defined by the organization.	• for a given software flaw (by software component, by information system; or for a class or category of flaws), the elapsed time between flaw identification and flaw remediation (mean, median) • for a given software flaw, percentage of elapsed time measures between identification and remediation that meet or fall below/exceed defined benchmarks

Related Drivers	Practices	Measures
	To the extent applicable, the remediation of software flaws to software components is performed using automated patch management tools.	- percentage of software components with software flaws that are addressed by a patch where an automated patch management tool is/is not used

SI-3 Malicious Code Protection

Family and Class		Control			Related Controls
SI	Family: System and Information Integrity Class: Operational	SI-3	Malicious Code Protection	The organization: a. employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code 1. transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or 2. inserted through the exploitation of information system vulnerabilities; b. updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. configures malicious code protection mechanisms to: 1. perform periodic scans of the information system and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. (select one or more) block malicious code; quarantine malicious code; send alert to administrator in response to malicious code detection; and d. addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	SA-4 SA-8 SA-12 SA-13 SI-4 SI-7

Related Driver	Practice	Measures
7. External Interfaces 13. Integrated System Security 16. Operational Security Preparedness The following drivers may also apply if there is a requirement for a software component to self-protect against malware compromises: 10. Security Requirements 11. Security Architecture and Design 12. Code Security	Software components[7] are regularly and automatically scanned for viruses, worms, Trojan horses, spyware, and other forms of malicious code. Detected malicious code is quarantined, blocked, or eradicated. Alerts are sent as specified. Information systems of interest[8] have strong software integrity controls (such as regular capture, review, and analysis of monitoring and scanning results). Information systems of interest are subject to regular configuration management review and update in accordance with policy and standards.	• elapsed time since software components were scanned for viruses, worms, Trojan horses, spyware, and other forms of malicious code or unauthorized code (mean, median) (if scanning is continuous and automatic, this measure is not applicable) • number of occurrences of malicious code that exceed defined criteria/thresholds • elapsed time to remediate malicious code that exceeds defined criteria/thresholds (mean, median) • percentage of information systems of interest for which a configuration management review and update has not been conducted in accordance with policy and standards (mean, median) and within the required timeframe
	Custom software components are subject to secure coding practices (as part of, for example, the contract or service level agreement for such components) (supplemental)[9]	• percentage of custom software components subject to secure coding practices that have not been reviewed for compliance in accordance with policy
	Malicious code protection mechanisms are regularly updated to reflect new forms of malicious code.	• percentage of malicious code protection mechanisms that are not updated (new releases, regular maintenance) within threshold in accordance with policy
	The impact of false positives during malicious code detection and eradication on the availability of information systems of interest is managed.	• percentage of information systems of interest where system availability is reduced above threshold due to malicious code false positives

[7] Includes custom software components

[8] Given that measures are intended to be software-component- centric (versus information system centric), the phrase “information systems of interest” is used to designate those information systems where software components that are the subject of measurement reside/execute.

[9] With the exception of this practice, this control is primarily focused on information systems, not software components.

SI-4 Information System Monitoring

Family and Class	Control			Related Controls
SI Family: System and Information Integrity Class: Operational	SI-4	Information System Monitoring[10]	The organization: a. monitors events on the information system in accordance with monitoring objectives and detects information system attacks; b. identifies unauthorized use of the information system; c. deploys monitoring devices: 1. strategically within the information system to collect organization-determined essential information; and 2. at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	AC-4 AC-8 AC-17 AU-2 AU-6 SI-3 SI-7

Related Drivers	Practices	Measures
13. Integrated System Security 15. Operational Security Compliance 16. Operational Security Preparedness	Partially covered by SI-3 (for malicious code monitoring, detection, and handling), which is the only practice that is applicable for this control.	• none applicable for software security other than information system monitoring software as noted in the comment above, also addressed in SI-6

[10] It is not clear if this control applies to the software used to monitor information systems. This may be worth considering as part of the SA family of controls (refer to SA-9 as applied to software acquired and used for monitoring information systems).

SI-5 Security Alerts, Advisories, and Directives

Family and Class		Control			Related Controls
SI	Family: System and Information Integrity Class: Operational	SI-5	Security Alerts, Advisories, and Directives	The organization: a. receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. generates internal security alerts, advisories, and directives as deemed necessary; c. disseminates security alerts, advisories, and directives to organization-defined list of personnel by role; and d. implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	none

Related Drivers	Practices	Measures
9. Event Management 13. Integrated System Security 15. Operational Security Compliance 16. Operational Security Preparedness	Not applicable for software security	• none

SI-6 Security Functionality Verification

Family and Class		Control			Related Controls
SI	Family: System and Information Integrity Class: Operational	SI-6	Security Functionality Verification	The information system verifies the correct operation of security functions (select one or more) a. at organization-defined system transitional states b. upon command by user with appropriate privilege c. periodically every organization-defined time-period d. (select one or more): notifies system administrator; shuts the system down; restarts the system; other organization-defined alternative action(s) when anomalies are discovered	none

Related Drivers	Practices	Measures
13. Integrated System Security 16. Operational Security Preparedness	Security functions are verified for correct operation in accordance with established criteria. Failure of security function tests are handled in accordance with established criteria.	• percentage of security functions that have not been verified in accordance with established criteria • percentage of security function test failures above threshold • percentage of security function test failures that are not handled in accordance with established criteria

SI-7 Software and Information Integrity

Family and Class		Control			Related Controls
SI	Family: System and Information Integrity Class: Operational	SI-7	Software and Information Integrity	The information system detects unauthorized changes to software and information. The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes). The organization uses tools to automatically monitor the integrity of the information system and the applications it hosts.	none

Related Drivers	Practices	Measures
13. Integrated System Security 15. Operational Security Compliance 16. Operational Security Preparedness	Integrity scans of information systems of interest detect unauthorized changes to software. Integrity scans of information systems of interest are performed in accordance with established criteria. Notification of integrity discrepancies is provided to designated individuals. The integrity of COTS software is determined in accordance with established criteria.	• number of unauthorized changes detected (by system, by software component) • percentage of information systems of interest that have not been integrity scanned in accordance with established criteria • number of reported integrity discrepancies (by system, by software component) • percentage of COTS software components that have not been integrity scanned in accordance with established criteria

SI-8 Spam Protection

Family and Class		Control			Related Controls
SI	Family: System and Information Integrity Class: Operational	SI-8	Spam Protection	The organization a. employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means and b. updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.	SC-5 SI-3

Related Drivers	Practices	Measures
13. Integrated System Security 15. Operational Security Compliance 16. Operational Security Preparedness	not applicable	- None applicable for software security Also addressed in SI-6.

SI-9 Information Input Restrictions

Family and Class		Control			Related Controls
SI	Family: System and Information Integrity Class: Operational	SI-9	Information Input Restrictions	The organization restricts the capability to input information to the information system to authorized personnel.	AC-5 AC-6

Related Drivers	Practices	Measures
13. Integrated System Security 15. Operational Security Compliance 16. Operational Security Preparedness	Software components enforce access control requirements in accordance with established criteria. Software components permit the input of information by authorized personnel only (or conversely, prohibit the input of information by unauthorized personnel).	- percentage of software components that permitted violations of access control requirements - percentage of software components that permitted input of information by unauthorized personnel

SI-10 Information Input Validation

Family and Class		Control			Related Controls
SI	Family: System and Information Integrity Class: Operational	SI-10	Information Input Validation	The information system checks the validity of information inputs. Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.	none

Related Drivers	Practices	Measures
13. Integrated System Security 15. Operational Security Compliance 16. Operational Security Preparedness	Software components ensure that syntax and semantics of information inputs is valid in accordance with established rules.	• percentage of software components that permitted input of information that violated established rules for valid syntax and semantics

SI-11 Error Handling

Family and Class	Control			Related Controls
SI Family: System and Information Integrity Class: Operational	SI-11	Error Handling	The information system a. identifies potentially security-relevant error conditions b. generates error messages that provide information necessary for corrective actions without revealing organization-defined sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries and c. reveals error messages only to authorized personnel The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, account numbers, social security numbers, and credit card numbers.	none

Related Drivers	Practices	Measures
13. Integrated System Security 15. Operational Security Compliance 16. Operational Security Preparedness	Software components detect identified security-relevant error conditions. Software components that detect identified security-relevant error conditions generate error messages that comply with organizational policy and operational requirements. (Error-handling) software components enforce access control requirements for error messages in accordance with established criteria.	• percentage of software components that fail to detect identified security-relevant error conditions • percentage of software components that detect identified security-relevant error conditions and fail to generate error messages that comply with organizational policy and operational requirements • percentage of (error- handling) software components that violate requirements for error messages

SI-12 Information Output Handling and Retention

Family and Class		Control			Related Controls
SI	Family: System and Information Integrity Class: Operational	SI-12	Information Output Handling and Retention	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	MP-2 MP-4

Related Drivers	Practices	Measures
13. Integrated System Security 15. Operational Security Compliance 16. Operational Security Preparedness	Software components that handle information meet all compliance obligations for that information (applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements).	• percentage of software components that handle information and that fail to meet information handling compliance obligations (by source of obligation)

SI-13 Predictable Failure Prevention

Family and Class		Control			Related Controls
SI	Family: System and Information Integrity Class: Operational	SI-13	Predictable Failure Prevention	The organization a. protects the information system from harm by considering mean time to failure for an organization-defined list of information system components in specific environments of operation and b. provides substitute information system components, when needed, and a mechanism to exchange active and standby roles of the components While mean time to failure is primarily a reliability issue, this control focuses on the potential failure of specific components of the information system that provide security capability. Mean time-to-failure rates are defendable and based on considerations that are installation-specific, not industry-average. The transfer of responsibilities between active and standby information system components does not compromise safety, operational readiness, or security (e.g., state variables are preserved). The standby component is available at all times except where a failure recovery is in progress or for maintenance reasons.	CP-2

Related Drivers	Practices	Measures
13. Integrated System Security 16. Operational Security Preparedness	Software components that provide security capabilities are protected from failing in accordance with mean time-to-failure requirements.	• percentage of software components that provide security capabilities that violate mean time-to-failure requirements

References

URLs are valid as of the publication date of this document.

[Alberts 2010]
Alberts, C.; Allen, J.; & Stoddard, R. *Integrated Measurement and Analysis Framework for Software Security* (CMU/SEI-2010-TN-025). Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tn025.cfm

[Alberts 2011]
Alberts, C.; Allen, J.; & Stoddard, R. "Security Measurement and Analysis" (annotated presentation). Software Engineering Institute, Carnegie Mellon University, 2011. http://www.cert.org/archive/pdf/SecurityMeasurementandAnalysis.pdf

[Alberts 2012]
Alberts, C.; Allen, J.; & Stoddard, R. *Risk-Based Measurement and Analysis: Application to Software Security* (CMU/SEI-2012-TN-004). Software Engineering Institute, Carnegie Mellon University, 2012. http://www.sei.cmu.edu/library/abstracts/reports/12tn004.cfm

[ISO 2005]
International Organization for Standardization. *ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management*. ISO, 2005.

[NIST 2010]
National Institute of Standards and Technology (NIST). *Recommended Security Controls for Federal Information Systems and Organizations: Special Publication 800-53 Revision 3*. NIST, August 2009 – May 2010.
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf