# Requirements and Recommendations for CWE Compatibility and CWE Effectiveness

**Document version:** 1.0    **Date:** July 28, 2011

*This is a draft report and does not represent an official position of The MITRE Corporation.* *This document is subject to change without notice.*

**Authors:**
Robert A. Martin, CWE Project Leader - ramartin@mitre.org
Steven M. Christey, CWE Technical Lead - coley@mitre.org

## Table of Contents

## 1 Definitions

**Accuracy Percentage** - The percentage of security elements in the Review Sample that reference the correct CWE identifiers.

**Capability** - An assessment tool, Integrated Development Environment (IDE), code review tool, code checking compiler, database, Web site, advisory, or service that provides information about implementation, design, or architecture-level weaknesses that can lead to an exploitable security vulnerability in software.

**Effectiveness Testing** - The process of determining whether a capability is CWE Effective.

**Map/Mapping** - The specification of relationships between weakness elements in a Repository and the CWE items that are related to those elements.

**Owner** - The custodian (real person or company) having responsibility for the capability.

**Repository** - An implicit or explicit collection of security-related software weakness elements that supports a capability, e.g., a database of security weaknesses, the set of patterns in a code analyzer, or a Web site.

**Review** - The process of determining whether a capability is CWE-Compatible.

**Review Authority** - An entity that performs a Review or effectiveness Testing and is authorized to grant CWE-Compatible or CWE-Effective status (MITRE is the only Review Authority at this time).

**Review Version** - The dated version of CWE that is being used for determining CWE compatibility or CWE effectiveness of a capability.

**Security Element** - A database record, assessment probe, signature, etc., that is related to a specific security weakness.

**Task** - A tool's probe, check, signature, etc., that performs some action that produces security information (i.e., the security element).

**Test Results** - Data representing the outcome of effectiveness testing.

**Tool** - A software application or device that examines a piece of software, binary, or other artifact and produces information about security weaknesses, e.g., a source code security analyzer, a code quality assessment tool, code checking compiler or a development environment.

**User** - A consumer or potential consumer of the Capability.

**Vulnerability** - Any weakness in software that could be exploited to violate a system or the information it contains (based upon ITU-T X.1500).

**Weakness** - A shortcoming or imperfection in the software code, design, architecture, or deployment that, could, at some point become a vulnerability, or could contribute to the introduction of other vulnerabilities.

## 2 High-Level Requirements

The following items define the concepts, roles, and responsibilities related to the proper use of CWE Identifiers to share data across separate security weakness capabilities (tools, repositories, and services) to allow these security weakness capabilities to be used together, and to facilitate the comparison of security weakness tools and services.

## Prerequisites

**2.1)** The capability owner MUST be a valid legal entity, i.e., an organization or a specific individual, with a valid phone number, email address, and street mail address.

**2.2)** The capability MUST provide additional value or information beyond that which is provided in CWE itself (i.e., name, description, risks, references, and associated weakness information).

**2.3)** The capability owner MUST provide the Review Authority with a technical point of contact who is qualified to answer questions related to the mapping accuracy, any CWE-related functionality of the capability, and to coordinate the testing of the capability in support of assessing its effectiveness in identifying CWEs.

**2.4)** The capability MUST be available to the public, or to a set of consumers, in a production or public version.

**2.5)** For CWE compatibility the capability owner MUST provide the Review Authority with a completed "CWE compatibility Requirements Evaluation Form."

**2.6)** The capability owner MUST provide the Review Authority with free access to the Repository so that the Authority can determine that the Repository satisfies all associated mapping accuracy requirements.

**2.7)** The capability owner MUST allow the Review Authority to use the Repository to identify any weaknesses that should be added to CWE.

**2.8)** For CWE effectiveness the capability MUST be CWE Compatible.

**2.9)** For CWE effectiveness the capability owner MUST provide the Review Authority with a completed "CWE effectiveness Requirements Evaluation Form."

**2.10)** For CWE effectiveness the capability owner MUST provide the Review Authority with effectiveness testing results so that the Authority can determine that the capability satisfies all associated effectiveness requirements.

**2.11)** The capability owner MUST agree to abide by all of the mandatory CWE compatibility and effectiveness Requirements, which includes the mandatory requirements for the specific type of capability.

## Functionality

**2.12)** For CWE compatibility the capability MUST allow users to locate security elements using CWE identifiers ("CWE-Searchable").

**2.13)** For CWE compatibility when the capability presents security elements to the user, it MUST allow the user to obtain the associated CWE identifiers ("CWE-Output").

**2.14)** For CWE compatibility the capability's mapping MUST accurately link security elements to the appropriate CWE identifiers ("Mapping Accuracy").

**2.15)** For CWE compatibility the capability's documentation MUST adequately describe CWE, CWE compatibility, and how the CWE-related functionality in the capability is used ("CWE-Documentation").

**2.16)** For CWE compatibility the capability's publicly available documentation MUST explicitly list the CWE identifiers that the capability owner considers the capability to cover as part of its functionality ("CWE-Coverage").

**2.17)** For CWE compatibility the capability’s publicly available web site SHOULD provide the capability’s CWE-Coverage as a CWE Coverage Claim Representation (CCR) XML document(s).

**2.18)** For CWE effectiveness the results from the capability's assessing the test sets for the CWE identifiers (listed as the capability's CWE-Coverage) MUST be posted on the CWE Web site. ("CWE-Test Results").

**2.19)** The capability MUST denote the dated CWE version used ("Version Usage").

**2.20)** The capability MUST satisfy any additional requirements for the specific type of capability, as specified in Appendix A.

**2.21)** The capability MUST satisfy all requirements for its distribution media, as specified in Appendix B.

**2.22)** The capability is NOT REQUIRED to do any of the following:

- use the same descriptions or references as CWE
- include every CWE identifier in its repository

### Miscellaneous

**2.23)** If the capability does not satisfy all of the applicable requirements above (2.1 through 2.22), then the capability owner shall not advertise that it is CWE-compatible or CWE-effective.

## 3 Accuracy

CWE compatibility only facilitates data sharing and correlation if the capability's mapping is accurate. Therefore, CWE-compatible capabilities must meet the following minimum accuracy requirements.

**3.1)** The Repository MUST have an accuracy of 100 percent.

**3.2)** During the review period, the capability owner MUST correct any mapping errors found by the Review Authority.

**3.3)** After the review period, the capability owner SHOULD correct a mapping error within a reasonable time frame after the error was initially reported, i.e., within two (2) versions of the capability repository or six (6) months, whichever is shorter.

**3.4)** The capability owner SHOULD prepare and sign a statement that, to the best of the capability owner's knowledge, there are no errors in the mapping.

**3.5)** If the capability is based on, or uses, another CWE-compatible capability (the "Source" capability), and the capability owner becomes aware of mapping errors in the Source capability, then the capability owner MUST report those errors to the capability owner of the Source capability.

## 4 Effectiveness

Effectiveness is focused on providing prospective users of a capability visibility into the abilities of the capability to identify the corresponding weaknesses in software. Insight into the ability of a capability to find weaknesses in the face of different levels of complexity is of interest to users when they are considering using a capability or relying on the results of someone else using a capability. Therefore, CWE-effective Capabilities must meet the following minimum effectiveness requirements.

**4.1)** Using the appropriate portion of the “CWE Effectiveness Requirements Evaluation Form” the capability owner MUST declare which CWE identifiers they claim their capability is effective in locating. This can be accomplished through the use of a CWE Coverage Claim Representation (CCR) XML document(s).

**4.2)** For the CWE identifiers declared, the capability owner MUST request the appropriate test sets so that the capability owner can use the capability to assess the test sets for all of the weaknesses corresponding to the declared CWE identifiers.

**4.3)** Within an agreed upon time-frame, the capability owner MUST submit the results they obtained from assessing the test sets with their capability.

**4.4)** The results MUST list each assessed test set file, and the line number for each weakness located along with the appropriate CWE identifier.

**4.5)** The capability owner MUST prepare and sign a statement agreeing to the posting of their Capabilities test results on the CWE Web site.

**4.6)** The capability owner MUST submit a revised “CWE Effectiveness Requirements Evaluation Form” with an updated listing of the CWE identifiers they claim their capability is effective in locating in order to retake the effectiveness tests for a different set of CWE identifiers. This can be accomplished through the use of an updated CWE Coverage Claim Representation (CCR) XML document(s).

## 5 Documentation

The following requirements apply to documentation that is provided with the capability.

**5.1)** The documentation MUST include a brief description of CWE and CWE compatibility, which can be based on verbatim portions of documents from the CWE Web site.

**5.2)** The documentation MUST describe how the user can find individual security elements in the capability's repository by using CWE identifiers.

**5.3)** The documentation MUST describe how the user can obtain CWE identifiers from individual elements in the capability's repository.

**5.4)** If the documentation includes an index, then it SHOULD include references to CWE-related documentation under the term "CWE."

## 6 CWE Version Usage

Users must know what version of CWE is used in a capability's repository with respect to its mapping to CWE. The capability owner can indicate the currency of a mapping by using the CWE version or date the mapping was updated.

**6.1)** The capability MUST identify the CWE version or update date that was used in creating or updating the mapping through at least one of the following: change logs, new feature lists, help files, or some other mechanism. The capability is "up-to-date" with respect to that version or update date.

**6.2)** Each new version of the capability SHOULD be up-to-date with respect to a CWE version that was released no more than four (4) months before the capability was made available to its users. If a capability does not satisfy this requirement, then it is "out-of-date."

**6.3)** The capability owner SHOULD publicize how quickly it will update the capability's repository after a new CWE version or update becomes available on the CWE Web site.

## 7 Revocation of CWE Compatibility

**7.1)** If a review authority has verified that a capability is CWE-compatible or CWE-effective, but at a later time the Review Authority has evidence that the requirements are not being met, then the Review Authority MAY revoke its approval.

**7.1.1)** The review authority MUST identify the specific requirements that are not being met.

**7.2)** The review authority MUST determine if the actions or claims of the capability owner are "intentionally misleading."

**7.2.1)** The review authority MAY interpret the phrase "intentionally misleading" at its discretion.

**7.3)** The review authority SHOULD NOT consider revoking CWE compatibility for a particular capability more often than once every six (6) months.

### Warning and Evaluation

**7.4)** The review authority MUST provide the capability owner and technical POC with a warning of revocation at least two (2) months before revocation is scheduled to occur.

**7.4.1)** If the review authority has found that the capability owner's actions or claims are intentionally misleading, then the Review Authority MAY disregard the warning period.

**7.5)** If the capability owner believes that the requirements are being met, then the capability owner MAY respond to the warning of revocation by providing specific details that indicate why the capability meets the requirements under question.

**7.6)** If the capability owner modifies the capability so that it complies with the requirements in question during the warning period, then the Review Authority SHOULD end the revocation action for the capability.

### Revocation

**7.7)** The review authority MAY delay the date of revocation.

**7.8)** The review authority MUST publicize that CWE compatibility or CWE effectiveness has been revoked for the capability.

**7.9)** If the review authority finds that the capability owner's actions with respect to CWE compatibility or CWE effectiveness requirements are intentionally misleading, then revocation SHOULD last a minimum of one year.

**7.10)** The review authority MAY publicize the reason for revocation.

**7.11)** The capability owner MAY post a public statement regarding the revocation on the same site.

**7.12)** If the approval is revoked, the capability owner MUST NOT apply for a new review during the period of revocation.

## 8 Review Authority

**8.1)** A Review Authority MUST review the Capability for CWE compatibility or CWE effectiveness with respect to a specific CWE version, i.e., the Review Version.

**8.2)** A review authority MUST clearly identify the Review Version that was used to determine compatibility or effectiveness for the capability.

**8.3)** A review authority MUST clearly identify the version of the CWE compatibility requirements and effectiveness document that was used to determine compatibility or effectiveness for the capability.

**8.4)** A review authority MUST review every element in the capability's repository for CWE mapping accuracy.

**8.5)** A review authority SHOULD review a capability for mapping accuracy at least once per year.

## 9 Appendix A: Type-Specific Requirements

Since a wide variety of capabilities use CWE, certain types of capabilities may have unique features that require special attention with respect to CWE compatibility.

**A.1)** The capability MUST satisfy all additional requirements that are related to the specific type of capability.

**A.1.1)** If the capability is an assessment tool, source or binary code security analyzer, a code quality assessment tool, code checking compiler, development environment, or a product that integrates the results of one or more of these types of items, then it must satisfy the Tool Requirements, A.2.1 - A.2.8.

**A.1.2)** If the capability is a service (such as a security assessment service, an education or training service, or a code and design review service) then it must satisfy the Security Service Requirements, A.3.1 - A.3.5.

**A.1.3)** If the capability is an online database of security issues or weaknesses in application software, Web-based resource, or information site, then it must satisfy the Online Capability Requirements, A.4.1 - A.4.3.

## Tool Requirements

**A.2.1)** The tool MUST allow the user to use CWE identifiers to locate associated tasks in that tool ("CWE-Searchable") by providing at least one of the following: a "find" or "search" function, a mapping between that tool's task names and CWE identifiers, or another mechanism determined to be sufficient by the review authority.

**A.2.2)** For any report that identifies individual security elements, the tool MUST allow the user to determine the associated CWE identifiers for those elements ("CWE-Output") by doing at least one of the following: including CWE identifiers directly in the report, providing a mapping between the tool's task names and CWE identifiers, or using some other mechanism determined to be sufficient by the review authority.

**A.2.3)** The publicly available documentation MUST explicitly list the CWE identifiers that the capability owner considers the tool effective at locating in software ("CWE-Compatibility Claim Coverage").

**A.2.4)** The capability's publicly available web site MAY provide the capability's CWE-Compatibility Claim Coverage as a CWE Coverage Claim Representation (CCR) XML document(s).

**A.2.5)** Any required reports or mappings MUST satisfy the media requirements as specified in Appendix B.

**A.2.6)** The tool, or the capability owner, SHOULD provide the user with a list of all CWE identifiers that are associated with the tool's tasks.

**A.2.7)** The tool SHOULD allow the user to select a set of tasks by providing a file that contains a list of CWE identifiers.

**A.2.8)** The interface of the tool SHOULD allow the user to browse, select, and deselect a set of tasks by using individual CWE identifiers.

**A.2.9)** If the tool does not have a task that is associated with a CWE identifier as specified by the user in the A.2.5 or A.2.6 tool requirements, then the tool SHOULD notify the user that it cannot perform the associated task.

**A.2.10)** The capability owner MUST warrant that (1) the rate of false positives is less than 100 percent, i.e., if the tool reports a specific security element, it is at least sometimes correct, and (2) the rate of false negatives is less than 100 percent, i.e., if an issue is in the artifacts of the system that is related to a specific security element, then sometimes the tool reports that issue.

## Security Service Requirements

Security services might use CWE-compatible and CWE-effective tools in their work, but they may not provide their customers with direct access to those tools. Thus it could be difficult for customers to identify and compare the capabilities of different services. The Security Service Requirements address this potential limitation.

**A.3.1)** The Security Service MUST be able to use CWE identifiers to tell a user which security elements are tested, detected, or covered by the service offering ("CWE-Searchable") by doing one or more of the following: providing the user with a list of CWE identifiers that identify the elements that are tested, detected, or covered by that Service, providing the user with a mapping between the Service's elements and CWE identifiers, responding to a user-supplied list of CWE identifiers by identifying which of the CWE identifiers are tested, detected, or covered by the Service, or by using some other mechanism.

**A.3.2)** For any report that identifies individual security elements, the Service MUST allow the user to determine the associated CWE identifiers for those elements ("CWE-Output") by doing one or more of the following: allowing the user to include CWE identifiers directly in the report, providing the user with a mapping between the security elements and CWE identifiers, or by using some other mechanism.

**A.3.3)** The publicly available documentation MUST explicitly list the CWE identifiers that the capability owner considers the Security Service to effectively cover in its offering ("CWE-Compatibility Claim Coverage").

**A.3.4)** The capability's publicly available web site MAY provide the capability's CWE-Compatibility Claim Coverage as a CWE Coverage Claim Representation (CCR) XML document(s).

**A.3.5)** Any required reports or mappings that are provided by the Service MUST satisfy the media requirements as specified in Appendix B.

**A.3.6)** If the Service provides the user with direct access to a product that identifies security elements, then that product SHOULD be CWE-compatible and CWE-effective.

**A.3.7)** The capability owner MUST warrant that (1) the rate of false positives is less than 100 percent, i.e., if a tool reports a specific security element, it is at least sometimes correct, and (2) the rate of false negatives is less than 100 percent, i.e., if an issue is in the artifacts of the system that is related to a specific security element, then sometimes the Service reports that issue.

## Online Capability Requirements

**A.4.1)** The online capability MUST allow a user to find related security elements from the online capability's repository ("CWE-Searchable") by providing one of the following: a search function that returns CWE identifiers for related elements, a mapping that links each element with its associated CWE identifier(s), or some other mechanism.

**A.4.1.1)** The online capability SHOULD provide a URL "template" that allows a computer program to easily construct a link that accesses the search function as outlined in online capability Requirements A.4.1.

Examples:
http://www.example.com/cgi-bin/db-search.cgi?cweid=XXX
http://www.example.com/cwe/xxx.html

**A.4.1.2)** If the site is publicly accessible without requiring login, then the cgi program SHOULD accept "GET" method.

**A.4.2)** For any report that identifies individual security elements, the online capability MUST allow the user to determine the associated CWE identifiers for those elements ("CWE-Output") by doing at least one of the following: by allowing the user to include CWE identifiers directly in the report, providing the user with a mapping between the security elements and CWE identifiers, or by some other mechanism.

**A.4.3)** The publicly available documentation MUST explicitly list the CWE identifiers that the capability owner considers the online capability's repository to cover ("CWE-Compatibility Claim Coverage").

**A.4.4)** The capability's publicly available web site MAY provide the capability's CWE-Compatibility Claim Coverage as a CWE Coverage Claim Representation (CCR) XML document(s).

**A.4.5)** If the online capability does not provide details for individual security elements, then the online capability MUST provide a mapping that links each element with its associated CWE identifier(s).

# 10 Appendix B: Media Requirements

**B.1)** The distribution media that is used by a CWE-compatible capability MUST use a media format that is covered in this appendix.

**B.2)** The media format MUST satisfy the specific requirements for that format.

## Electronic Documents (HTML, word processor, PDF, ASCII text, etc.)

**B.3.1)** The document MUST be in a commonly available format that has readers which support a "find" or "search" function ("CWE-Searchable"), such as raw ASCII text, HTML, or PDF.

**B.3.2)** If the document only provides short names or titles for individual elements, then it MUST list the CWE identifiers that are related to those elements ("CWE-Output").

**B.3.3)** The document SHOULD include a mapping from elements to CWE identifiers, which lists the appropriate pages for each element.

## Graphical User Interface (GUI)

**B.4.1)** The GUI MUST provide the user with a search function that allows the user to enter a CWE identifier and retrieve the related elements ("CWE-Searchable").

**B.4.2)** If the GUI lists details for an individual element, then it MUST list the CWE identifiers that map to that element ("CWE-Output"). Otherwise, the GUI MUST provide the user with a mapping in a format that satisfies the B.3.1 Electronic Documents requirement.

**B.4.3)** The GUI SHOULD allow the user to export or access CWE-related data in an alternate format that satisfies the B.3.1 Electronic Documents requirement.

## Learn More about CWE Compatibility

http://cwe.mitre.org/compatible/index.html