

---

---

**Information technology — Software  
measurement — Software quality  
measurement — Automated source  
code quality measures**

**iTeh Standards**  
**(<https://standards.itih.ai>)**  
**Document Preview**

[ISO/IEC 5055:2021](https://standards.itih.ai/catalog/standards/iso/17e93555-8fbc-47c2-8495-32371a9a0d7c/iso-iec-5055-2021)

<https://standards.itih.ai/catalog/standards/iso/17e93555-8fbc-47c2-8495-32371a9a0d7c/iso-iec-5055-2021>



**iTeh Standards**  
**(<https://standards.iteh.ai>)**  
**Document Preview**

[ISO/IEC 5055:2021](https://standards.iteh.ai/catalog/standards/iso/17e93555-8fbc-47c2-8495-32371a9a0d7c/iso-iec-5055-2021)

<https://standards.iteh.ai/catalog/standards/iso/17e93555-8fbc-47c2-8495-32371a9a0d7c/iso-iec-5055-2021>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier; Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

## Contents

<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>1.1</b>	<b>Purpose .....</b>	<b>1</b>
<b>1.2</b>	<b>Overview of Structural Quality Measurement in Software.....</b>	<b>1</b>
<b>2</b>	<b>Conformance .....</b>	<b>2</b>
<b>3</b>	<b>Normative References.....</b>	<b>3</b>
<b>4</b>	<b>Terms and Definitions .....</b>	<b>4</b>
<b>5</b>	<b>Symbols (and Abbreviated Terms) .....</b>	<b>7</b>
<b>6</b>	<b>Weaknesses Included in Quality Measures and Representation Metamodels.....</b>	<b>8</b>
<b>6.1</b>	<b>Purpose .....</b>	<b>8</b>
<b>6.2</b>	<b>Software Product Inputs .....</b>	<b>8</b>
<b>6.3</b>	<b>Automated Source Code Quality Measure Elements.....</b>	<b>8</b>
<b>6.4</b>	<b>Automated Source Code Maintainability Measure Element Descriptions .....</b>	<b>9</b>
<b>6.5</b>	<b>Automated Source Code Performance Efficiency Measure Element Descriptions .....</b>	<b>11</b>
<b>6.6</b>	<b>Automated Source Code Reliability Measure Element Descriptions .....</b>	<b>15</b>
<b>6.7</b>	<b>Automated Source Code Security Measure Element Descriptions .....</b>	<b>23</b>
<b>6.8</b>	<b>Introduction to the Specification of Quality Measure Elements .....</b>	<b>32</b>
<b>6.9</b>	<b>Knowledge Discovery Metamodel (KDM).....</b>	<b>32</b>
<b>6.10</b>	<b>Software Patterns Metamodel Standard (SPMS).....</b>	<b>36</b>
<b>6.11</b>	<b>Reading guide.....</b>	<b>37</b>
<b>7</b>	<b>List of ASCQM Weaknesses.....</b>	<b>38</b>
<b>7.1</b>	<b>Weakness Category Maintainability .....</b>	<b>38</b>
<b>7.1.1</b>	<b>CWE-407 Algorithmic Complexity .....</b>	<b>38</b>
<b>7.1.2</b>	<b>CWE-478 Missing Default Case in Switch Statement.....</b>	<b>38</b>
<b>7.1.3</b>	<b>Weakness CWE-480 Use of Incorrect Operator .....</b>	<b>38</b>
<b>7.1.4</b>	<b>CWE-484 Omitted Break Statement in Switch .....</b>	<b>39</b>
<b>7.1.5</b>	<b>CWE-561 Dead Code .....</b>	<b>39</b>
<b>7.1.6</b>	<b>CWE-570 Expression is Always False .....</b>	<b>39</b>
<b>7.1.7</b>	<b>CWE-571 Expression is Always True .....</b>	<b>39</b>
<b>7.1.8</b>	<b>CWE-783 Operator Precedence Logic Error .....</b>	<b>40</b>
<b>7.1.9</b>	<b>CWE-1075 Unconditional Control Flow Transfer Outside of Switch Block .....</b>	<b>40</b>
<b>7.1.10</b>	<b>CWE-1121 Excessive McCabe Cyclomatic Complexity Value.....</b>	<b>40</b>
<b>7.1.11</b>	<b>CWE-1054 Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer (Layer-skipping Call).....</b>	<b>41</b>
<b>7.1.12</b>	<b>CWE-1064 Invokable Control Element with Signature Containing an Excessive Number of Parameters .....</b>	<b>41</b>
<b>7.1.13</b>	<b>CWE-1084 Invokable Control Element with Excessive File or Data Access Operations .....</b>	<b>41</b>
<b>7.1.14</b>	<b>CWE-1051 Initialization with Hard-Coded Network Resource Configuration Data ...</b>	<b>42</b>
<b>7.1.15</b>	<b>CWE-1090 Method Containing Access of a Member Element from Another Class .....</b>	<b>42</b>
<b>7.1.16</b>	<b>CWE-1074 Class with Excessively Deep Inheritance .....</b>	<b>42</b>
<b>7.1.17</b>	<b>CWE-1086 Class with Excessive Number of Child Classes.....</b>	<b>43</b>
<b>7.1.18</b>	<b>CWE-1041 Use of Redundant Code (Copy-Paste) .....</b>	<b>43</b>
<b>7.1.19</b>	<b>CWE-1055 Multiple Inheritance from Concrete Classes.....</b>	<b>43</b>
<b>7.1.20</b>	<b>CWE-1045 Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor .....</b>	<b>44</b>
<b>7.1.21</b>	<b>CWE-1052 Excessive Use of Hard-Coded Literals in Initialization .....</b>	<b>44</b>

7.1.22 CWE-1048 Invokable Control Element with Large Number of Outward Calls (Excessive Coupling or Fan-out) .....44

7.1.23 CWE-1095 Loop Condition Value Update within the Loop .....45

7.1.24 CWE-1085 Invokable Control Element with Excessive Volume of Commented-out Code .....45

7.1.25 CWE-1047 Modules with Circular Dependencies .....45

7.1.26 CWE-1080 Source Code File with Excessive Number of Lines of Code .....46

7.1.27 CWE-1062 Parent Class Element with References to Child Class .....46

7.1.28 CWE-1087 Class with Virtual Method without a Virtual Destructor .....46

7.1.29 CWE-1079 Parent Class without Virtual Destructor Method .....47

7.1.30 Maintainability Detection Patterns .....47

7.2 Weakness Category Performance Efficiency .....48

7.2.1 CWE-401 Improper Release of Memory Before Removing Last Reference ('Memory Leak') .....48

7.2.2 Weakness CWE-404 Improper Resource Shutdown or Release .....48

7.2.3 CWE-424 Improper Protection of Alternate Path .....49

7.2.4 CWE-772 Missing Release of Resource after Effective Lifetime .....49

7.2.5 CWE-775 Missing Release of File Descriptor or Handle after Effective Lifetime .....49

7.2.6 CWE-1073 Non-SQL Invokable Control Element with Excessive Number of Data Resource Access .....49

7.2.7 CWE-1057 Data Access Operations Outside of Designated Data Manager Component .....50

7.2.8 CWE-1043 Storable and Member Data Element Excessive Number of Aggregated Storable and Member Data Elements .....50

7.2.9 CWE-1072 Data Resource Access without use of Connection Pooling .....50

7.2.10 CWE-1060 Excessive Number of Inefficient Server-Side Data Accesses .....51

7.2.11 CWE-1091 Use of Object without Invoking Destructor Method .....51

7.2.12 CWE-1046 Creation of Immutable Text Using String Concatenation .....51

7.2.13 CWE-1042 Static Member Data Element outside of a Singleton Class Element .....52

7.2.14 CWE-1049 Excessive Data Query Operations in a Large Data Table .....52

7.2.15 CWE-1067 Excessive Execution of Sequential Searches of Data Resource .....52

7.2.16 CWE-1089 Large Data Table with Excessive Number of Indices .....53

7.2.17 CWE-1094 Excessive Index Range Scan for a Data Resource .....53

7.2.18 CWE-1050 Excessive Platform Resource Consumption within a Loop .....53

7.2.19 CWE-1060 Excessive Number of Inefficient Server-Side Data Accesses .....54

7.2.20 Performance Efficiency Detection Patterns .....54

7.3 Weakness Category Reliability .....54

7.3.1 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer .....54

7.3.2 CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') .....55

7.3.3 CWE-123 Write-what-where Condition .....55

7.3.4 CWE-125 Out-of-bounds Read .....56

7.3.5 CWE-130 Improper Handling of Length Parameter Inconsistency .....56

7.3.6 CWE-131 Incorrect Calculation of Buffer Size .....56

7.3.7 CWE-170 Improper Null Termination .....57

7.3.8 CWE-194 Unexpected Sign Extension .....57

7.3.9 CWE-195 Signed to Unsigned Conversion Error .....57

7.3.10 CWE-196 Unsigned to Signed Conversion Error .....58

7.3.11 CWE-197 Numeric Truncation Error .....58

7.3.12 CWE-248 Uncaught Exception .....58

7.3.13 CWE-252 Unchecked Return Value .....59

7.3.14 CWE-366 Race Condition within a Thread .....59

7.3.15 CWE-369 Divide by Zero .....59

7.3.16	CWE-390 Detection of Error Condition Without Action .....	59
7.3.17	CWE-391 Unchecked Error Condition .....	60
7.3.18	CWE-392 Missing Report of Error Condition .....	60
7.3.19	CWE-394 Unexpected Status Code or Return Value .....	60
7.3.20	CWE-401 Improper Release of Memory Before Removing Last Reference ('Memory Leak') .....	61
7.3.21	CWE-404 Improper Resource Shutdown or Release .....	61
7.3.22	CWE-415 Double Free .....	61
7.3.23	CWE-416 Use After Free .....	62
7.3.24	CWE-424 Improper Protection of Alternate Path .....	62
7.3.25	CWE-456 Missing Initialization of a Variable .....	62
7.3.26	CWE-459 Incomplete Cleanup .....	63
7.3.27	CWE-476 NULL Pointer Dereference .....	63
7.3.28	CWE-480 Use of Incorrect Operator .....	63
7.3.29	CWE-484 Omitted Break Statement in Switch .....	64
7.3.30	CWE-543 Use of Singleton Pattern Without Synchronization in a Multithreaded Context .....	64
7.3.31	CWE-562 Return of Stack Variable Address .....	64
7.3.32	CWE-567 Unsynchronized Access to Shared Data in a Multithreaded Context .....	64
7.3.33	CWE-595 Comparison of Object References Instead of Object Contents .....	65
7.3.34	CWE-597 Use of Wrong Operator in String Comparison .....	65
7.3.35	CWE-662 Improper Synchronization .....	65
7.3.36	CWE-667 Improper Locking .....	66
7.3.37	CWE-672 Operation on a Resource after Expiration or Release .....	67
7.3.38	CWE-681 Incorrect Conversion between Numeric Types .....	67
7.3.39	CWE-682 Incorrect Calculation .....	67
7.3.40	CWE-703 Improper Check or Handling of Exceptional Conditions .....	68
7.3.41	CWE-704 Incorrect Type Conversion or Cast .....	68
7.3.42	CWE-758 Reliance on Undefined, Unspecified, or Implementation-Defined Behavior .....	68
7.3.43	CWE-764 Multiple Locks of a Critical Resource .....	69
7.3.44	CWE-772 Missing Release of Resource after Effective Lifetime .....	69
7.3.45	CWE-775 Missing Release of File Descriptor or Handle after Effective Lifetime .....	69
7.3.46	CWE-786 Access of Memory Location Before Start of Buffer .....	70
7.3.47	CWE-787 Out-of-bounds Write .....	70
7.3.48	CWE-788 Access of Memory Location After End of Buffer .....	70
7.3.49	CWE-805 Buffer Access with Incorrect Length Value .....	71
7.3.50	CWE-820 Missing Synchronization .....	71
7.3.51	CWE-821 Incorrect Synchronization .....	71
7.3.52	7.3.52 CWE-822 Untrusted Pointer Dereference .....	72
7.3.53	7.3.53 CWE-823 Use of Out-of-range Pointer Offset .....	72
7.3.54	CWE-824 Access of Uninitialized Pointer .....	72
7.3.55	CWE-825 Expired Pointer Dereference .....	73
7.3.56	CWE-833 Deadlock .....	73
7.3.57	CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop') .....	73
7.3.58	CWE-908 Use of Uninitialized Resource .....	74
7.3.59	CWE-1083 Data Access from Outside Designated Data Manager Component .....	74
7.3.60	CWE-1058 Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element .....	74
7.3.61	CWE-1096 Singleton Class Instance Creation without Proper Locking or Synchronization .....	75
7.3.62	CWE-1087 Class with Virtual Method without a Virtual Destructor .....	75
7.3.63	CWE-1079 Parent Class without Virtual Destructor Method .....	75

7.3.64 CWE-1045 Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor .....76

7.3.65 CWE-1051 Initialization with Hard-Coded Network Resource Configuration Data ...76

7.3.66 CWE-1088 Synchronous Access of Remote Resource without Timeout.....76

7.3.67 CWE-1066 Missing Serialization Control Element .....77

7.3.68 CWE-1070 Serializable Storable Data Element with non-Serializable Item Elements .....77

7.3.69 CWE-1097 Persistent Storable Data Element without Associated Comparison Control Element.....77

7.3.70 CWE-1098 Data Element containing Pointer Item without Proper Copy Control Element.....77

7.3.71 CWE-1082 Class Instance Self Destruction Control Element.....78

7.3.72 CWE-1077 Floating Point Comparison with Incorrect Operator .....78

7.3.73 CWE-665 Improper Initialization.....78

7.3.74 CWE-457 Use of Uninitialized Variable .....79

7.3.75 Reliability Detection Patterns .....79

7.4 Weakness Category Security .....80

7.4.1 Improper Restriction of Operations within the Bounds of a Memory Buffer.....80

7.4.2 CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').....81

7.4.3 CWE-123 Write-what-where Condition .....81

7.4.4 CWE-125 Out-of-bounds Read .....82

7.4.5 CWE-129 Improper Validation of Array Index .....82

7.4.6 CWE-130 Improper Handling of Length Parameter Inconsistency.....82

7.4.7 CWE-131 Incorrect Calculation of Buffer Size.....83

7.4.8 CWE-134 Use of Externally-Controlled Format String.....83

7.4.9 CWE-194 Unexpected Sign Extension .....83

7.4.10 CWE-195 Signed to Unsigned Conversion Error .....83

7.4.11 CWE-196 Unsigned to Signed Conversion Error .....84

7.4.12 CWE-197 Numeric Truncation Error.....84

7.4.13 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') .....84

7.4.14 CWE-23 Relative Path Traversal.....85

7.4.15 CWE-252 Unchecked Return Value.....85

7.4.16 CWE-259 Use of Hard-coded Password.....85

7.4.17 CWE-321 Use of Hard-coded Cryptographic Key .....86

7.4.18 CWE-36 Absolute Path Traversal .....86

7.4.19 CWE-366 Race Condition within a Thread .....86

7.4.20 CWE-369 Divide by Zero .....87

7.4.21 CWE-401 Improper Release of Memory Before Removing Last Reference ('Memory Leak') .....87

7.4.22 CWE-404 Improper Resource Shutdown or Release .....87

7.4.23 CWE-424 Improper Protection of Alternate Path.....88

7.4.24 CWE-434 Unrestricted Upload of File with Dangerous Type .....88

7.4.25 CWE-456 Missing Initialization of a Variable.....88

7.4.26 CWE-457 Use of Uninitialized Variable .....89

7.4.27 CWE-477 Use of Obsolete Function.....89

7.4.28 CWE-480 Use of Incorrect Operator .....89

7.4.29 CWE-502 Deserialization of Untrusted Data .....90

7.4.30 CWE-543 Use of Singleton Pattern Without Synchronization in a Multithreaded Context .....90

7.4.31 CWE-564 SQL Injection: Hibernate .....90

7.4.32 CWE-567 Unsynchronized Access to Shared Data in a Multithreaded Context .....90

7.4.33 CWE-570 Expression is Always False .....91

7.4.34	CWE-571 Expression is Always True .....	91
7.4.35	CWE-606 Unchecked Input for Loop Condition .....	91
7.4.36	CWE-643 Improper Neutralization of Data within XPath Expressions ('XPath Injection') .....	92
7.4.37	CWE-652 Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') .....	92
7.4.38	CWE-662 Improper Synchronization .....	92
7.4.39	CWE-665 Improper Initialization .....	93
7.4.40	CWE-667 Improper Locking .....	93
7.4.41	CWE-672 Operation on a Resource after Expiration or Release .....	94
7.4.42	CWE-681 Incorrect Conversion between Numeric Types .....	94
7.4.43	CWE-682 Incorrect Calculation .....	94
7.4.44	CWE-732 Incorrect Permission Assignment for Critical Resource .....	95
7.4.45	CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection') .....	95
7.4.46	CWE-772 Missing Release of Resource after Effective Lifetime .....	95
7.4.47	CWE-775 Missing Release of File Descriptor or Handle after Effective Lifetime .....	96
7.4.48	CWE-778 Insufficient Logging .....	96
7.4.49	CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') .....	96
7.4.50	CWE-783 Operator Precedence Logic Error .....	97
7.4.51	CWE-786 Access of Memory Location Before Start of Buffer .....	97
7.4.52	CWE-787 Out-of-bounds Write .....	97
7.4.53	CWE-788 Access of Memory Location After End of Buffer .....	98
7.4.54	CWE-789 Uncontrolled Memory Allocation .....	98
7.4.55	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') .....	98
7.4.56	CWE-798 Use of Hard-coded Credentials .....	98
7.4.57	CWE-805 Buffer Access with Incorrect Length Value .....	99
7.4.58	CWE-820 Missing Synchronization .....	99
7.4.59	CWE-821 Incorrect Synchronization .....	100
7.4.60	CWE-822 Untrusted Pointer Dereference .....	100
7.4.61	CWE-823 Use of Out-of-range Pointer Offset .....	100
7.4.62	CWE-824 Access of Uninitialized Pointer .....	101
7.4.63	CWE-825 Expired Pointer Dereference .....	101
7.4.64	CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop') .....	101
7.4.65	CWE-88 Argument Injection or Modification .....	101
7.4.66	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') .....	102
7.4.67	CWE-90 Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') .....	102
7.4.68	CWE-91 XML Injection (aka Blind XPath Injection) .....	102
7.4.69	CWE-99 Improper Control of Resource Identifiers ('Resource Injection') .....	103
7.4.70	CWE-611 Improper Restriction of XML External Entity Reference ('XXE') .....	103
7.4.71	CWE-1057 Data Access Control Element from Outside Designated Data Manager Component .....	103
7.4.72	CWE-415 Double Free .....	104
7.4.73	CWE-416 Use After Free .....	104
7.4.74	Security Detection Patterns .....	104
8	ASCQM Weakness Detection Patterns .....	107
8.1	Specification of Detection Patterns .....	107
8.2	ASCQM Check Index of Array Access .....	107