

Date: May 2016

Style Definition: Body Text: Font color: Black, (none), Do not check spelling or grammar, Space Before: 8 pt, Hyphenate, Allow hanging punctuation, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Font Alignment: Auto

Operational Threat and Risk Information Sharing and Federation Model

OMG Document Numbers

INVENTORY SYSA/XX

SUBMISSION DOCUMENT SYSA/2016-12-01 (THIS DOCUMENT)

NON-NORMATIVE ARTIFACTS (ZIP) SYSA/2016-12-02

THREAT/RISK CONCEPTUAL MODEL CONCEPTUAL REFERENCE MODEL XMI SYSA/XX

SMIF PROFILE XMI SYSA/XX

NIEM MAPPING MODEL XMI SYSA/XX

STIX UML MODEL XMI SYSA/XX

STIX MAPPING MODEL SYSA/XX

Normative reference: <http://www.omg.org/spec/threat/1.0/>

Copyright © 2016, Object Management Group, Inc.

Copyright © 2016, Model Driven Solutions division of Data Access Technologies, Inc.

Copyright © 2016, KDM Analytics, Inc.

Copyright © 2016, International Business Machines, Inc.

Copyright © 2016, EMC, Inc.

Copyright © 2016, Oracle Corporation

Copyright © 2016, Fujitsu Corporation

USE OF SPECIFICATION - TERMS, CONDITIONS & NOTICES

The material in this document details an Object Management Group specification in accordance with the terms, conditions and notices set forth below. This document does not represent a commitment to implement any portion of this specification in any company's products. The information contained in this document is subject to change without notice.

LICENSES

The companies listed above have granted to the Object Management Group, Inc. (OMG) a nonexclusive, royalty-free, paid up, worldwide license to copy and distribute this document and to modify this document and distribute copies of the modified version. Each of the copyright holders listed above has agreed that no person shall be deemed to have infringed the copyright in the included material of any such copyright holder by reason of having used the specification set forth herein or having conformed any computer software to the specification.

Subject to all of the terms and conditions below, the owners of the copyright in this specification hereby grant you a fully-paid up, non-exclusive, nontransferable, perpetual, worldwide license (without the right to sublicense), to use this specification to create and distribute software and special purpose specifications that are based upon this specification, and to use, copy, and distribute this specification as provided under the Copyright Act; provided that: (1) both the copyright notice identified above and this permission notice appear on any copies of this specification; (2) the use of the specifications is for informational purposes and will not be copied or posted on any network computer or broadcast in any media and will not be otherwise resold or transferred for commercial purposes; and (3) no modifications are made to this specification. This limited permission automatically terminates without notice if you breach any of these terms or conditions. Upon termination, you will destroy immediately any copies of the specifications in your possession or control.

PATENTS

The attention of adopters is directed to the possibility that compliance with or adoption of OMG specifications may require use of an invention covered by patent rights. OMG shall not be responsible for identifying patents for which a license may be required by any OMG specification, or for conducting legal inquiries into the legal validity or scope of those patents that are brought to its attention. OMG specifications are prospective and advisory only. Prospective users are responsible for protecting themselves against liability for infringement of patents.

GENERAL USE RESTRICTIONS

Any unauthorized use of this specification may violate copyright laws, trademark laws, and communications regulations and statutes. This document contains information which is protected by copyright. All Rights Reserved. No part of this work covered by copyright herein may be reproduced or used in any form or by any means--graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems--without permission of the copyright owner.

DISCLAIMER OF WARRANTY

WHILE THIS PUBLICATION IS BELIEVED TO BE ACCURATE, IT IS PROVIDED "AS IS" AND MAY CONTAIN ERRORS OR MISPRINTS. THE OBJECT MANAGEMENT GROUP AND THE COMPANIES LISTED ABOVE MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS PUBLICATION, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF TITLE OR OWNERSHIP, IMPLIED WARRANTY OF MERCHANTABILITY OR WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE OR USE. IN NO EVENT SHALL THE OBJECT MANAGEMENT GROUP OR ANY OF THE COMPANIES LISTED ABOVE BE LIABLE FOR ERRORS CONTAINED HEREIN OR FOR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, RELIANCE OR COVER DAMAGES, INCLUDING LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY ANY USER OR ANY THIRD PARTY IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The entire risk as to the quality and performance of software developed using this specification is borne by you. This disclaimer of warranty constitutes an essential part of the license granted to you to use this specification.

RESTRICTED RIGHTS LEGEND

Use, duplication or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c) (1) (ii) of The Rights in Technical Data and Computer Software Clause at DFARS 252.227-7013 or in subparagraph (c)(1) and (2) of the Commercial Computer Software - Restricted Rights clauses at 48 C.F.R. 52.227-19 or as specified in 48 C.F.R. 227-7202-2 of the DoD F.A.R. Supplement and its successors, or as specified in 48 C.F.R. 12.212 of the Federal Acquisition Regulations and its successors, as applicable. The specification copyright owners are as indicated above and may be contacted through the Object Management Group, 109 Highland Avenue, Needham, MA 02494, U.S.A.

TRADEMARKS

IMM®, MDA®, Model Driven Architecture®, UML®, UML Cube logo®, OMG Logo®, CORBA® and XMI® are registered trademarks of the Object Management Group, Inc., and Object Management Group™, OMG™, Unified Modeling Language™, Model Driven Architecture Logo™, Model Driven Architecture Diagram™, CORBA logos™, XMI Logo™, CWM™, CWM Logo™, IIOP™, MOF™, OMG Interface Definition Language (IDL)™, and OMG SysML™ are trademarks of the Object Management Group. All other products or company names mentioned are used for identification purposes only, and may be trademarks of their respective owners.

COMPLIANCE

The copyright holders listed above acknowledge that the Object Management Group (acting itself or through its designees) is and shall at all times be the sole entity that may authorize developers, suppliers, and sellers of computer software to use certification marks, trademarks, or other special designations to indicate compliance with these materials.

Software developed under the terms of this license may claim compliance or conformance with this specification if and only if the software compliance is of a nature fully matching the applicable compliance points as stated in the specification. Software developed only partially matching the applicable compliance points may claim only that the software was based on this specification, but may not claim compliance or conformance with this specification. In the event that testing suites are implemented or approved by Object Management Group, Inc., software developed using this specification may claim compliance or conformance with the specification only if the software satisfactorily completes the testing suites.

OMG's Issue Reporting Procedure

All OMG specifications are subject to continuous review and improvement. As part of this process we encourage readers to report any ambiguities, inconsistencies, or inaccuracies they may find by completing the Issue

Reporting Form listed on the main web page <http://www.omg.org>, under Documents, Report a Bug/Issue
(http://www.omg.org/report_issue.)

Table of Contents

0	Submission-related material.....	42
0.1	Submission Introduction.....	42
0.2	Submission Team	42
0.2.1	Submitters	42
0.2.2	Contributors & Supporters.....	42
0.3	Proof of concept.....	43
0.4	Resolution of Requirements	44
0.4.1	Mandatory requirements	44
0.4.2	Non-mandatory features.....	47
0.5	Resolution of Discussion Issues	47
1.1	Scope	49
2	Conformance.....	49
2.1	Canonical model conformance	50
2.2	Informatin model mapping conformance.....	50
2.3	STIX mapping conformance	50
2.4	NIEM mapping conformance	50
2.5	OWL mapping conformance	51
2.6	Conceptual reference modeling profile conformance.....	51
3	References	52
4	Terms and Definitions	53
5	Symbols and Notation.....	54
6	Additional Information	54
6.1	Acknowledgments	55
7	Operational Threat and Risk Guide (Non Normative).....	57
7.1	Mission and purpose.....	57
7.2	Technology capabilities.....	58
7.2.1	Federated analytics and simulation capabilities.....	58
7.2.2	Information Translating, Analytics, and Sharing capabilities	59
7.2.3	Risk Analytics Capabilities.....	60
7.2.4	Semantic federation and translation	62
7.3	Defining and Leveraging Conceptual reference models.....	66
7.3.1	Expressing conceptual reference models	66
7.3.2	Pivoting through conceptual reference models	68

7.3.3	Mapping to information and data models	68
7.3.4	Layering	69
7.3.5	Source of concepts.....	70
7.4	Modeling Style	73
7.4.1	Mixing Concepts with “multiple classification”	80
8	Operational Threat and Risk Model Reference.....	81
8.1	Threat-risk-conceptual-model::Threat and Risk Specific Concepts	81
8.1.1	Diagram: Threat and Risk Specific Concepts	82
8.2	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Campaigns	84
8.2.1	Diagram: Campaign.....	84
8.2.2	Class Campaign	84
8.3	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger	85
8.3.1	Diagram: Danger	86
8.3.2	Class Attack <<Role>>.....	87
8.3.3	Class Indirect Threat <<Role>>	87
8.3.4	Class Natural Threat <<Role>>.....	87
8.3.5	Association Class Target of Attack <<Relationship>>.....	87
8.3.6	Class Threat <<Role>>.....	88
8.3.7	Class Unintentional Threat <<Role>>.....	89
8.4	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger Categories.....	90
8.4.1	Diagram: Danger Categories.....	90
8.4.2	Diagram: Danger Source Categories.....	91
8.4.3	Diagram: Failure Categories	92
8.4.4	Diagram: Impact Categories	93
8.4.5	Class Access Control Failure <<Category>>.....	93
8.4.6	Class Biological Danger <<Category>>.....	94
8.4.7	Class CBRN Danger <<Category>>.....	94
8.4.8	Class Chemical Danger <<Category>>	94
8.4.9	Class Civil Unrest Danger <<Category>>	94
8.4.10	Class Compliance Impact <<Category>>	94
8.4.11	Class Control Failure <<Category>>	94
8.4.12	Class Criminal Danger <<Category>>	95
8.4.13	Class Cyber Danger <<Category>>	95
8.4.14	Class Cyber System Failure <<Category>>	95
8.4.15	Class Danger Category <<Category>>	95
8.4.16	Class Decision-making Impact <<Category>>	95
8.4.17	Class Disinformation Impact <<Category>>	95

8.4.18	Class Electromagnetic Spectrum Impact <<Category>>	95
8.4.19	Class Environmental Impact <<Category>>.....	96
8.4.20	Class Failure Category <<Category>>.....	96
8.4.21	Class Financial Impact <<Category>>	96
8.4.22	Class Fire Danger <<Category>>.....	96
8.4.23	Class Geophysical Danger <<Category>>.....	96
8.4.24	Class Health Impact <<Category>>.....	96
8.4.25	Class Identity Theft <<Category>>	97
8.4.26	Class Image Impact <<Category>>	97
8.4.27	Class Impact Category <<Category>>.....	97
8.4.28	Class Inability to Communicate Impact <<Category>>.....	97
8.4.29	Class Industrial Control Failure <<Category>>.....	97
8.4.30	Class Information Impact <<Category>>	97
8.4.31	Class Information Loss Impact <<Category>>.....	98
8.4.32	Class Infrastructure Impact <<Category>>.....	98
8.4.33	Class Intellectual Property Impact <<Category>>.....	98
8.4.34	Class Legal Impact <<Category>>	98
8.4.35	Class Loss of Control Danger <<Category>>.....	98
8.4.36	Class Meteorological Danger <<Category>>	98
8.4.37	Class Mission Impact <<Category>>	99
8.4.38	Class Non-Technical Impact <<Category>>	99
8.4.39	Class Nuclear Danger <<Category>>	99
8.4.40	Class Physical System Failure <<Category>>	99
8.4.41	Class Process Failure <<Category>>	99
8.4.42	Class Radiological Danger <<Category>>	99
8.4.43	Class Safety Danger <<Category>>	100
8.4.44	Class Safety Impact <<Category>>	100
8.4.45	Class Security Danger <<Category>>	100
8.4.46	Class Source of Danger Category <<Category>>	100
8.4.47	Class System Failure <<Category>>	100
8.4.48	Class Terrorism Danger <<Category>>	100
8.4.49	Class Transport Impact <<Category>>	101
8.4.50	Class War Danger <<Category>>	101
8.5	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger Sources.....	102
8.5.1	Diagram: Danger Sources.....	102
8.5.2	Class Accident <<Role>>.....	102
8.5.3	Association Class Contribution to Danger <<Relationship>>.....	103

8.5.4	<u>Class Danger Source <<Role>></u>	103
8.5.5	<u>Class Dangerous Condition <<Role>></u>	103
8.5.6	<u>Class Dangerous Event <<Role>></u>	104
8.5.7	<u>Class Disrupt Stakeholder's Objective</u>	104
8.5.8	<u>Association Class Exploit of Vulnerability <<Relationship>></u>	104
8.5.9	<u>Class Objective to Disrupt</u>	105
8.5.10	<u>Class Unwitting Participant <<Role>></u>	106
8.6	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents and failures	107
8.6.1	<u>Diagram: Incident</u>	107
8.6.2	<u>Association Class Danger Leads to Incident <<Relationship>></u>	107
8.6.3	<u>Class Failure</u> 108	
8.6.4	<u>Association Class Failure of Resource <<Relationship>></u>	109
8.6.5	<u>Class Incident <<Role>></u>	109
8.6.6	<u>Class Witness <<Role>></u>	110
8.6.7	<u>Association Class Witnessing <<Relationship>></u>	110
8.7	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Indicators	112
8.7.1	<u>Diagram: Indicator</u>	112
8.7.2	<u>Diagram: Sighting</u>	113
8.7.3	<u>Class Blacklist Indicator</u>	113
8.7.4	<u>Class Indicator</u>	113
8.7.5	<u>Association Class Indicator Indicates Situation <<Relationship>></u>	114
8.7.6	<u>Class Indicator Pattern</u>	115
8.7.7	<u>Class Indicator Watchlist</u>	115
8.7.8	<u>Association Class Sighting <<Relationship>></u>	115
8.7.9	<u>Association Class Sighting Indicates Situation <<Relationship>></u>	116
8.7.10	<u>Association Class Sighting Matches Indicator <<Relationship>></u>	117
8.7.11	<u>Association Class Watch <<Relationship>></u>	118
8.7.12	<u>Class Whitelist Indicator</u>	119
8.8	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk	120
8.8.1	<u>Diagram: Risk</u>	120
8.8.2	<u>Diagram: Risk Metrics</u>	121
8.8.3	<u>Class Accept Risk</u>	121
8.8.4	<u>Association Class Impose Strategy <<Relationship>></u>	121
8.8.5	<u>Class Objective for Safety and Security</u>	122
8.8.6	<u>Class Objective to Protect Assets</u>	122
8.8.7	<u>Class Risk</u> 122	
8.8.8	<u>Class Risk Mitigation Strategy</u>	123

8.8.9	Class Risk Owner <<Role>>.....	123
8.8.10	Class Risk Reduction Objective.....	124
8.8.11	Association Class Risk To Resource <<Relationship>>.....	125
8.8.12	Association Class Risk Topic <<Relationship>>	125
8.8.13	Association Class Stakeholder Risk <<Relationship>>.....	126
8.8.14	Class Threat Likelihood <<Quantity Kind>>.....	127
8.8.15	Association Class Valuation of Asset <<Relationship>>	128
8.8.16	Class Valued Asset <<Role>>.....	128
8.9	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments	131
8.9.1	Diagram: Risk Treatment.....	131
8.9.2	Diagram: Safeguard Monitoring	132
8.9.3	Association Class Assume Risk <<Relationship>>.....	132
8.9.4	Class Avoid Danger	133
8.9.5	Class Countermeasure <<Role>>.....	133
8.9.6	Association Class Countermeasure for Strategy <<Relationship>>	134
8.9.7	Association Class Countermeasure Mitigates <<Relationship>>	134
8.9.8	Class Mitigation Actor <<Role>>	135
8.9.9	Association Class Monitor <<Relationship>>.....	135
8.9.10	Class Monitoring Safeguard	136
8.9.11	Association Class Protection <<Relationship>>.....	136
8.9.12	Class Risk Agent <<Role>>	137
8.9.13	Association Class Risk Treatment <<Relationship>>	138
8.9.14	Class Risk Treatment Strategy.....	138
8.9.15	Class Safeguard Activity.....	139
8.9.16	Association Class Safeguarding <<Relationship>>.....	139
8.9.17	Class Transfer Risk.....	140
8.10	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Threat Actors	141
8.10.1	Diagram: Threat Actors	141
8.10.2	Class Disruptive Action <<Role>>.....	142
8.10.3	Association Class Perpetrate <<Relationship>>.....	142
8.10.4	Class Threat Actor <<Role>>	143
8.11	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Undesirable Situations	145
8.11.1	Diagram: Undesirable Situations	146
8.11.2	Class Harm	146
8.11.3	Association Class Harms Resource <<Relationship>>	147
8.11.4	Association Class Harms Victim <<Relationship>>	148
8.11.5	Association Class Source of Harm <<Relationship>>	149

8.11.6	Class Undesirable Condition <<Role>>.....	149
8.11.7	Class Undesirable Event <<Role>>.....	150
8.11.8	Class Undesirable Situation <<Role>>.....	150
8.11.9	Class Victim <<Role>>	151
8.12	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities.....	152
8.12.1	Diagram: Vulnerability	152
8.12.2	Diagram: Vulnerability Identifiers.....	153
8.12.3	Class Physical Vulnerability	153
8.12.4	Association Class Supporting Condition <<Relationship>>.....	153
8.12.5	Class Vulnerability	154
8.12.6	Class Vulnerability Identifier <<Value>>	155
8.12.7	Class Vulnerability Metric <<Quantity Kind>>	156
8.12.8	Association Class Vulnerability of Resource <<Relationship>>.....	156
8.13	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Cyber Vulnerabilities.....	157
8.13.1	Diagram: Cyber Vulnerability	157
8.13.2	Class Communications Vulnerability.....	157
8.13.3	Class CVE Identifier <<Value>>	158
8.13.4	Class Cyber Vulnerability	158
8.13.5	Class Information System Vulnerability	158
8.13.6	Class Information Vulnerability.....	158
8.13.7	Class OSVDB Identifier <<Value>>	159
8.13.8	Class Software Vulnerability	159
8.14	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability Vectors.....	160
8.14.1	Diagram: Vulnerability Vectors.....	161
8.14.2	Class CVSS Score <<Quantity Kind>>.....	162
8.15	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Weapons	172
8.15.1	Diagram: Weapons	172
8.15.2	Class Physical Weapon <<Role>>	172
8.15.3	Class Weapon <<Role>>.....	172
8.15.4	Association Class Weapon Leverages Vulnerability <<Relationship>>	173
9	Generic Concept Library (Normative).....	174
9.1	Threat-risk-conceptual-model::Generic Concept Library.....	174
9.1.1	Diagram: Generic Concept Library.....	174
9.2	Threat-risk-conceptual-model::Generic Concept Library::Abilities	176
9.2.1	Diagram: Ability	176

<u>9.2.2</u>	<u>Diagram: Alter ability or control</u>	<u>177</u>
<u>9.2.3</u>	<u>Association Class Ability <<Relationship>>.....</u>	<u>177</u>
<u>9.2.4</u>	<u>Association Class Affected Available Resource <<Relationship>>.....</u>	<u>178</u>
<u>9.2.5</u>	<u>Class Alter Ability</u>	<u>179</u>
<u>9.2.6</u>	<u>Association Class Capability <<Relationship>></u>	<u>180</u>
<u>9.2.7</u>	<u>Class Facilitator <<Role>>.....</u>	<u>180</u>
<u>9.2.8</u>	<u>Class Lose Ability.....</u>	<u>181</u>
<u>9.2.9</u>	<u>Class Obtain Ability.....</u>	<u>181</u>
<u>9.2.10</u>	<u>Association Class Strenthened Actor <<Relationship>>.....</u>	<u>181</u>
<u>9.2.11</u>	<u>Class Transfer Ability</u>	<u>182</u>
<u>9.2.12</u>	<u>Association Class Weakened Actor <<Relationship>></u>	<u>182</u>
<u>9.3</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Assessments</u>	<u>184</u>
<u>9.3.1</u>	<u>Diagram: Assessment.....</u>	<u>184</u>
<u>9.3.2</u>	<u>Class Assessed Entity <<Role>>.....</u>	<u>184</u>
<u>9.3.3</u>	<u>Class Assessment</u>	<u>185</u>
<u>9.3.4</u>	<u>Class Assessment Activity</u>	<u>185</u>
<u>9.3.5</u>	<u>Association Class Entity Assessment <<Relationship>></u>	<u>185</u>
<u>9.4</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Contact Information</u>	<u>187</u>
<u>9.4.1</u>	<u>Diagram: Contact Information</u>	<u>188</u>
<u>9.4.2</u>	<u>Class Communications Security Level <<Value>></u>	<u>189</u>
<u>9.4.3</u>	<u>Class Contact Means <<Value>></u>	<u>189</u>
<u>9.4.4</u>	<u>Association Class Contact Via <<Relationship>>.....</u>	<u>189</u>
<u>9.4.5</u>	<u>Class Contactable.....</u>	<u>190</u>
<u>9.4.6</u>	<u>Class Electronic Contact <<Value>></u>	<u>191</u>
<u>9.4.7</u>	<u>Class Email Address <<Value>></u>	<u>191</u>
<u>9.4.8</u>	<u>Class Internet Contact <<Value>></u>	<u>192</u>
<u>9.4.9</u>	<u>Class Network Identifier <<Value>>.....</u>	<u>192</u>
<u>9.4.10</u>	<u>Class Postal Address <<Value>></u>	<u>192</u>
<u>9.4.11</u>	<u>Class Postal Address Structured <<Value>></u>	<u>192</u>
<u>9.4.12</u>	<u>Class Postal Address Text <<Value>></u>	<u>193</u>
<u>9.4.13</u>	<u>Class Postal Code <<Value>></u>	<u>194</u>
<u>9.4.14</u>	<u>Class Private Network Contact <<Value>>.....</u>	<u>194</u>
<u>9.4.15</u>	<u>Class Radio Contact <<Value>></u>	<u>194</u>
<u>9.4.16</u>	<u>Class Social Network Contact <<Value>></u>	<u>195</u>
<u>9.4.17</u>	<u>Class Telephone Area Code <<Value>></u>	<u>195</u>
<u>9.4.18</u>	<u>Class Telephone Country Code <<Value>></u>	<u>195</u>
<u>9.4.19</u>	<u>Class Telephone Number <<Value>></u>	<u>195</u>

<u>9.4.20</u>	<u>Class Telephone Number Structured <<Value>>.....</u>	<u>196</u>
<u>9.4.21</u>	<u>Class Telephone Number Text <<Value>>.....</u>	<u>196</u>
<u>9.4.22</u>	<u>Class Website Contact <<Value>>.....</u>	<u>196</u>
<u>9.5</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Containment</u>	<u>199</u>
<u>9.5.1</u>	<u>Diagram: Containment.....</u>	<u>199</u>
<u>9.5.2</u>	<u>Diagram: Move Between Containers</u>	<u>200</u>
<u>9.5.3</u>	<u>Diagram: Physical Containment</u>	<u>201</u>
<u>9.5.4</u>	<u>Class Add To Container Event</u>	<u>201</u>
<u>9.5.5</u>	<u>Class Container <<Role>></u>	<u>201</u>
<u>9.5.6</u>	<u>Association Class Containment <<Relationship>>.....</u>	<u>202</u>
<u>9.5.7</u>	<u>Class Containment Event.....</u>	<u>203</u>
<u>9.5.8</u>	<u>Class Physical Container <<Role>>.....</u>	<u>203</u>
<u>9.5.9</u>	<u>Association Class Physical Containment <<Relationship>>.....</u>	<u>203</u>
<u>9.5.10</u>	<u>Association Class Recieving Container <<Relationship>></u>	<u>204</u>
<u>9.5.11</u>	<u>Class Relocation</u>	<u>204</u>
<u>9.5.12</u>	<u>Class Removal Event</u>	<u>204</u>
<u>9.5.13</u>	<u>Association Class Supplying Container <<Relationship>></u>	<u>205</u>
<u>9.6</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Control</u>	<u>206</u>
<u>9.6.1</u>	<u>Diagram: Control</u>	<u>206</u>
<u>9.6.2</u>	<u>Diagram: Control Authority</u>	<u>207</u>
<u>9.6.3</u>	<u>Diagram: Custody</u>	<u>207</u>
<u>9.6.4</u>	<u>Class Authority <<Role>>.....</u>	<u>208</u>
<u>9.6.5</u>	<u>Association Class Control <<Relationship>>.....</u>	<u>208</u>
<u>9.6.6</u>	<u>Class Controlled Entity <<Role>></u>	<u>209</u>
<u>9.6.7</u>	<u>Class Controlling Actor <<Role>>.....</u>	<u>210</u>
<u>9.6.8</u>	<u>Class Custodian <<Role>></u>	<u>210</u>
<u>9.6.9</u>	<u>Association Class Custody <<Relationship>></u>	<u>210</u>
<u>9.6.10</u>	<u>Class Leader <<Role>></u>	<u>211</u>
<u>9.6.11</u>	<u>Association Class Leadership <<Relationship>></u>	<u>211</u>
<u>9.6.12</u>	<u>Class Managed Entity <<Role>></u>	<u>211</u>
<u>9.6.13</u>	<u>Class Owner <<Role>></u>	<u>212</u>
<u>9.6.14</u>	<u>Association Class Ownership <<Relationship>></u>	<u>212</u>
<u>9.6.15</u>	<u>Association Class Possession <<Relationship>></u>	<u>212</u>
<u>9.6.16</u>	<u>Class Property <<Role>></u>	<u>213</u>
<u>9.6.17</u>	<u>Association Class Subject to Authority <<Relationship>></u>	<u>213</u>
<u>9.7</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Credentials</u>	<u>214</u>
<u>9.7.1</u>	<u>Diagram: Credentials and Managed Identifiers</u>	<u>214</u>

<u>9.7.2</u>	<u>Association Actor Identifier of Credential.....</u>	214
<u>9.7.3</u>	<u>Association Class Attest to Ability <<Relationship>></u>	215
<u>9.7.4</u>	<u>Class Credential</u>	216
<u>9.7.5</u>	<u>Class Identity Provider <<Role>>.....</u>	216
<u>9.7.6</u>	<u>Association Class Issue Credential <<Relationship>></u>	217
<u>9.7.7</u>	<u>Class Managed Actor Identifier <<Value>>.....</u>	217
<u>9.7.8</u>	<u>Association Class Valid for Time Interval <<Relationship>>.....</u>	218
<u>9.8</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Cyber.....</u>	219
<u>9.8.1</u>	<u>Diagram: Cyber</u>	220
<u>9.8.2</u>	<u>Diagram: Cyber Platforms</u>	221
<u>9.8.3</u>	<u>Diagram: Cyber Resource.....</u>	221
<u>9.8.4</u>	<u>Association Class Ability To Execute Software <<Relationship>></u>	222
<u>9.8.5</u>	<u>Association Class Automated Capability <<Relationship>>.....</u>	223
<u>9.8.6</u>	<u>Association Class Automated Control <<Relationship>></u>	223
<u>9.8.7</u>	<u>Class Automated Entity <<Role>>.....</u>	224
<u>9.8.8</u>	<u>Class Automation Type.....</u>	225
<u>9.8.9</u>	<u>Class Automaton.....</u>	225
<u>9.8.10</u>	<u>Class Communicating Device</u>	225
<u>9.8.11</u>	<u>Class Communications Link</u>	225
<u>9.8.12</u>	<u>Class Communications Network.....</u>	226
<u>9.8.13</u>	<u>Class Computer Control System <<Role>>.....</u>	226
<u>9.8.14</u>	<u>Class Computer System</u>	226
<u>9.8.15</u>	<u>Class Cyber Resource <<Union>></u>	227
<u>9.8.16</u>	<u>Class Cyber Weapon <<Role>></u>	227
<u>9.8.17</u>	<u>Class Execution Platform <<Union>>.....</u>	227
<u>9.8.18</u>	<u>Association Class Information In Computer <<Relationship>></u>	228
<u>9.8.19</u>	<u>Association Class Node of a Network <<Relationship>></u>	228
<u>9.8.20</u>	<u>Class Software</u>	229
<u>9.9</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Enterprises.....</u>	230
<u>9.9.1</u>	<u>Diagram: Enterprise</u>	230
<u>9.9.2</u>	<u>Class Enterprise</u>	231
<u>9.10</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Entities</u>	232
<u>9.10.1</u>	<u>Diagram: Identifiable Entity</u>	233
<u>9.10.2</u>	<u>Diagram: Identifiable Entity Relationships.....</u>	234
<u>9.10.3</u>	<u>Association Class Impact <<Relationship>></u>	234
<u>9.10.4</u>	<u>Association Class Parthood <<Relationship>>.....</u>	235
<u>9.10.5</u>	<u>Association Class Related <<Relationship>>.....</u>	236

<u>9.11</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Events and Activities.....</u>	238
<u>9.11.1</u>	<u>Diagram: Events and Activities</u>	238
<u>9.11.2</u>	<u>Class Activity.....</u>	239
<u>9.11.3</u>	<u>Class Actor</u> 239	
<u>9.11.4</u>	<u>Class Actual Activity <<Intersection>>.....</u>	241
<u>9.11.5</u>	<u>Class Actual Event <<Intersection>></u>	241
<u>9.11.6</u>	<u>Class Event</u> 242	
<u>9.11.7</u>	<u>Association Class Output <<Relationship>>.....</u>	242
<u>9.11.8</u>	<u>Association Class Performance <<Relationship>>.....</u>	243
<u>9.11.9</u>	<u>Association Class Usage <<Relationship>></u>	244
<u>9.12</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Identifiers and Coordinates</u>	245
<u>9.12.1</u>	<u>Diagram: Identifiers.....</u>	246
<u>9.12.2</u>	<u>Class Coordinate <<Value>></u>	246
<u>9.12.3</u>	<u>Class Coordinate System</u>	247
<u>9.12.4</u>	<u>Association System of Coordinate</u>	247
<u>9.13</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Information.....</u>	248
<u>9.13.1</u>	<u>Diagram: Information Action.....</u>	248
<u>9.13.2</u>	<u>Diagram: Information Objects</u>	249
<u>9.13.3</u>	<u>Diagram: Metadata</u>	250
<u>9.13.4</u>	<u>Class Add Information.....</u>	250
<u>9.13.5</u>	<u>Class Atomic Information Object</u>	251
<u>9.13.6</u>	<u>Class Close Information.....</u>	251
<u>9.13.7</u>	<u>Class Confidence</u>	251
<u>9.13.8</u>	<u>Association Confidence in Assertion</u>	251
<u>9.13.9</u>	<u>Association Class Contained Information <<Relationship>>.....</u>	252
<u>9.13.10</u>	<u>Class Create Information</u>	253
<u>9.13.11</u>	<u>Class Delete Information</u>	253
<u>9.13.12</u>	<u>Class Document</u>	253
<u>9.13.13</u>	<u>Class Information Action.....</u>	253
<u>9.13.14</u>	<u>Class Information Object.....</u>	254
<u>9.13.15</u>	<u>Class Information Repository</u>	254
<u>9.13.16</u>	<u>Class Information Resource <<Union>></u>	254
<u>9.13.17</u>	<u>Class Information Type</u>	255
<u>9.13.18</u>	<u>Class Modify Information</u>	255
<u>9.13.19</u>	<u>Class Open Information</u>	255
<u>9.13.20</u>	<u>Class Read Information</u>	255
<u>9.13.21</u>	<u>Class Remove Information.....</u>	256

<u>9.13.22</u>	<u>Class Structured Information Object</u>	256
<u>9.13.23</u>	<u>Class Transfer Information</u>	256
<u>9.14</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Locations</u>	257
<u>9.14.1</u>	<u>Diagram: Location</u>	257
<u>9.14.2</u>	<u>Diagram: Location Identification</u>	258
<u>9.14.3</u>	<u>Association Address of Location</u>	258
<u>9.14.4</u>	<u>Association Coordinate of location</u>	259
<u>9.14.5</u>	<u>Association Designation of a Location</u>	259
<u>9.14.6</u>	<u>Class Location ID <<Value>></u>	259
<u>9.14.7</u>	<u>Class Location Identifier <<Value>></u>	259
<u>9.14.8</u>	<u>Association Class Physical Boundary <<Relationship>></u>	260
<u>9.14.9</u>	<u>Class Physical Location</u>	260
<u>9.14.10</u>	<u>Class Physical Point</u>	261
<u>9.14.11</u>	<u>Class Point On Earth <<Value>></u>	261
<u>9.14.12</u>	<u>Association Reference Point</u>	262
<u>9.14.13</u>	<u>Class Relative Coordinate <<Value>></u>	262
<u>9.14.14</u>	<u>Class Spacial Coordinate <<Value>></u>	262
<u>9.14.15</u>	<u>Association Topological Region</u>	263
<u>9.14.16</u>	<u>Class Topology</u>	263
<u>9.14.17</u>	<u>Class World Geodetic System <<Value>></u>	263
<u>9.15</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Objectives</u>	265
<u>9.15.1</u>	<u>Diagram: Objectives</u>	265
<u>9.15.2</u>	<u>Class Benefit</u>	266
<u>9.15.3</u>	<u>Class Consequence</u>	266
<u>9.15.4</u>	<u>Association Class Consequence of Situation <<Relationship>></u>	268
<u>9.15.5</u>	<u>Class Desirability Assessment</u>	269
<u>9.15.6</u>	<u>Class Means <<Role>></u>	269
<u>9.15.7</u>	<u>Association Class Means To End <<Relationship>></u>	270
<u>9.15.8</u>	<u>Class Objective</u>	270
<u>9.15.9</u>	<u>Association Class Objective of Stakeholder <<Relationship>></u>	272
<u>9.15.10</u>	<u>Class Opportunity</u>	272
<u>9.15.11</u>	<u>Class Stakeholder <<Role>></u>	273
<u>9.15.12</u>	<u>Association Class Stakeholder Desirability <<Relationship>></u>	274
<u>9.16</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Observations</u>	275
<u>9.16.1</u>	<u>Diagram: Measurement</u>	275
<u>9.16.2</u>	<u>Diagram: Observability</u>	275
<u>9.16.3</u>	<u>Diagram: Observations</u>	276

9.16.4	Association Context of Observation	276
9.16.5	Association Class Measurement <<Relationship>>	276
9.16.6	Association Class Observability <<Relationship>>	277
9.16.7	Association Class Observation <<Relationship>>	277
9.16.8	Class Observation Tool <<Role>>	278
9.16.9	Class Observer <<Role>>	278
9.17	Threat-risk-conceptual-model::Generic Concept Library::Organizations	280
9.17.1	Diagram: Organization	280
9.17.2	Association Class Membership <<Relationship>>	280
9.17.3	Class Mission Objective	281
9.17.4	Class Organization	282
9.17.5	Class Organizational Unit <<Role>>	282
9.17.6	Class Parent Organization <<Role>>	282
9.17.7	Association Class Part of Organization <<Relationship>>	283
9.17.8	Class Program	284
9.18	Threat-risk-conceptual-model::Generic Concept Library::Organizations::Corporations	285
9.18.1	Diagram: Corporations	285
9.18.2	Class Incorporated Organization	285
9.18.3	Association Class Incorporation <<Relationship>>	286
9.19	Threat-risk-conceptual-model::Generic Concept Library::Organizations::Geopolitical Organizations	287
9.19.1	Diagram: Geopolitical Entities	287
9.19.2	Class Country	287
9.19.3	Class Country ID <<Value>>	288
9.19.4	Class Geopolitical Entity	288
9.19.5	Class Geopolitical ID <<Value>>	288
9.19.6	Class Geopolitical Region <<Role>>	289
9.19.7	Association Class Governing Authority <<Relationship>>	289
9.20	Threat-risk-conceptual-model::Generic Concept Library::Permissions	290
9.20.1	Diagram: Permission	290
9.20.2	Association Class Permission	291
9.21	Threat-risk-conceptual-model::Generic Concept Library::Persons	292
9.21.1	Diagram: Person	292
9.21.2	Diagram: Person Identifiers	293
9.21.3	Diagram: Person Name Representations	294
9.21.4	Class Access Identifier <<Value>>	294
9.21.5	Class Financial Identifier <<Value>>	294
9.21.6	Class Managed Person Identifier <<Value>>	295

<u>9.21.7</u>	<u>Class Passport Identifier <<Value>></u>	295
<u>9.21.8</u>	<u>Class Person</u> 295	
<u>9.21.9</u>	<u>Association Class Person at location <<Relationship>></u>	296
<u>9.21.10</u>	<u>Class Person Name <<Value>></u>	296
<u>9.21.11</u>	<u>Class Person Structured Name <<Value>></u>	297
<u>9.21.12</u>	<u>Association Class Residency <<Relationship>></u>	298
<u>9.21.13</u>	<u>Class Social Security Number <<Value>></u>	298
<u>9.22</u>	<u>Threat-risk-conceptual-model::Generic Concept Library:Physical Entities</u>	299
<u>9.22.1</u>	<u>Diagram: Physical Entities</u>	300
<u>9.22.2</u>	<u>Class Animal</u> 300	
<u>9.22.3</u>	<u>Class Conveyance</u>	301
<u>9.22.4</u>	<u>Class Device</u> 302	
<u>9.22.5</u>	<u>Class Item</u> 302	
<u>9.22.6</u>	<u>Class Managed Item Identifier <<Value>></u>	302
<u>9.22.7</u>	<u>Class Physical Entity</u>	303
<u>9.22.8</u>	<u>Class Physical Feature</u>	303
<u>9.22.9</u>	<u>Class Physical Tool <<Role>></u>	303
<u>9.22.10</u>	<u>Class Spacial Entity</u>	303
<u>9.22.11</u>	<u>Class Telecommunication Device</u>	304
<u>9.23</u>	<u>Threat-risk-conceptual-model::Generic Concept Library:Places</u>	307
<u>9.23.1</u>	<u>Diagram: Place</u>	307
<u>9.23.2</u>	<u>Class Facility <<Role>></u>	307
<u>9.23.3</u>	<u>Association Class Operating Location <<Relationship>></u>	307
<u>9.23.4</u>	<u>Class Place <<Role>></u>	308
<u>9.23.5</u>	<u>Association Class Place of Occurrence <<Relationship>></u>	309
<u>9.23.6</u>	<u>Class Residence <<Role>></u>	309
<u>9.24</u>	<u>Threat-risk-conceptual-model::Generic Concept Library:Policies</u>	311
<u>9.24.1</u>	<u>Diagram: Policy</u>	311
<u>9.24.2</u>	<u>Association Class Assertion of Policy <<Relationship>></u>	311
<u>9.24.3</u>	<u>Class Policy</u> 312	
<u>9.25</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Predictions</u>	314
<u>9.25.1</u>	<u>Diagram: Prediction</u>	314
<u>9.25.2</u>	<u>Association Class Prediction <<Relationship>></u>	314
<u>9.25.3</u>	<u>Class Predictor <<Role>></u>	315
<u>9.26</u>	<u>Threat-risk-conceptual-model::Generic Concept Library:Processes</u>	317
<u>9.26.1</u>	<u>Diagram: Process</u>	318
<u>9.26.2</u>	<u>Association Class Invoke Process <<Relationship>></u>	319

<u>9.26.3</u>	<u>Class Modus Operandi</u>	319
<u>9.26.4</u>	<u>Class Plan</u>	320
<u>9.26.5</u>	<u>Class Process Action</u>	320
<u>9.26.6</u>	<u>Association Class Process Decomposition <<Relationship>></u>	320
<u>9.26.7</u>	<u>Class Process Pattern</u>	321
<u>9.26.8</u>	<u>Class Scenario</u>	322
<u>9.26.9</u>	<u>Association Class When <<Relationship>></u>	323
<u>9.27</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Processes::Composite Conditions</u>	325
<u>9.27.1</u>	<u>Diagram: Composite Condition</u>	325
<u>9.27.2</u>	<u>Class AND Condition</u>	325
<u>9.27.3</u>	<u>Class Composite Condition</u>	325
<u>9.27.4</u>	<u>Class OR Condition</u>	326
<u>9.27.5</u>	<u>Class XOR Condition</u>	326
<u>9.28</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Processes::Process Effects</u>	327
<u>9.28.1</u>	<u>Diagram: Process Effects</u>	327
<u>9.28.2</u>	<u>Class Activity Effecting Entity</u>	328
<u>9.28.3</u>	<u>Class Create</u>	328
<u>9.28.4</u>	<u>Class Damage</u>	328
<u>9.28.5</u>	<u>Class Destroy</u>	329
<u>9.28.6</u>	<u>Class Disrupt Process</u>	329
<u>9.28.7</u>	<u>Class Entry Action</u>	329
<u>9.28.8</u>	<u>Class Exit Action</u>	329
<u>9.28.9</u>	<u>Class Pause Process</u>	329
<u>9.28.10</u>	<u>Class Possible Actions</u>	330
<u>9.28.11</u>	<u>Class Stop Process</u>	330
<u>9.29</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Quantities and Units</u>	331
<u>9.29.1</u>	<u>Diagram: Quantities and units</u>	332
<u>9.29.2</u>	<u>Class Confidence Metric <<Quantity Kind>></u>	333
<u>9.29.3</u>	<u>Class Count <<Quantity Kind>></u>	333
<u>9.29.4</u>	<u>Class Currency Benefit Metric <<Quantity Kind>></u>	333
<u>9.29.5</u>	<u>Class Harm-Benefit Metric <<Quantity Kind>></u>	333
<u>9.29.6</u>	<u>Class Metric <<Quantity Kind>></u>	333
<u>9.29.7</u>	<u>Class Probability Metric <<Quantity Kind>></u>	334
<u>9.29.8</u>	<u>Class Time Coordinate <<Quantity Kind>></u>	334
<u>9.30</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Quantities and Units::Quantity Kinds</u>	339
<u>9.30.1</u>	<u>Diagram: Quantity Kinds</u>	339
<u>9.30.2</u>	<u>Class Absorbed Dose (Radiation) <<Quantity Kind>></u>	339

9.30.3	Class Acceleration <<Quantity Kind>>.....	340
9.30.4	Class Amount of Substance <<Quantity Kind>>.....	340
9.30.5	Class Angle <<Quantity Kind>>	340
9.30.6	Class Area <<Quantity Kind>>	340
9.30.7	Class Color <<Quantity Kind>>	340
9.30.8	Class Concentration <<Quantity Kind>>	341
9.30.9	Class Concentration (amount of substance) <<Quantity Kind>>	341
9.30.10	Class Concentration (Mass) <<Quantity Kind>>	341
9.30.11	Class Concentration (Volume) <<Quantity Kind>>	341
9.30.12	Class Currency <<Quantity Kind>>	341
9.30.13	Class Dose Equivalent (Radiation) <<Quantity Kind>>.....	342
9.30.14	Class Duration <<Quantity Kind>>.....	342
9.30.15	Class Electric Current <<Quantity Kind>>	342
9.30.16	Class Electric Potential <<Quantity Kind>>	343
9.30.17	Class Energy <<Quantity Kind>>.....	343
9.30.18	Class Force <<Quantity Kind>>.....	343
9.30.19	Class Frequency <<Quantity Kind>>	343
9.30.20	Class Length <<Quantity Kind>>	344
9.30.21	Class Luminosity <<Quantity Kind>>	344
9.30.22	Class Mass <<Quantity Kind>>.....	344
9.30.23	Class Mass Density <<Quantity Kind>>	344
9.30.24	Class Physical Quantity <<Quantity Kind>>.....	344
9.30.25	Class Power <<Quantity Kind>>	345
9.30.26	Class Pressure <<Quantity Kind>>	345
9.30.27	Class Radiation Exposure <<Quantity Kind>>.....	345
9.30.28	Class Radioactivity <<Quantity Kind>>.....	345
9.30.29	Class Speed <<Quantity Kind>>	345
9.30.30	Class Temperature <<Quantity Kind>>	346
9.30.31	Class Volume <<Quantity Kind>>	346
9.31	Threat-risk-conceptual-model::Generic Concept Library::Resources	347
9.31.1	Diagram: Resource	347
9.31.2	Diagram: Resource Actions	348
9.31.3	Class Abuse Resource.....	348
9.31.4	Class Capture Resource	348
9.31.5	Class Damage Resource.....	348
9.31.6	Class Exceed Resource Capacity	349
9.31.7	Class Modify Resource	349

<u>9.31.8</u>	<u>Class Performer <<Role>></u>	349
<u>9.31.9</u>	<u>Class Resource <<Role>></u>	349
<u>9.31.10</u>	<u>Class Resource Actions</u>	350
<u>9.31.11</u>	<u>Association Class Resource Dependency <<Relationship>></u>	351
<u>9.31.12</u>	<u>Class Tool <<Role>></u>	351
<u>9.32</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Situations</u>	353
<u>9.32.1</u>	<u>Diagram: Situation</u>	354
<u>9.32.2</u>	<u>Diagram: Situation Timeframes</u>	355
<u>9.32.3</u>	<u>Class Actual State <<Intersection>></u>	355
<u>9.32.4</u>	<u>Association Class Cause and Effect <<Relationship>></u>	355
<u>9.32.5</u>	<u>Class Current Situation</u>	356
<u>9.32.6</u>	<u>Association Class Effect <<Relationship>></u>	357
<u>9.32.7</u>	<u>Association Class Involvement <<Relationship>></u>	357
<u>9.32.8</u>	<u>Association Class Negation Effect <<Relationship>></u>	358
<u>9.32.9</u>	<u>Class Past Situation</u>	359
<u>9.32.10</u>	<u>Class Potential Situation</u>	360
<u>9.32.11</u>	<u>Association Class Scope of Indicator <<Relationship>></u>	360
<u>9.32.12</u>	<u>Class State</u>	361
<u>9.32.13</u>	<u>Association State of Entity</u>	361
<u>9.33</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Social Agents</u>	362
<u>9.33.1</u>	<u>Diagram: Social Agent</u>	362
<u>9.33.2</u>	<u>Diagram: Social Agent Identifiers</u>	363
<u>9.33.3</u>	<u>Association Class Associated Actor <<Relationship>></u>	363
<u>9.33.4</u>	<u>Class License Identifier <<Value>></u>	364
<u>9.33.5</u>	<u>Class Local Identifier <<Value>></u>	364
<u>9.33.6</u>	<u>Class Managed Social Agent Identifier <<Value>></u>	364
<u>9.33.7</u>	<u>Class Regional Identifier <<Value>></u>	364
<u>9.33.8</u>	<u>Class Social Agent</u>	365
<u>9.33.9</u>	<u>Class Tax Authority Identifier <<Value>></u>	365
<u>9.34</u>	<u>Threat-risk-conceptual-model::Generic Concept Library::Systems</u>	366
<u>9.34.1</u>	<u>Diagram: System</u>	366
<u>9.34.2</u>	<u>Class Access Point</u>	367
<u>9.34.3</u>	<u>Class Boundary</u>	367
<u>9.34.4</u>	<u>Association Class Boundary of System <<Relationship>></u>	367
<u>9.34.5</u>	<u>Association Class Opening in a Boundary <<Relationship>></u>	368
<u>9.34.6</u>	<u>Association Class Point Of Entry <<Relationship>></u>	369
<u>9.34.7</u>	<u>Class Subsystem <<Role>></u>	370

9.34.8	Class System	370
9.35	Threat-risk-conceptual-model::Generic Concept Library::Time & Temporal Entities.....	372
9.35.1	Diagram: Time.....	373
9.35.2	Class Date and Time <<Quantity Kind>>	374
9.35.3	Class Date Coordinate <<Quantity Kind>>.....	374
9.35.4	Association Duration of Entity	374
9.35.5	Association Entity Exists for Interval	375
9.35.6	Association Finish Time	375
9.35.7	Association Overlaps in Time.....	376
9.35.8	Association Start Time.....	377
9.35.9	Association Temporal Order.....	378
9.35.10	Association Class Temporal Part <<Relationship>>.....	379
9.35.11	Class Time Coordinate <<Quantity Kind>>.....	380
9.35.12	Class Time Interval.....	380
9.35.13	Class Time Point.....	380
9.35.14	Class Time Scale.....	381
9.35.15	Association Time Scale Granularity	381
9.35.16	Association Time Scale of Time Point	382
9.36	Threat-risk-conceptual-model::Generic Concept Library::Time & Temporal Entities::ISO Time Scale	383
9.36.1	Diagram: ISO Time	383
9.36.2	Class Date Time Coordinate (ISO 8601) <<Unit Value>>.....	384
9.37	Threat-risk-conceptual-model::Generic Concept Library::Time & Temporal Entities::XSD Time Scale	385
9.37.1	Diagram: XSD Time Scale	385
9.37.2	Class XSD Date <<Unit Value>>.....	385
9.37.3	Class XSD Date Time <<Unit Value>>	386
9.37.4	Class XSD Time <<Unit Value>>	386
9.38	Threat-risk-conceptual-model::Generic Concept Library::Vendors and Producers	387
9.38.1	Diagram: Vendors and Producers	387
9.38.2	Class Client <<Role>>	387
9.38.3	Class Individual Product <<Role>>	388
9.38.4	Class Manufactured Thing <<Role>>	388
9.38.5	Class Producer <<Role>>	388
9.38.6	Class Product Kind	389
9.38.7	Association Class Product Line of Supplier <<Relationship>>.....	389
9.38.8	Association Class Production <<Relationship>>	390
9.38.9	Association Class Providing <<Relationship>>	390
9.38.10	Class Serial Number <<Value>>	391

<u>9.38.11 Class Supplier <<Role>>.....</u>	392
<u>10 STIX Mapping Specification (Normative)</u>	393
<u>10.1 How STIX is represented.....</u>	393
<u>10.2 Generic STIX Mapping Rules and Conventions</u>	393
<u>10.3 STIX Mapping to the threat/risk conceptual reference model.....</u>	395
<u>10.3.1 Diagram: High Level STIX Mapping</u>	395
<u>10.4 STIX Mapping to the threat/risk conceptual reference model::Facades.....</u>	396
<u>10.4.1 Diagram: Facade Summary.....</u>	396
<u>10.4.2 Class ActualObservableFacade.....</u>	397
<u>10.4.3 Class AffectedAssetFacade.....</u>	397
<u>10.4.4 Class ExploitTargetFacade</u>	397
<u>10.4.5 Class ObservablePatternFacade</u>	397
<u>10.4.6 Class Threat Report</u>	398
<u>10.5 STIX Mapping to the threat/risk conceptual reference model::STIX Mapping Rules</u>	399
<u>10.6 Class STIX Campaign Rule.....</u>	399
<u>10.7 Class STIX Categories Rule</u>	400
<u>10.8 Class STIX Course Of Action Rule.....</u>	401
<u>10.9 Class STIX Incident Rule.....</u>	402
<u>10.10 Class STIX Indicator Rule</u>	403
<u>10.11 Class STIX Objective Rule</u>	404
<u>10.12 Class STIX Observable Rule.....</u>	405
<u>10.13 Class STIX Sighting Rule</u>	406
<u>10.14 Class STIX Statement Rule</u>	407
<u>10.15 Class STIX Threat Actor Rule</u>	408
<u>10.16 Class STIX TTP Rule.....</u>	409
<u>10.17 Class STIX Vocabulary Rule</u>	410
<u>10.18 Class STIX Vulnerability Rule.....</u>	411
<u>11 NIEM Mapping Specification (Normative)</u>	412
<u>11.1 How NIEM is represented.....</u>	412
<u>11.2 Generic NIEM mapping rules and conventions.....</u>	412
<u>11.3 NIEM Mapping to the threat / risk model::Facades::Contact Information</u>	415
<u>11.3.1 Diagram: Contact Information Facades</u>	415
<u>11.3.2 Class Postal Address Facade.....</u>	415
<u>11.3.3 Class Telephone Number Facade.....</u>	416
<u>11.4 NIEM Mapping to the threat / risk model::Facades::Injury.....</u>	417
<u>11.4.1 Diagram: Person Injury Facade</u>	417
<u>11.4.2 Class PersonInjuryFacade.....</u>	417

<u>11.5</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships.....</u>	418
<u>11.5.1</u>	<u>Diagram: NIEM Mapping Rules.....</u>	418
<u>11.5.2</u>	<u>Diagram: NIEM Mapping Summary 1.....</u>	419
<u>11.5.3</u>	<u>Diagram: NIEM Mapping Summary 2.....</u>	420
<u>11.6</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Activity</u>	421
<u>11.6.1</u>	<u>Diagram: Activity Mapping Summary.....</u>	421
<u>11.6.2</u>	<u>Class Activity Map Rule.....</u>	421
<u>11.7</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Assessment</u>	423
<u>11.7.1</u>	<u>Diagram: Assessment Mapping Summary</u>	423
<u>11.7.2</u>	<u>Class Assessment Map Rule</u>	424
<u>11.8</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation.....</u>	425
<u>11.8.1</u>	<u>Diagram: Contact Information Mapping Summary.....</u>	425
<u>11.8.2</u>	<u>Class Address Map Rule.....</u>	426
<u>11.8.3</u>	<u>Class Contact Information Mapping Rule.....</u>	427
<u>11.8.4</u>	<u>Class Internet Contact Map Rule</u>	428
<u>11.8.5</u>	<u>Class Radio Map Rule</u>	429
<u>11.8.6</u>	<u>Class Telephone Map Rule</u>	430
<u>11.9</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Entity</u>	431
<u>11.9.1</u>	<u>Diagram: Entity Mapping Summary</u>	431
<u>11.9.2</u>	<u>Class Entiy Map Rule</u>	431
<u>11.10</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Identification</u>	433
<u>11.10.1</u>	<u>Diagram: Identification Mapping Summary</u>	433
<u>11.10.2</u>	<u>Class Identification Map Rule</u>	434
<u>11.11</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Incident</u>	435
<u>11.11.1</u>	<u>Diagram: Incident mapping summary</u>	435
<u>11.11.2</u>	<u>Class Incident Map Rule</u>	435
<u>11.12</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Injury</u>	437
<u>11.12.1</u>	<u>Diagram: Injury Mapping Summary</u>	437
<u>11.12.2</u>	<u>Class Injury Map Rule</u>	438
<u>11.13</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Item</u>	439
<u>11.13.1</u>	<u>Diagram: Item Mapping Summary</u>	439
<u>11.13.2</u>	<u>Class Item Map Rule</u>	440
<u>11.14</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location</u>	441
<u>11.14.1</u>	<u>Diagram: Location mapping summary</u>	442
<u>11.14.2</u>	<u>Class Area Map Rule</u>	443

<u>11.14.3</u>	<u>Class Coordinate Map Rule</u>	443
<u>11.14.4</u>	<u>Class Facility Map Rule.....</u>	444
<u>11.14.5</u>	<u>Class Location Map Rule.....</u>	445
<u>11.15</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Organization</u>	446
<u>11.15.1</u>	<u>Diagram: NIEM Organization Mapping Summary.....</u>	446
<u>11.15.2</u>	<u>Class Organization Map Rule.....</u>	447
<u>11.16</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Person</u>	448
<u>11.16.1</u>	<u>Diagram: Person Mapping Summary.....</u>	448
<u>11.16.2</u>	<u>Class Person Map Rule.....</u>	449
<u>11.16.3</u>	<u>Class Person Name Map Rule.....</u>	450
<u>11.17</u>	<u>NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM PrimitiveTypes</u>	451
<u>11.17.1</u>	<u>Diagram: Primitive Type Mapping</u>	451
<u>12</u>	<u>Threat and Risk Alignment to NIST 800-53.....</u>	452
<u>13</u>	<u>Concept Index.....</u>	485
<u>0</u>	<u>Submission related material.....</u>	23
<u>0.1</u>	<u>Submission Introduction.....</u>	23
<u>0.2</u>	<u>Submission Team</u>	23
<u>0.2.1</u>	<u>Submitters</u>	23
<u>0.2.2</u>	<u>Contributors & Supporters.....</u>	23
<u>0.3</u>	<u>Proof of concept</u>	24
<u>0.4</u>	<u>Resolution of Requirements</u>	25
<u>0.4.1</u>	<u>Mandatory requirements</u>	25
<u>0.4.2</u>	<u>Non-mandatory features.....</u>	28
<u>0.5</u>	<u>Resolution of Discussion Issues</u>	28
<u>1.1</u>	<u>Scope</u>	30
<u>2</u>	<u>Conformance.....</u>	30
<u>2.1</u>	<u>Canonical model conformance</u>	31
<u>2.2</u>	<u>Informatin model mapping conformance.....</u>	31
<u>2.3</u>	<u>STIX mapping conformance</u>	31
<u>2.4</u>	<u>NIEM mapping conformance</u>	31
<u>2.5</u>	<u>OWL mapping conformance</u>	32
<u>2.6</u>	<u>Conceptual reference modeling profile conformance</u>	32
<u>3</u>	<u>References</u>	33
<u>4</u>	<u>Terms and Definitions</u>	34
<u>5</u>	<u>Symbols and Notation.....</u>	35

<u>6</u>	<u>Additional Information</u>	35
<u>6.1</u>	<u>Acknowledgments</u>	35
<u>7</u>	<u>Operational Threat and Risk Guide (Non Normative).....</u>	37
<u>7.1</u>	<u>Mission and purpose.....</u>	37
<u>7.2</u>	<u>Technology capabilities.....</u>	38
<u>7.2.1</u>	<u>Federated analytics and simulation capabilities</u>	38
<u>7.2.2</u>	<u>Information Translating, Analytics, and Sharing capabilities</u>	39
<u>7.2.3</u>	<u>Risk Analytics Capabilities.....</u>	40
<u>7.2.4</u>	<u>Semantic federation and translation.....</u>	41
<u>7.3</u>	<u>Defining and Leveraging Conceptual reference models.....</u>	44
<u>7.3.1</u>	<u>Expressing conceptual reference models</u>	44
<u>7.3.2</u>	<u>Mapping to information and data models</u>	45
<u>7.3.3</u>	<u>Layering</u>	45
<u>7.3.4</u>	<u>Source of concepts.....</u>	46
<u>7.4</u>	<u>Top Level Concepts</u>	48
<u>7.5</u>	<u>Modeling Style</u>	50
<u>7.5.1</u>	<u>Mixing Concepts with “multiple classification”</u>	53
<u>8</u>	<u>Operational Threat and Risk Model Reference.....</u>	54
<u>8.1</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts</u>	54
<u>8.1.1</u>	<u>Diagram: Threat and Risk Specific Concepts</u>	55
<u>8.2</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts:: Summary Diagrams</u>	56
<u>8.2.1</u>	<u>Diagram: Entity Kinds</u>	56
<u>8.3</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts::Campaigns</u>	57
<u>8.3.1</u>	<u>Diagram: Campaign</u>	57
<u>8.3.2</u>	<u>Class Campaign</u>	57
<u>8.4</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts::Danger</u>	58
<u>8.4.1</u>	<u>Diagram: Danger</u>	59
<u>8.4.2</u>	<u>Class Attack <<Role>>.....</u>	60
<u>8.4.3</u>	<u>Class Indirect Threat <<Role>>.....</u>	60
<u>8.4.4</u>	<u>Class Natural Threat <<Role>>.....</u>	60
<u>8.4.5</u>	<u>Association Class Target of Attack <<Relationship>>.....</u>	60
<u>8.4.6</u>	<u>Class Threat <<Role>>.....</u>	61
<u>8.4.7</u>	<u>Class Unintentional Threat <<Role>>.....</u>	62
<u>8.5</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts::Danger Categories.....</u>	63
<u>8.5.1</u>	<u>Diagram: Danger Categories</u>	63
<u>8.5.2</u>	<u>Diagram: Danger Source Categories</u>	64
<u>8.5.3</u>	<u>Diagram: Failure Categories</u>	65

<u>8.5.4</u>	<u>Diagram: Impact Categories</u>	66
<u>8.5.5</u>	<u>Class Access Control Failure <<Category>></u>	66
<u>8.5.6</u>	<u>Class Biological Danger <<Category>></u>	67
<u>8.5.7</u>	<u>Class CBRN Danger <<Category>></u>	67
<u>8.5.8</u>	<u>Class Chemical Danger <<Category>></u>	67
<u>8.5.9</u>	<u>Class Civil Unrest Danger <<Category>></u>	67
<u>8.5.10</u>	<u>Class Compliance Impact <<Category>></u>	67
<u>8.5.11</u>	<u>Class Control Failure <<Category>></u>	67
<u>8.5.12</u>	<u>Class Criminal Danger <<Category>></u>	68
<u>8.5.13</u>	<u>Class Cyber Danger <<Category>></u>	68
<u>8.5.14</u>	<u>Class Cyber System Failure <<Category>></u>	68
<u>8.5.15</u>	<u>Class Danger Category <<Category>></u>	68
<u>8.5.16</u>	<u>Class Decision-making Impact <<Category>></u>	68
<u>8.5.17</u>	<u>Class Disinformation Impact <<Category>></u>	68
<u>8.5.18</u>	<u>Class Electromagnetic Spectrum Impact <<Category>></u>	68
<u>8.5.19</u>	<u>Class Environmental Impact <<Category>></u>	69
<u>8.5.20</u>	<u>Class Failure Category <<Category>></u>	69
<u>8.5.21</u>	<u>Class Financial Impact <<Category>></u>	69
<u>8.5.22</u>	<u>Class Fire Danger <<Category>></u>	69
<u>8.5.23</u>	<u>Class Geophysical Danger <<Category>></u>	69
<u>8.5.24</u>	<u>Class Health Impact <<Category>></u>	69
<u>8.5.25</u>	<u>Class Identity Theft <<Category>></u>	70
<u>8.5.26</u>	<u>Class Image Impact <<Category>></u>	70
<u>8.5.27</u>	<u>Class Impact Category <<Category>></u>	70
<u>8.5.28</u>	<u>Class Inability to Communicate Impact <<Category>></u>	70
<u>8.5.29</u>	<u>Class Industrial Control Failure <<Category>></u>	70
<u>8.5.30</u>	<u>Class Information Impact <<Category>></u>	70
<u>8.5.31</u>	<u>Class Information Loss Impact <<Category>></u>	71
<u>8.5.32</u>	<u>Class Infrastructure Impact <<Category>></u>	71
<u>8.5.33</u>	<u>Class Intellectual Property Impact <<Category>></u>	71
<u>8.5.34</u>	<u>Class Legal Impact <<Category>></u>	71
<u>8.5.35</u>	<u>Class Loss of Control Danger <<Category>></u>	71
<u>8.5.36</u>	<u>Class Meteorological Danger <<Category>></u>	71
<u>8.5.37</u>	<u>Class Mission Impact <<Category>></u>	72
<u>8.5.38</u>	<u>Class Non-Technical Impact <<Category>></u>	72
<u>8.5.39</u>	<u>Class Nuclear Danger <<Category>></u>	72
<u>8.5.40</u>	<u>Class Physical System Failure <<Category>></u>	72

<u>8.5.41</u>	<u>Class Process Failure <<Category>></u>	72
<u>8.5.42</u>	<u>Class Radiological Danger <<Category>></u>	72
<u>8.5.43</u>	<u>Class Safety Danger <<Category>></u>	73
<u>8.5.44</u>	<u>Class Safety Impact <<Category>></u>	73
<u>8.5.45</u>	<u>Class Security Danger <<Category>></u>	73
<u>8.5.46</u>	<u>Class Source of Danger Category <<Category>></u>	73
<u>8.5.47</u>	<u>Class System Failure <<Category>></u>	73
<u>8.5.48</u>	<u>Class Terrorism Danger <<Category>></u>	73
<u>8.5.49</u>	<u>Class Transport Impact <<Category>></u>	74
<u>8.5.50</u>	<u>Class War Danger <<Category>></u>	74
<u>8.6</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts::Danger Sources</u>	75
<u>8.6.1</u>	<u>Diagram: Danger Sources</u>	75
<u>8.6.2</u>	<u>Class Accident <<Role>></u>	75
<u>8.6.3</u>	<u>Association Class Contribution to Danger <<Relationship>></u>	76
<u>8.6.4</u>	<u>Class Danger Source <<Role>></u>	76
<u>8.6.5</u>	<u>Class Dangerous Condition <<Role>></u>	76
<u>8.6.6</u>	<u>Class Dangerous Event <<Role>></u>	77
<u>8.6.7</u>	<u>Class Disrupt Stakeholder's Objective</u>	77
<u>8.6.8</u>	<u>Association Class Exploit of Vulnerability <<Relationship>></u>	77
<u>8.6.9</u>	<u>Class Objective to Disrupt</u>	78
<u>8.6.10</u>	<u>Class Unwitting Participant <<Role>></u>	79
<u>8.7</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts::Incidents and failures</u>	80
<u>8.7.1</u>	<u>Diagram: Incident</u>	80
<u>8.7.2</u>	<u>Association Class Danger Leads to Incident <<Relationship>></u>	80
<u>8.7.3</u>	<u>Class Failure</u>	81
<u>8.7.4</u>	<u>Association Class Failure of Resource <<Relationship>></u>	82
<u>8.7.5</u>	<u>Class Incident <<Role>></u>	82
<u>8.7.6</u>	<u>Class Witness <<Role>></u>	83
<u>8.7.7</u>	<u>Association Class Witnessing <<Relationship>></u>	83
<u>8.8</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts::Indicators</u>	85
<u>8.8.1</u>	<u>Diagram: Indicator</u>	85
<u>8.8.2</u>	<u>Diagram: Sighting</u>	86
<u>8.8.3</u>	<u>Class Blacklist Indicator</u>	86
<u>8.8.4</u>	<u>Class Indicator</u>	86
<u>8.8.5</u>	<u>Association Class Indicator Indicates Situation <<Relationship>></u>	87
<u>8.8.6</u>	<u>Class Indicator Pattern</u>	88
<u>8.8.7</u>	<u>Class Indicator Watchlist</u>	88

<u>8.8.8</u>	<u>Association Class Sighting <<Relationship>></u>	88
<u>8.8.9</u>	<u>Association Class Sighting Indicates Situation <<Relationship>></u>	89
<u>8.8.10</u>	<u>Association Class Sighting Matches Indicator <<Relationship>></u>	90
<u>8.8.11</u>	<u>Association Class Watch <<Relationship>></u>	91
<u>8.8.12</u>	<u>Class Whitelist Indicator</u>	92
<u>8.9</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts::Risk</u>	93
<u>8.9.1</u>	<u>Diagram: Risk</u>	93
<u>8.9.2</u>	<u>Diagram: Risk Metrics</u>	94
<u>8.9.3</u>	<u>Class Accept Risk</u>	94
<u>8.9.4</u>	<u>Association Class Impose Strategy <<Relationship>></u>	94
<u>8.9.5</u>	<u>Class Objective for Safety and Security</u>	95
<u>8.9.6</u>	<u>Class Objective to Protect Assets</u>	95
<u>8.9.7</u>	<u>Class Risk</u>95	
<u>8.9.8</u>	<u>Class Risk Mitigation Strategy</u>	96
<u>8.9.9</u>	<u>Class Risk Owner <<Role>></u>	96
<u>8.9.10</u>	<u>Class Risk Reduction Objective</u>	97
<u>8.9.11</u>	<u>Association Class Risk To Resource <<Relationship>></u>	98
<u>8.9.12</u>	<u>Association Class Risk Topic <<Relationship>></u>	98
<u>8.9.13</u>	<u>Association Class Stakeholder Risk <<Relationship>></u>	99
<u>8.9.14</u>	<u>Class Threat Likelihood <<Quantity Kind>></u>	100
<u>8.9.15</u>	<u>Association Class Valuation of Asset <<Relationship>></u>	101
<u>8.9.16</u>	<u>Class Valued Asset <<Role>></u>	101
<u>8.10</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts::Risk Treatments</u>	104
<u>8.10.1</u>	<u>Diagram: Risk Treatment</u>	104
<u>8.10.2</u>	<u>Diagram: Safeguard Monitoring</u>	105
<u>8.10.3</u>	<u>Association Class Assume Risk <<Relationship>></u>	105
<u>8.10.4</u>	<u>Class Avoid Danger</u>	106
<u>8.10.5</u>	<u>Class Countermeasure <<Role>></u>	106
<u>8.10.6</u>	<u>Association Class Countermeasure for Strategy <<Relationship>></u>	106
<u>8.10.7</u>	<u>Association Class Countermeasure Mitigates <<Relationship>></u>	107
<u>8.10.8</u>	<u>Class Mitigation Actor <<Role>></u>	108
<u>8.10.9</u>	<u>Association Class Monitor <<Relationship>></u>	108
<u>8.10.10</u>	<u>Class Monitoring Safeguard</u>	109
<u>8.10.11</u>	<u>Association Class Protection <<Relationship>></u>	109
<u>8.10.12</u>	<u>Class Risk Agent <<Role>></u>	110
<u>8.10.13</u>	<u>Association Class Risk Treatment <<Relationship>></u>	110
<u>8.10.14</u>	<u>Class Risk Treatment Strategy</u>	111

<u>8.10.15</u> — <u>Class Safeguard Activity</u>	111
<u>8.10.16</u> — <u>Association Class Safeguarding <<Relationship>></u>	112
<u>8.10.17</u> — <u>Class Transfer Risk</u>	112
<u>8.11</u> — <u>Threat risk conceptual model::Threat and Risk Specific Concepts::Threat Actors</u>	113
<u>8.11.1</u> — <u>Diagram: Threat Actors</u>	113
<u>8.11.2</u> — <u>Class Disruptive Action <<Role>></u>	114
<u>8.11.3</u> — <u>Association Class Perpetrate <<Relationship>></u>	114
<u>8.11.4</u> — <u>Class Threat Actor <<Role>></u>	115
<u>8.12</u> — <u>Threat risk conceptual model::Threat and Risk Specific Concepts::Undesirable Situations</u>	117
<u>8.12.1</u> — <u>Diagram: Undesirable Situations</u>	118
<u>8.12.2</u> — <u>Class Harm</u>	118
<u>8.12.3</u> — <u>Association Class Harms Resource <<Relationship>></u>	119
<u>8.12.4</u> — <u>Association Class Harms Victim <<Relationship>></u>	120
<u>8.12.5</u> — <u>Association Class Source of Harm <<Relationship>></u>	121
<u>8.12.6</u> — <u>Class Undesirable Condition <<Role>></u>	121
<u>8.12.7</u> — <u>Class Undesirable Event <<Role>></u>	122
<u>8.12.8</u> — <u>Class Undesirable Situation <<Role>></u>	122
<u>8.12.9</u> — <u>Class Victim <<Role>></u>	123
<u>8.13</u> — <u>Threat risk conceptual model::Threat and Risk Specific Concepts::Vulnerabilities</u>	124
<u>8.13.1</u> — <u>Diagram: Vulnerability</u>	124
<u>8.13.2</u> — <u>Diagram: Vulnerability Identifiers</u>	125
<u>8.13.3</u> — <u>Class Physical Vulnerability</u>	125
<u>8.13.4</u> — <u>Association Class Supporting Condition <<Relationship>></u>	125
<u>8.13.5</u> — <u>Class Vulnerability</u>	126
<u>8.13.6</u> — <u>Class Vulnerability Identifier <<Value>></u>	127
<u>8.13.7</u> — <u>Class Vulnerability Metric <<Quantity Kind>></u>	128
<u>8.13.8</u> — <u>Association Class Vulnerability of Resource <<Relationship>></u>	128
<u>8.14</u> — <u>Threat risk conceptual model::Threat and Risk Specific Concepts::Vulnerabilities::Cyber Vulnerabilities</u>	129
<u>8.14.1</u> — <u>Diagram: Cyber Vulnerability</u>	129
<u>8.14.2</u> — <u>Class Communications Vulnerability</u>	129
<u>8.14.3</u> — <u>Class CVE Identifier <<Value>></u>	130
<u>8.14.4</u> — <u>Class Cyber Vulnerability</u>	130
<u>8.14.5</u> — <u>Class Information System Vulnerability</u>	130
<u>8.14.6</u> — <u>Class Information Vulnerability</u>	130
<u>8.14.7</u> — <u>Class OSVDB Identifier <<Value>></u>	134
<u>8.14.8</u> — <u>Class Software Vulnerability</u>	134

<u>8.15</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability Vectors</u>	132
.....
<u>8.15.1</u>	<u>Diagram: Vulnerability Vectors</u>	133
<u>8.15.2</u>	<u>Class CVSS Score <<Quantity Kind>></u>	134
<u>8.16</u>	<u>Threat risk conceptual model::Threat and Risk Specific Concepts::Weapons</u>	144
.....
<u>8.16.1</u>	<u>Diagram: Weapons</u>	144
<u>8.16.2</u>	<u>Class Physical Weapon <<Role>></u>	144
<u>8.16.3</u>	<u>Class Weapon <<Role>></u>	144
<u>8.16.4</u>	<u>Association Class Weapon Leverages Vulnerability <<Relationship>></u>	145
<u>9</u>	<u>Generic Concept Library (Normative)</u>	146
.....
<u> 9.1</u>	<u>Threat risk conceptual model::Generic Concept Library</u>	146
<u>9.1.1</u>	<u>Diagram: Generic Concept Library</u>	146
<u> 9.2</u>	<u>Threat risk conceptual model::Generic Concept Library::Abilities</u>	148
.....
<u>9.2.1</u>	<u>Diagram: Ability</u>	148
<u>9.2.2</u>	<u>Diagram: Alter ability or control</u>	149
<u>9.2.3</u>	<u>Association Class Ability <<Relationship>></u>	149
<u>9.2.4</u>	<u>Association Class Affected Available Resource <<Relationship>></u>	150
<u>9.2.5</u>	<u>Class Alter Ability</u>	151
<u>9.2.6</u>	<u>Association Class Capability <<Relationship>></u>	152
<u>9.2.7</u>	<u>Class Facilitator <<Role>></u>	152
<u>9.2.8</u>	<u>Class Lose Ability</u>	153
<u>9.2.9</u>	<u>Class Obtain Ability</u>	153
<u>9.2.10</u>	<u>Association Class Strengthened Actor <<Relationship>></u>	153
<u>9.2.11</u>	<u>Class Transfer Ability</u>	154
<u>9.2.12</u>	<u>Association Class Weakened Actor <<Relationship>></u>	154
<u> 9.3</u>	<u>Threat risk conceptual model::Generic Concept Library::Assessments</u>	156
.....
<u>9.3.1</u>	<u>Diagram: Assessment</u>	156
<u>9.3.2</u>	<u>Class Assessed Entity <<Role>></u>	156
<u>9.3.3</u>	<u>Class Assessment</u>	157
<u>9.3.4</u>	<u>Class Assessment Activity</u>	157
<u>9.3.5</u>	<u>Association Class Entity Assessment <<Relationship>></u>	157
<u> 9.4</u>	<u>Threat risk conceptual model::Generic Concept Library::Contact Information</u>	159
.....
<u>9.4.1</u>	<u>Diagram: Contact Information</u>	160
<u>9.4.2</u>	<u>Class Communications Security Level <<Value>></u>	161
<u>9.4.3</u>	<u>Class Contact Means <<Value>></u>	161
<u>9.4.4</u>	<u>Association Class Contact Via <<Relationship>></u>	161
<u>9.4.5</u>	<u>Class Contactable</u>	162

<u>9.4.6</u>	<u>Class Electronic Contact <<Value>></u>	163
<u>9.4.7</u>	<u>Class Email Address <<Value>></u>	163
<u>9.4.8</u>	<u>Class Internet Contact <<Value>></u>	164
<u>9.4.9</u>	<u>Class Network Identifier <<Value>></u>	164
<u>9.4.10</u>	<u>Class Postal Address <<Value>></u>	164
<u>9.4.11</u>	<u>Class Postal Address Structured <<Value>></u>	164
<u>9.4.12</u>	<u>Class Postal Address Text <<Value>></u>	165
<u>9.4.13</u>	<u>Class Postal Code <<Value>></u>	166
<u>9.4.14</u>	<u>Class Private Network Contact <<Value>></u>	166
<u>9.4.15</u>	<u>Class Radio Contact <<Value>></u>	166
<u>9.4.16</u>	<u>Class Social Network Contact <<Value>></u>	166
<u>9.4.17</u>	<u>Class Telephone Area Code <<Value>></u>	167
<u>9.4.18</u>	<u>Class Telephone Country Code <<Value>></u>	167
<u>9.4.19</u>	<u>Class Telephone Number <<Value>></u>	167
<u>9.4.20</u>	<u>Class Telephone Number Structured <<Value>></u>	167
<u>9.4.21</u>	<u>Class Telephone Number Text <<Value>></u>	168
<u>9.4.22</u>	<u>Class Website Contact <<Value>></u>	168
<u>9.5</u>	<u>Threat risk conceptual model::Generic Concept Library::Containment</u>	171
<u>9.5.1</u>	<u>Diagram: Containment</u>	171
<u>9.5.2</u>	<u>Diagram: Move Between Containers</u>	172
<u>9.5.3</u>	<u>Diagram: Physical Containment</u>	173
<u>9.5.4</u>	<u>Class Add To Container Event</u>	173
<u>9.5.5</u>	<u>Class Container <<Role>></u>	173
<u>9.5.6</u>	<u>Association Class Containment <<Relationship>></u>	174
<u>9.5.7</u>	<u>Class Containment Event</u>	175
<u>9.5.8</u>	<u>Class Physical Container <<Role>></u>	175
<u>9.5.9</u>	<u>Association Class Physical Containment <<Relationship>></u>	175
<u>9.5.10</u>	<u>Association Class Recieving Container <<Relationship>></u>	176
<u>9.5.11</u>	<u>Class Relocation</u>	176
<u>9.5.12</u>	<u>Class Removal Event</u>	176
<u>9.5.13</u>	<u>Association Class Supplying Container <<Relationship>></u>	177
<u>9.6</u>	<u>Threat risk conceptual model::Generic Concept Library::Control</u>	178
<u>9.6.1</u>	<u>Diagram: Control</u>	178
<u>9.6.2</u>	<u>Diagram: Control Authority</u>	179
<u>9.6.3</u>	<u>Diagram: Custody</u>	179
<u>9.6.4</u>	<u>Class Authority <<Role>></u>	180
<u>9.6.5</u>	<u>Association Class Control <<Relationship>></u>	180

<u>9.6.6</u>	<u>Class Controlled Entity <<Role>></u>	181
<u>9.6.7</u>	<u>Class Controlling Actor <<Role>></u>	182
<u>9.6.8</u>	<u>Class Custodian <<Role>></u>	182
<u>9.6.9</u>	<u>Association Class Custody <<Relationship>></u>	183
<u>9.6.10</u>	<u>Class Leader <<Role>></u>	183
<u>9.6.11</u>	<u>Association Class Leadership <<Relationship>></u>	183
<u>9.6.12</u>	<u>Class Managed Entity <<Role>></u>	184
<u>9.6.13</u>	<u>Class Owner <<Role>></u>	184
<u>9.6.14</u>	<u>Association Class Ownership <<Relationship>></u>	184
<u>9.6.15</u>	<u>Association Class Possession <<Relationship>></u>	185
<u>9.6.16</u>	<u>Class Property <<Role>></u>	185
<u>9.6.17</u>	<u>Association Class Subject to Authority <<Relationship>></u>	185
<u>9.7</u>	<u>Threat risk conceptual model: Generic Concept Library: Credentials</u>	187
<u>9.7.1</u>	<u>Diagram: Credentials and Managed Identifiers</u>	187
<u>9.7.2</u>	<u>Association Actor Identifier of Credential</u>	187
<u>9.7.3</u>	<u>Association Class Attest to Ability <<Relationship>></u>	188
<u>9.7.4</u>	<u>Class Credential</u>	189
<u>9.7.5</u>	<u>Class Identity Provider <<Role>></u>	189
<u>9.7.6</u>	<u>Association Class Issue Credential <<Relationship>></u>	190
<u>9.7.7</u>	<u>Class Managed Actor Identifier <<Value>></u>	190
<u>9.7.8</u>	<u>Association Class Valid for Time Interval <<Relationship>></u>	191
<u>9.8</u>	<u>Threat risk conceptual model: Generic Concept Library: Cyber</u>	192
<u>9.8.1</u>	<u>Diagram: Cyber</u>	193
<u>9.8.2</u>	<u>Diagram: Cyber Platforms</u>	194
<u>9.8.3</u>	<u>Diagram: Cyber Resource</u>	194
<u>9.8.4</u>	<u>Association Class Ability To Execute Software <<Relationship>></u>	195
<u>9.8.5</u>	<u>Association Class Automated Capability <<Relationship>></u>	196
<u>9.8.6</u>	<u>Association Class Automated Control <<Relationship>></u>	196
<u>9.8.7</u>	<u>Class Automated Entity <<Role>></u>	197
<u>9.8.8</u>	<u>Class Automation Type</u>	198
<u>9.8.9</u>	<u>Class Automaton</u>	198
<u>9.8.10</u>	<u>Class Communicating Device</u>	198
<u>9.8.11</u>	<u>Class Communications Link</u>	198
<u>9.8.12</u>	<u>Class Communications Network</u>	199
<u>9.8.13</u>	<u>Class Computer Control System <<Role>></u>	199
<u>9.8.14</u>	<u>Class Computer System</u>	199
<u>9.8.15</u>	<u>Class Cyber Resource <<Union>></u>	200

<u>9.8.16</u>	<u>Class Cyber Weapon <<Role>></u>	200
<u>9.8.17</u>	<u>Class Execution Platform <<Union>></u>	200
<u>9.8.18</u>	<u>Association Class Information In Computer <<Relationship>></u>	201
<u>9.8.19</u>	<u>Association Class Node of a Network <<Relationship>></u>	201
<u>9.8.20</u>	<u>Class Software</u>	202
<u>9.9</u>	<u>Threat risk conceptual model::Generic Concept Library::Enterprises</u>	203
<u>9.9.1</u>	<u>Diagram: Enterprise</u>	203
<u>9.9.2</u>	<u>Class Enterprise</u>	204
<u>9.10</u>	<u>Threat risk conceptual model::Generic Concept Library::Entities</u>	205
<u>9.10.1</u>	<u>Diagram: Identifiable Entity</u>	206
<u>9.10.2</u>	<u>Diagram: Identifiable Entity Relationships</u>	207
<u>9.10.3</u>	<u>Association Class Impact <<Relationship>></u>	207
<u>9.10.4</u>	<u>Association Class Parthood <<Relationship>></u>	208
<u>9.10.5</u>	<u>Association Class Related <<Relationship>></u>	209
<u>9.11</u>	<u>Threat risk conceptual model::Generic Concept Library::Events and Activities</u>	211
<u>9.11.1</u>	<u>Diagram: Events and Activities</u>	211
<u>9.11.2</u>	<u>Class Activity</u>	212
<u>9.11.3</u>	<u>Class Actor</u> ..212	
<u>9.11.4</u>	<u>Class Actual Activity <<Intersection>></u>	214
<u>9.11.5</u>	<u>Class Actual Event <<Intersection>></u>	214
<u>9.11.6</u>	<u>Class Event</u> ..215	
<u>9.11.7</u>	<u>Association Class Output <<Relationship>></u>	215
<u>9.11.8</u>	<u>Association Class Performance <<Relationship>></u>	216
<u>9.11.9</u>	<u>Association Class Usage <<Relationship>></u>	217
<u>9.12</u>	<u>Threat risk conceptual model::Generic Concept Library::Identifiers and Coordinates</u>	218
<u>9.12.1</u>	<u>Diagram: Identifiers</u>	219
<u>9.12.2</u>	<u>Class Coordinate <<Value>></u>	219
<u>9.12.3</u>	<u>Class Coordinate System</u>	220
<u>9.12.4</u>	<u>Association System of Coordinate</u>	220
<u>9.13</u>	<u>Threat risk conceptual model::Generic Concept Library::Information</u>	221
<u>9.13.1</u>	<u>Diagram: Information Action</u>	221
<u>9.13.2</u>	<u>Diagram: Information Objects</u>	222
<u>9.13.3</u>	<u>Diagram: Metadata</u>	223
<u>9.13.4</u>	<u>Class Add Information</u>	223
<u>9.13.5</u>	<u>Class Atomic Information Object</u>	224
<u>9.13.6</u>	<u>Class Close Information</u>	224
<u>9.13.7</u>	<u>Class Confidence</u> ..224	

<u>9.13.8</u> — <u>Association Confidence in Assertion</u>	224
<u>9.13.9</u> — <u>Association Class Contained Information <<Relationship>></u>	225
<u>9.13.10</u> — <u>Class Create Information</u>	226
<u>9.13.11</u> — <u>Class Delete Information</u>	226
<u>9.13.12</u> — <u>Class Document</u>	226
<u>9.13.13</u> — <u>Class Information Action</u>	226
<u>9.13.14</u> — <u>Class Information Object</u>	227
<u>9.13.15</u> — <u>Class Information Repository</u>	227
<u>9.13.16</u> — <u>Class Information Resource <<Union>></u>	227
<u>9.13.17</u> — <u>Class Information Type</u>	228
<u>9.13.18</u> — <u>Class Modify Information</u>	228
<u>9.13.19</u> — <u>Class Open Information</u>	228
<u>9.13.20</u> — <u>Class Read Information</u>	228
<u>9.13.21</u> — <u>Class Remove Information</u>	229
<u>9.13.22</u> — <u>Class Structured Information Object</u>	229
<u>9.13.23</u> — <u>Class Transfer Information</u>	229
<u>9.14</u> — <u>Threat risk conceptual model::Generic Concept Library::Locations</u>	230
<u>9.14.1</u> — <u>Diagram: Location</u>	230
<u>9.14.2</u> — <u>Diagram: Location Identification</u>	231
<u>9.14.3</u> — <u>Association Address of Location</u>	231
<u>9.14.4</u> — <u>Association Coordinate of location</u>	232
<u>9.14.5</u> — <u>Association Designation of a Location</u>	232
<u>9.14.6</u> — <u>Class Location ID <<Value>></u>	232
<u>9.14.7</u> — <u>Class Location Identifier <<Value>></u>	232
<u>9.14.8</u> — <u>Association Class Physical Boundary <<Relationship>></u>	233
<u>9.14.9</u> — <u>Class Physical Location</u>	233
<u>9.14.10</u> — <u>Class Physical Point</u>	234
<u>9.14.11</u> — <u>Class Point On Earth <<Value>></u>	234
<u>9.14.12</u> — <u>Association Reference Point</u>	235
<u>9.14.13</u> — <u>Class Relative Coordinate <<Value>></u>	235
<u>9.14.14</u> — <u>Class Spacial Coordinate <<Value>></u>	235
<u>9.14.15</u> — <u>Association Topological Region</u>	236
<u>9.14.16</u> — <u>Class Topology</u>	236
<u>9.14.17</u> — <u>Class World Geodetic System <<Value>></u>	236
<u>9.15</u> — <u>Threat risk conceptual model::Generic Concept Library::Objectives</u>	238
<u>9.15.1</u> — <u>Diagram: Objectives</u>	238
<u>9.15.2</u> — <u>Class Benefit</u>	239

<u>9.15.3</u> — <u>Class Consequence</u>	239
<u>9.15.4</u> — <u>Association Class Consequence of Situation <<Relationship>></u>	241
<u>9.15.5</u> — <u>Class Desirability Assessment</u>	242
<u>9.15.6</u> — <u>Class Means <<Role>></u>	242
<u>9.15.7</u> — <u>Association Class Means To End <<Relationship>></u>	243
<u>9.15.8</u> — <u>Class Objective</u>	243
<u>9.15.9</u> — <u>Association Class Objective of Stakeholder <<Relationship>></u>	245
<u>9.15.10</u> — <u>Class Opportunity</u>	245
<u>9.15.11</u> — <u>Class Stakeholder <<Role>></u>	246
<u>9.15.12</u> — <u>Association Class Stakeholder Desirability <<Relationship>></u>	247
<u>9.16</u> — <u>Threat risk conceptual model::Generic Concept Library::Observations</u>	248
<u>9.16.1</u> — <u>Diagram: Measurement</u>	248
<u>9.16.2</u> — <u>Diagram: Observability</u>	248
<u>9.16.3</u> — <u>Diagram: Observations</u>	249
<u>9.16.4</u> — <u>Association Context of Observation</u>	249
<u>9.16.5</u> — <u>Association Class Measurement <<Relationship>></u>	249
<u>9.16.6</u> — <u>Association Class Observability <<Relationship>></u>	250
<u>9.16.7</u> — <u>Association Class Observation <<Relationship>></u>	250
<u>9.16.8</u> — <u>Class Observation Tool <<Role>></u>	251
<u>9.16.9</u> — <u>Class Observer <<Role>></u>	251
<u>9.17</u> — <u>Threat risk conceptual model::Generic Concept Library::Organizations</u>	253
<u>9.17.1</u> — <u>Diagram: Organization</u>	253
<u>9.17.2</u> — <u>Association Class Membership <<Relationship>></u>	253
<u>9.17.3</u> — <u>Class Mission Objective</u>	254
<u>9.17.4</u> — <u>Class Organization</u>	255
<u>9.17.5</u> — <u>Class Organizational Unit <<Role>></u>	255
<u>9.17.6</u> — <u>Class Parent Organization <<Role>></u>	255
<u>9.17.7</u> — <u>Association Class Part of Organization <<Relationship>></u>	256
<u>9.17.8</u> — <u>Class Program</u>	257
<u>9.18</u> — <u>Threat risk conceptual model::Generic Concept Library::Organizations::Corporations</u>	258
<u>9.18.1</u> — <u>Diagram: Corporations</u>	258
<u>9.18.2</u> — <u>Class Incorporated Organization</u>	258
<u>9.18.3</u> — <u>Association Class Incorporation <<Relationship>></u>	258
<u>9.19</u> — <u>Threat risk conceptual model::Generic Concept Library::Organizations::Geopolitical Organizations</u>	260
<u>9.19.1</u> — <u>Diagram: Geopolitical Entities</u>	260
<u>9.19.2</u> — <u>Class Country</u>	260
<u>9.19.3</u> — <u>Class Country ID <<Value>></u>	261

<u>9.19.4</u> — <u>Class Geopolitical Entity</u>	261
<u>9.19.5</u> — <u>Class Geopolitical ID <<Value>></u>	261
<u>9.19.6</u> — <u>Class Geopolitical Region <<Role>></u>	262
<u>9.19.7</u> — <u>Association Class Governing Authority <<Relationship>></u>	262
<u>9.20</u> — <u>Threat risk conceptual model: Generic Concept Library::Permissions</u>	263
<u>9.20.1</u> — <u>Diagram: Permission</u>	263
<u>9.20.2</u> — <u>Association Class Permission</u>	264
<u>9.21</u> — <u>Threat risk conceptual model: Generic Concept Library::Persons</u>	265
<u>9.21.1</u> — <u>Diagram: Person</u>	265
<u>9.21.2</u> — <u>Diagram: Person Identifiers</u>	266
<u>9.21.3</u> — <u>Diagram: Person Name Representations</u>	267
<u>9.21.4</u> — <u>Class Access Identifier <<Value>></u>	267
<u>9.21.5</u> — <u>Class Financial Identifier <<Value>></u>	267
<u>9.21.6</u> — <u>Class Managed Person Identifier <<Value>></u>	268
<u>9.21.7</u> — <u>Class Passport Identifier <<Value>></u>	268
<u>9.21.8</u> — <u>Class Person</u> 268	
<u>9.21.9</u> — <u>Association Class Person at location <<Relationship>></u>	269
<u>9.21.10</u> — <u>Class Person Name <<Value>></u>	269
<u>9.21.11</u> — <u>Class Person Structured Name <<Value>></u>	270
<u>9.21.12</u> — <u>Association Class Residency <<Relationship>></u>	271
<u>9.21.13</u> — <u>Class Social Security Number <<Value>></u>	271
<u>9.22</u> — <u>Threat risk conceptual model: Generic Concept Library::Physical Entities</u>	272
<u>9.22.1</u> — <u>Diagram: Physical Entities</u>	273
<u>9.22.2</u> — <u>Class Animal</u> 273	
<u>9.22.3</u> — <u>Class Conveyance</u>	274
<u>9.22.4</u> — <u>Class Device</u> 275	
<u>9.22.5</u> — <u>Class Item</u> 275	
<u>9.22.6</u> — <u>Class Managed Item Identifier <<Value>></u>	275
<u>9.22.7</u> — <u>Class Physical Entity</u>	276
<u>9.22.8</u> — <u>Class Physical Feature</u>	276
<u>9.22.9</u> — <u>Class Physical Tool <<Role>></u>	276
<u>9.22.10</u> — <u>Class Spacial Entity</u>	276
<u>9.22.11</u> — <u>Class Telecommunication Device</u>	277
<u>9.23</u> — <u>Threat risk conceptual model: Generic Concept Library::Places</u>	280
<u>9.23.1</u> — <u>Diagram: Place</u>	280
<u>9.23.2</u> — <u>Class Facility <<Role>></u>	280
<u>9.23.3</u> — <u>Association Class Operating Location <<Relationship>></u>	280

<u>9.23.4</u>	<u>Class Place <<Role>></u>	281
<u>9.23.5</u>	<u>Association Class Place of Occurrence <<Relationship>></u>	282
<u>9.23.6</u>	<u>Class Residence <<Role>></u>	282
<u>9.24</u>	<u>Threat risk conceptual model::Generic Concept Library::Policies</u>	284
<u>9.24.1</u>	<u>Diagram: Policy</u>	284
<u>9.24.2</u>	<u>Association Class Assertion of Policy <<Relationship>></u>	284
<u>9.24.3</u>	<u>Class Policy</u>	285
<u>9.25</u>	<u>Threat risk conceptual model::Generic Concept Library::Predictions</u>	287
<u>9.25.1</u>	<u>Diagram: Prediction</u>	287
<u>9.25.2</u>	<u>Association Class Prediction <<Relationship>></u>	287
<u>9.25.3</u>	<u>Class Predictor <<Role>></u>	288
<u>9.26</u>	<u>Threat risk conceptual model::Generic Concept Library::Processes</u>	290
<u>9.26.1</u>	<u>Diagram: Process</u>	291
<u>9.26.2</u>	<u>Association Class Invoke Process <<Relationship>></u>	292
<u>9.26.3</u>	<u>Class Modus Operandi</u>	292
<u>9.26.4</u>	<u>Class Plan</u>	293
<u>9.26.5</u>	<u>Class Process Action</u>	293
<u>9.26.6</u>	<u>Association Class Process Decomposition <<Relationship>></u>	293
<u>9.26.7</u>	<u>Class Process Pattern</u>	294
<u>9.26.8</u>	<u>Class Scenario</u>	295
<u>9.26.9</u>	<u>Association Class When <<Relationship>></u>	296
<u>9.27</u>	<u>Threat risk conceptual model::Generic Concept Library::Processes::Composite Conditions</u>	298
<u>9.27.1</u>	<u>Diagram: Composite Condition</u>	298
<u>9.27.2</u>	<u>Class AND Condition</u>	298
<u>9.27.3</u>	<u>Class Composite Condition</u>	298
<u>9.27.4</u>	<u>Class OR Condition</u>	299
<u>9.27.5</u>	<u>Class XOR Condition</u>	299
<u>9.28</u>	<u>Threat risk conceptual model::Generic Concept Library::Processes::Process Effects</u>	300
<u>9.28.1</u>	<u>Diagram: Process Effects</u>	300
<u>9.28.2</u>	<u>Class Activity Effecting Entity</u>	301
<u>9.28.3</u>	<u>Class Create</u>	301
<u>9.28.4</u>	<u>Class Damage</u>	301
<u>9.28.5</u>	<u>Class Destroy</u>	302
<u>9.28.6</u>	<u>Class Disrupt Process</u>	302
<u>9.28.7</u>	<u>Class Entry Action</u>	302
<u>9.28.8</u>	<u>Class Exit Action</u>	302
<u>9.28.9</u>	<u>Class Pause Process</u>	302

9.28.10	Class Possible Actions	303
9.28.11	Class Stop Process	303
9.29	Threat risk conceptual model::Generic Concept Library::Quantities and Units	304
9.29.1	Diagram: Quantities and units	305
9.29.2	Class Confidence Metric <<Quantity Kind>>	306
9.29.3	Class Count <<Quantity Kind>>	306
9.29.4	Class Currency Benefit Metric <<Quantity Kind>>	306
9.29.5	Class Harm Benefit Metric <<Quantity Kind>>	306
9.29.6	Class Metrie <<Quantity Kind>>	306
9.29.7	Class Probability Metric <<Quantity Kind>>	307
9.29.8	Class Time Coordinate <<Quantity Kind>>	307
9.30	Threat risk conceptual model::Generic Concept Library::Quantities and Units::Quantity Kinds	312
9.30.1	Diagram: Quantity Kinds	312
9.30.2	Class Absorbed Dose (Radiation) <<Quantity Kind>>	312
9.30.3	Class Acceleration <<Quantity Kind>>	313
9.30.4	Class Amount of Substance <<Quantity Kind>>	313
9.30.5	Class Angle <<Quantity Kind>>	313
9.30.6	Class Area <<Quantity Kind>>	313
9.30.7	Class Color <<Quantity Kind>>	313
9.30.8	Class Concentration <<Quantity Kind>>	314
9.30.9	Class Concentration (amount of substance) <<Quantity Kind>>	314
9.30.10	Class Concentration (Mass) <<Quantity Kind>>	314
9.30.11	Class Concentration (Volume) <<Quantity Kind>>	314
9.30.12	Class Currency <<Quantity Kind>>	314
9.30.13	Class Dose Equivalent (Radiation) <<Quantity Kind>>	315
9.30.14	Class Duration <<Quantity Kind>>	315
9.30.15	Class Electric Current <<Quantity Kind>>	315
9.30.16	Class Elecrtic Potential <<Quantity Kind>>	316
9.30.17	Class Energy <<Quantity Kind>>	316
9.30.18	Class Force <<Quantity Kind>>	316
9.30.19	Class Frequency <<Quantity Kind>>	316
9.30.20	Class Length <<Quantity Kind>>	317
9.30.21	Class Luminosity <<Quantity Kind>>	317
9.30.22	Class Mass <<Quantity Kind>>	317
9.30.23	Class Mass Density <<Quantity Kind>>	317
9.30.24	Class Physical Quantity <<Quantity Kind>>	317
9.30.25	Class Power <<Quantity Kind>>	318

<u>9.30.26</u> <u>Class Pressure <<Quantity Kind>></u>	318
<u>9.30.27</u> <u>Class Radiation Exposure <<Quantity Kind>></u>	318
<u>9.30.28</u> <u>Class Radioactivity <<Quantity Kind>></u>	318
<u>9.30.29</u> <u>Class Speed <<Quantity Kind>></u>	318
<u>9.30.30</u> <u>Class Temperature <<Quantity Kind>></u>	319
<u>9.30.31</u> <u>Class Volume <<Quantity Kind>></u>	319
<u>9.31</u> Threat risk conceptual model::Generic Concept Library::Resources	320
<u>9.31.1</u> <u>Diagram: Resource</u>	320
<u>9.31.2</u> <u>Diagram: Resource Actions</u>	321
<u>9.31.3</u> <u>Class Abuse Resource</u>	321
<u>9.31.4</u> <u>Class Capture Resource</u>	321
<u>9.31.5</u> <u>Class Damage Resource</u>	321
<u>9.31.6</u> <u>Class Exceed Resource Capacity</u>	322
<u>9.31.7</u> <u>Class Modify Resource</u>	322
<u>9.31.8</u> <u>Class Performer <<Role>></u>	322
<u>9.31.9</u> <u>Class Resource <<Role>></u>	322
<u>9.31.10</u> <u>Class Resource Actions</u>	323
<u>9.31.11</u> <u>Association Class Resource Dependency <<Relationship>></u>	324
<u>9.31.12</u> <u>Class Tool <<Role>></u>	324
<u>9.32</u> Threat risk conceptual model::Generic Concept Library::Situations	325
<u>9.32.1</u> <u>Diagram: Situation</u>	326
<u>9.32.2</u> <u>Diagram: Situation Timeframes</u>	327
<u>9.32.3</u> <u>Class Actual State <<Intersection>></u>	327
<u>9.32.4</u> <u>Association Class Cause and Effect <<Relationship>></u>	327
<u>9.32.5</u> <u>Class Current Situation</u>	328
<u>9.32.6</u> <u>Association Class Effect <<Relationship>></u>	329
<u>9.32.7</u> <u>Association Class Involvement <<Relationship>></u>	329
<u>9.32.8</u> <u>Association Class Negation Effect <<Relationship>></u>	330
<u>9.32.9</u> <u>Class Past Situation</u>	331
<u>9.32.10</u> <u>Class Potential Situation</u>	332
<u>9.32.11</u> <u>Association Class Scope of Indicator <<Relationship>></u>	332
<u>9.32.12</u> <u>Class State</u>	333
<u>9.32.13</u> <u>Association State of Entity</u>	333
<u>9.33</u> Threat risk conceptual model::Generic Concept Library::Social Agents	334
<u>9.33.1</u> <u>Diagram: Social Agent</u>	334
<u>9.33.2</u> <u>Diagram: Social Agent Identifiers</u>	335
<u>9.33.3</u> <u>Association Class Associated Actor <<Relationship>></u>	335

<u>9.33.4</u>	<u>Class License Identifier <<Value>></u>	336
<u>9.33.5</u>	<u>Class Local Identifier <<Value>></u>	336
<u>9.33.6</u>	<u>Class Managed Social Agent Identifier <<Value>></u>	336
<u>9.33.7</u>	<u>Class Regional Identifier <<Value>></u>	336
<u>9.33.8</u>	<u>Class Social Agent</u>	337
<u>9.33.9</u>	<u>Class Tax Authority Identifier <<Value>></u>	337
<u>9.34</u>	<u>Threat risk conceptual model::Generic Concept Library::Systems</u>	338
<u>9.34.1</u>	<u>Diagram: System</u>	338
<u>9.34.2</u>	<u>Class Access Point</u>	339
<u>9.34.3</u>	<u>Class Boundary</u>	339
<u>9.34.4</u>	<u>Association Class Boundary of System <<Relationship>></u>	339
<u>9.34.5</u>	<u>Association Class Opening in a Boundary <<Relationship>></u>	340
<u>9.34.6</u>	<u>Association Class Point Of Entry <<Relationship>></u>	341
<u>9.34.7</u>	<u>Class Subsystem <<Role>></u>	342
<u>9.34.8</u>	<u>Class System</u>	342
<u>9.35</u>	<u>Threat risk conceptual model::Generic Concept Library::Time & Temporal Entities</u>	344
<u>9.35.1</u>	<u>Diagram: Time</u>	345
<u>9.35.2</u>	<u>Class Date and Time <<Quantity Kind>></u>	346
<u>9.35.3</u>	<u>Class Date Coordinate <<Quantity Kind>></u>	346
<u>9.35.4</u>	<u>Association Duration of Entity</u>	346
<u>9.35.5</u>	<u>Association Entity Exists for Interval</u>	347
<u>9.35.6</u>	<u>Association Finish Time</u>	347
<u>9.35.7</u>	<u>Association Overlaps in Time</u>	348
<u>9.35.8</u>	<u>Association Start Time</u>	349
<u>9.35.9</u>	<u>Association Temporal Order</u>	350
<u>9.35.10</u>	<u>Association Class Temporal Part <<Relationship>></u>	351
<u>9.35.11</u>	<u>Class Time Coordinate <<Quantity Kind>></u>	351
<u>9.35.12</u>	<u>Class Time Interval</u>	352
<u>9.35.13</u>	<u>Class Time Point</u>	352
<u>9.35.14</u>	<u>Class Time Scale</u>	353
<u>9.35.15</u>	<u>Association Time Scale Granularity</u>	353
<u>9.35.16</u>	<u>Association Time Scale of Time Point</u>	354
<u>9.36</u>	<u>Threat risk conceptual model::Generic Concept Library::Time & Temporal Entities::ISO Time Scale</u>	355
<u>9.36.1</u>	<u>Diagram: ISO Time</u>	355
<u>9.36.2</u>	<u>Class Date Time Coordinate (ISO 8601) <<Unit Value>></u>	356
<u>9.37</u>	<u>Threat risk conceptual model::Generic Concept Library::Time & Temporal Entities::XSD Time Scale</u>	357
<u>9.37.1</u>	<u>Diagram: XSD Time Scale</u>	357

<u>9.37.2</u>	<u>Class XSD Date <<Unit Value>></u>	357
<u>9.37.3</u>	<u>Class XSD Date Time <<Unit Value>></u>	358
<u>9.37.4</u>	<u>Class XSD Time <<Unit Value>></u>	358
<u>9.38</u>	<u>Threat risk conceptual model::Generic Concept Library::Vendors and Producers</u>	359
<u>9.38.1</u>	<u>Diagram: Vendors and Producers</u>	359
<u>9.38.2</u>	<u>Class Client <<Role>></u>	359
<u>9.38.3</u>	<u>Class Individual Product <<Role>></u>	360
<u>9.38.4</u>	<u>Class Manufactured Thing <<Role>></u>	360
<u>9.38.5</u>	<u>Class Producer <<Role>></u>	360
<u>9.38.6</u>	<u>Class Product Kind</u>	361
<u>9.38.7</u>	<u>Association Class Product Line of Supplier <<Relationship>></u>	361
<u>9.38.8</u>	<u>Association Class Production <<Relationship>></u>	362
<u>9.38.9</u>	<u>Association Class Providing <<Relationship>></u>	362
<u>9.38.10</u>	<u>Class Serial Number <<Value>></u>	363
<u>9.38.11</u>	<u>Class Supplier <<Role>></u>	364
<u>10</u>	<u>STIX Mapping Specification (Normative)</u>	365
<u>10.1</u>	<u>How STIX is represented</u>	365
<u>10.2</u>	<u>Generic STIX Mapping Rules and Conventions</u>	365
<u>10.3</u>	<u>STIX Mapping to the threat/risk conceptual reference model</u>	367
<u>10.3.1</u>	<u>Diagram: High Level STIX Mapping</u>	367
<u>10.4</u>	<u>STIX Mapping to the threat/risk conceptual reference model::Facades</u>	368
<u>10.4.1</u>	<u>Diagram: Facade Summary</u>	368
<u>10.4.2</u>	<u>Class ActualObservableFacade</u>	369
<u>10.4.3</u>	<u>Class AffectedAssetFacade</u>	369
<u>10.4.4</u>	<u>Class ExploitTargetFacade</u>	369
<u>10.4.5</u>	<u>Class ObservablePatternFacade</u>	369
<u>10.4.6</u>	<u>Class Threat Report</u>	369
<u>10.5</u>	<u>STIX Mapping to the threat/risk conceptual reference model::STIX Mapping Rules</u>	371
<u>10.6</u>	<u>Class STIX Campaign Rule</u>	371
<u>10.7</u>	<u>Class STIX Categories Rule</u>	372
<u>10.8</u>	<u>Class STIX Course Of Action Rule</u>	373
<u>10.9</u>	<u>Class STIX Incident Rule</u>	374
<u>10.10</u>	<u>Class STIX Indicator Rule</u>	375
<u>10.11</u>	<u>Class STIX Objective Rule</u>	376
<u>10.12</u>	<u>Class STIX Observable Rule</u>	377
<u>10.13</u>	<u>Class STIX Sighting Rule</u>	378
<u>10.14</u>	<u>Class STIX Statement Rule</u>	379

10.15	Class STIX Threat Actor Rule	380
10.16	Class STIX TTP Rule	381
10.17	Class STIX Vocabulary Rule	382
10.18	Class STIX Vulnerability Rule	383
11	NIEM Mapping Specification (Normative)	384
11.1	How NIEM is represented	384
11.2	Generic NIEM mapping rules and conventions	384
11.3	NIEM Mapping to the threat / risk model::Facades::Contact Information	387
11.3.1	Diagram: Contact Information Facades	387
11.3.2	Class Postal Address Facade	387
11.3.3	Class Telephone Number Facade	388
11.4	NIEM Mapping to the threat / risk model::Facades::Injury	389
11.4.1	Diagram: Person Injury Facade	389
11.4.2	Class PersonInjuryFacade	389
11.5	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships	390
11.5.1	Diagram: NIEM Mapping Rules	390
11.5.2	Diagram: NIEM Mapping Summary 1	391
11.5.3	Diagram: NIEM Mapping Summary 2	392
11.6	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Activity	393
11.6.1	Diagram: Activity Mapping Summary	393
11.6.2	Class Activity Map Rule	393
11.7	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Assessment	395
11.7.1	Diagram: Assessment Mapping Summary	395
11.7.2	Class Assessment Map Rule	396
11.8	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation	397
11.8.1	Diagram: Contact Information Mapping Summary	397
11.8.2	Class Address Map Rule	398
11.8.3	Class Contact Information Mapping Rule	399
11.8.4	Class Internet Contact Map Rule	400
11.8.5	Class Radio Map Rule	401
11.8.6	Class Telephone Map Rule	402
11.9	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Entity	403
11.9.1	Diagram: Entity Mapping Summary	403
11.9.2	Class Entity Map Rule	403
11.10	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Identification	405

<u>11.10.1—Diagram: Identification Mapping Summary</u>	405
<u>11.10.2—Class Identification Map Rule</u>	406
<u>11.11—NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Incident</u>	407
<u>11.11.1—Diagram: Incident mapping summary</u>	407
<u>11.11.2—Class Incident Map Rule</u>	407
<u>11.12—NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Injury</u>	409
<u>11.12.1—Diagram: Injury Mapping Summary</u>	409
<u>11.12.2—Class Injury Map Rule</u>	410
<u>11.13—NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Item</u>	411
<u>11.13.1—Diagram: Item Mapping Summary</u>	411
<u>11.13.2—Class Item Map Rule</u>	412
<u>11.14—NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location</u>	413
<u>11.14.1—Diagram: Location mapping summary</u>	414
<u>11.14.2—Class Area Map Rule</u>	415
<u>11.14.3—Class Coordinate Map Rule</u>	415
<u>11.14.4—Class Facility Map Rule</u>	416
<u>11.14.5—Class Location Map Rule</u>	417
<u>11.15—NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Organization</u>	418
<u>11.15.1—Diagram: NIEM Organization Mapping Summary</u>	418
<u>11.15.2—Class Organization Map Rule</u>	419
<u>11.16—NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Person</u>	420
<u>11.16.1—Diagram: Person Mapping Summary</u>	420
<u>11.16.2—Class Person Map Rule</u>	421
<u>11.16.3—Class Person Name Map Rule</u>	422
<u>11.17—NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM PrimitiveTypes</u>	423
<u>11.17.1—Diagram: Primitive Type Mapping</u>	423
<u>12—Threat and Risk Alignment to NIST 800-53</u>	424
<u>13—Concept Index</u>	457

Preface

OMG

Founded in 1989, the Object Management Group, Inc. (OMG) is an open membership, not-for-profit computer industry standards consortium that produces and maintains computer industry specifications for interoperable, portable, and

reusable enterprise applications in distributed, heterogeneous environments. Membership includes Information Technology vendors, end users, government agencies, and academia.

OMG member companies write, adopt, and maintain its specifications following a mature, open process. OMG's specifications implement the Model Driven Architecture® (MDA®), maximizing ROI through a full-lifecycle approach to enterprise integration that covers multiple operating systems, programming languages, middleware and networking infrastructures, and software development environments. OMG's specifications include: UML® (Unified Modeling Language™); CORBA® (Common Object Request Broker Architecture); CWM™ (Common Warehouse Metamodel); and industry-specific standards for dozens of vertical markets.

More information on the OMG is available at <http://www.omg.org/>.

OMG Specifications

As noted, OMG specifications address middleware, modeling, and vertical domain frameworks. All OMG Specifications are available from the OMG website at:

<http://www.omg.org/spec>

Specifications are organized by the following categories:

Business Modeling Specifications

Middleware Specifications

- CORBA/IOP
- Data Distribution Services
- Specialized CORBA

IDL/Language Mapping Specifications

Modeling and Metadata Specifications

- UML, MOF, CWM, XMI
- UML Profile

Modernization Specifications

Platform Independent Model (PIM), Platform Specific Model (PSM), Interface Specifications

- CORBAServices
- CORBAFacilities

CORBA Embedded Intelligence Specifications

CORBA Security Specifications

OMG Domain Specifications

Signal and Image Processing Specifications

All of OMG's formal specifications may be downloaded without charge from our website. (Products implementing OMG specifications are available from individual suppliers.) Copies of specifications, available in PostScript and PDF format, may be obtained from the Specifications Catalog cited above or by contacting the Object Management Group, Inc. at:

OMG Headquarters
109 Highland Avenue
Needham, MA 02494
USA
Tel: +1-781-444-0404
Fax: +1-781-444-0320
Email: pubs@omg.org

Certain OMG specifications are also available as ISO standards. Please consult <http://www.iso.org>

Typographical Conventions

The type styles shown below are used in this document to distinguish programming statements from ordinary English. However, these conventions are not used in tables or section headings where no distinction is necessary.

Times/Times New Roman - 10 pt.: Standard body text

Helvetica/Arial - 10 pt. Bold: OMG Interface Definition Language (OMG IDL) and syntax elements.

Courier - 10 pt. Bold: Programming language elements.

Helvetica/Arial - 10 pt.: Exceptions.

NOTE: Terms that appear in italics are defined in the glossary. Italic text also represents the name of a document, specification, or other publication.

Issues

The reader is encouraged to report any technical or editing issues/problems with this specification to http://www.omg.org/report_issue.htm.

0 Submission-related material

0.1 Submission Introduction

The Threat/Risk submission team is pleased to present a revised submission to the “UML Operational Threat & Risk Model” Request for Proposal SysA/2014-06-17

The IPR mode for this submission is **Non-Assert**.

Clause 0 of this document contains information specific to the OMG submission process and is not part of the proposed specification. The proposed specification starts with Clause 1. All clauses are normative unless otherwise specified.

0.2 Submission Team

0.2.1 Submitters

- Model Driven Solutions division of Data Access Technologies (<http://www.modeldriven.com>)
 - Cory Casanave
- KDM Analytics, Inc. (<http://www.kdmanalytics.com>)
 - Djenana Campara
 - Nick Mansourov
- International Business Machines, Inc. (<http://www.ibm.com>)
 - Bruce Douglass
- RSA, The Security Division of EMC (<http://www.rsa.com>)
 - Chris Hoover
- Oracle Corporation
 - Pat Sack
- Fujitsu
 - Kazuo Noguchi

0.2.2 Contributors & Supporters

- U.S. Information Sharing Environment PMO (<http://www.ise.gov>)
 - Kshemendra Paul
 - Pamela Wise-Martinez
 - Vijay Mehra
- Demandware (<http://www.demandware.com/>)
 - Gerald Beuchelt
- U.S. Air Force

- Harrell Van Norman
 - Kalabhi Patel
- U.S. Defense Security Services
 - Mark Nehmer
- California Public Safety (<http://www.Caloes.ca.gov>)
 - Nicole Meyer-Morse
 - Caroline Thomas Jacobs
- U.S. National Information Sharing Model PMO (<https://www.niem.gov/>)
 - Justin Stekervetz
- Lockheed Martin, Inc.
 - Ben Calloni
- Duke Energy
 - Stuart Laval
 - David Lawrence
- NSA/UCDMO
- NIST
 - Ron Ross
- INCOSE
 - Joe Weiss
- Integrated Networking Technologies, Inc.
 - Patrick Maroney
- Tibco Software Inc.
 - Paul Brown
- FRHack
 - Jerome Athias

0.3 Proof of concept

The NoMagic “Concept Modeler” product implements most of the conceptual reference modeling profile and is evolving to implement the entire profile and OWL mapping.

Formatted: omg-body, No bullets or numbering

Prototype efforts are expected but have not yet fully validated the model and mappings.

0.4 Resolution of Requirements

0.4.1 Mandatory requirements

6.5.1 Conceptual model Conceptual reference models	The conceptual model conceptual reference models are specified in section Error! Reference source not found. 8. Conceptual Model Conceptual reference model Specification (Normative) Each package represents a module.
6.5.1.1 Submissions shall define modular UML conceptual model conceptual reference models to specify the concepts required to represent information about operational threats and risks.	The conceptual model conceptual reference models are specified in section Error! Reference source not found. 8. Conceptual Model Conceptual reference model Specification (Normative) Each package represents a module.
6.5.1.2 The conceptual model conceptual reference model shall capture the intended meaning of operational threat and risk related concepts such that it may be used as a reference for the use of those concepts in specific exchanges and data stores.	The conceptual model conceptual reference model is a model of the concepts of threat and risk; these are then mapped to data structures in STIX and NIEM.
6.5.1.3 The conceptual model conceptual reference model shall not assume any particular technology, domain, and representation, structure of information, or schema. It shall be a model of the concepts representing real-world entities, not of a specific data representation.	No technology is assumed. The conceptual model conceptual reference model is a model of the concepts representing real-world entities, not of a specific data representation.
6.5.2 Operational Threat and Risk Concepts	
6.5.2.1 The conceptual model conceptual reference models shall provide definitions of the concepts of "operational threats" and "operational risk". Proposals shall use standard terminology when applicable. References to existing standards shall be provided to facilitate mappings and avoid ambiguity.	Risk and threat are defined in the model. The operational focus is defined in the glossary. "operational threat" and "operational risk" are defined in the glossary.
6.5.2.2 Proposal's conceptual model conceptual reference models shall define other concepts related to common operational threat and risk terms including but not limited to: Asset, Campaign, Cause, Effect, Exploit target, Goal, Hazard, Impact, Incident, Indicator, Likelihood, Mitigation, Observable, Observation, Observation metadata, Procedures, Risk, Safeguard, Severity, Strategy, Tactics, Techniques, Threat, Threat actor, Threat source, Undesired event.	All of the specified concepts are defined and modeled, however the terms may be slightly different in the model or glossary.
6.5.2.3 The concepts of threats shall include the following classifications: <ul style="list-style-type: none">• Cyber/information and communication systems and assets• Physical systems and assets, including embedded and manufacturing• Electromagnetic spectrum assets (E.g., interference with wireless systems or radio)	Categories are provided for all identified classifications in section 8.32. Others have been be -added as extensions.

Formatted: Font: 9 pt

Formatted: omg-body

<ul style="list-style-type: none"> Industrial control systems 	
6.5.2.4 Models for operational threats and risks shall be consistent with the following constraints: <ul style="list-style-type: none"> Defensive, offensive, or other actors may or may not have insight into the plans or strategies of the respective other actors. As such, model implementations will in those cases be incomplete and rely on estimates and assumed parameters. Models must be able to support non-actor threats (such as natural disasters) that will not be associated with any coherent intentions or plans. Bystanders and inadvertent actors may perform actions that result in behavior that provides benefits to any other actor (offensive or defensive). Such actions are understood to be non-intentional. The focus of risks will be those that go beyond the normal course of business and expose the enterprise to increased risk due to threats & vulnerabilities. 	The model: <ul style="list-style-type: none"> Defines relations and properties not the specifics of data formats. The model is agnostic to who knows what, it is not expected that any party will have full knowledge however that knowledge may be represented when available. Intentional (actor related), natural and systematic threats and risks are supported. Actors in an incident may be non-intentional. I.e. Bystanders and inadvertent actors. Risks are focused on those caused by any danger, including human and non-human.
6.5.2.5 Models for operational threats and risks shall include concepts for expressing probability and/or confidence levels (e.g., for likelihood of occurrence and impact).	Likelihood and confidence metrics are included.
6.5.3 Risk Management concepts	
6.5.3.1 The conceptual model shall include concepts related to systematic identification of operational risks and assessing their likelihood and severity.	Operational risks and their likelihood and severity may be represented. This specification does not specify process or methodology.
6.5.3.2 The proposals shall include concepts related to prioritization of risks.	Risks may be rated as to their priority.
6.5.3.3 The proposals shall include concepts related to the mapping of risks, hazards and undesired events to descriptions of systems for the purpose of systematic hazard analysis and justifiable identification of risks.	This model does provide all the information necessary to support systematic hazard analysis and justifiable identification of risks. The processes, guidance and policies for such analysis are out of scope. The NIST framework provides process and policy guidance. A mapping to the NIST framework is included in section 12.
6.5.3.4 The proposals shall describe concepts related to exchange of risk indicators, including patterns for systematic identification of risks.	Indicators and patterns are included; see “pattern” (Error! Reference source not found.^{8.4}) and “indicator” (Error! Reference source not found.^{8.37}). These concepts are mapped to data types used in exchanges. Normative mapping of these concepts is specified in the STIX mapping.

6.5.4 Mitigation and courses of action	
6.5.4.1 The conceptual model conceptual reference models shall include concepts of “course of action” and mitigation of threats and risks.	Course of action rules are included (Error! Reference source not found. ^{8.39}).
Explanation: Coincident with understanding any threat or risk is taking steps to mitigate the specific threat and mitigate similar risks in the future. The conceptual model conceptual reference models for “course of action” and mitigation shall include corrective concepts for deterring, protecting, detecting, monitoring, limiting, preventive and recovery strategies, and courses of action.	
6.5.5 Threat and Risk Planning	
6.5.5.1 The conceptual model conceptual reference model shall include concepts for understanding, planning for and treating operational risks, threats and their contingencies at the governmental and enterprise level.	Options for risk treatment are included.
6.5.6 NIEM Representation and Mapping	
6.5.6.1 Submissions shall define a normative NIEM-UML PIM representation sufficient to capture the concepts as defined in the conceptual model conceptual reference models as defined above.	A NIEM mapping is provided in section 10.340 .
6.5.6.2 This NIEM-UML representation shall be mapped to the conceptual model conceptual reference models such that the meaning of each threat/risk relevant NIEM element is described in the conceptual model conceptual reference model .	A NIEM mapping is provided in section 10.340 .
6.5.6.3 The mapping shall be sufficiently expressive such that any set of instances represented in or logically mapped to the conceptual model conceptual reference model shall be able to be represented in NIEM (understanding that choices and rules will have to be made).	A full NIEM domain such that it could capture all of the threat/risk concepts would require support of the NIEM-PMO for the threat and risk related domains. Support and a domain steward has not been identified. The common concepts between the NIEM reference models and the conceptual model conceptual reference model have been defined in section 10.340 .
6.5.6.4 Any instance of the NIEM specification shall be able to be logically mapped to the conceptual model conceptual reference model .	The intent of the NIEM mapping is that the mapping shall be sufficiently expressive such that any instance of the subset of NIEM specification that is mapped shall support mapping data.
6.5.7 STIX mapping	
6.5.7.1 Submissions shall define a mapping to the subset of STIX that corresponds with the conceptual model conceptual reference model . This mapping shall demonstrate that the conceptual model conceptual reference model is sufficient to represent high-level STIX concepts.	A STIX mapping of common concepts and their representation in STIX is included in clause 89 .
6.5.8 Common requirements	
6.5.8.1 All models shall utilize UML and UML profiles as a foundation.	UML is utilized for the conceptual model conceptual reference model and mappings. Profiles are specified for

	<p>The conceptual modelconceptual reference modeling and mapping in section Error! Reference source not found. The profile is consistent with the proposed SMIF specification.</p>
6.5.8.2 Concepts that are required for understanding threats or risks should, as much as possible, be defined in a modular fashion such that these concepts may be reused for related threat/risk concepts NIEM and other reference models shall be used as a reference for such cross-domain concepts. It is understood that a model may be composed of multiple sub-models.	The conceptual model conceptual reference models are subdivided into multiple purpose specific packages with coupling minimized.

0.4.2 Non-mandatory features

6.6.1 Optional mappings Submissions may provide normative or non-normative mappings to support the following Platform Specific Models, or logical models for the following protocols or communities: <ul style="list-style-type: none">o OASIS Common Alerting Program & EDXLo Others as deemed important by submitters	A Mapping to NIST 800-53 is included in section 12. Unlike NIEM and STIX, this is not a data mapping – it is a mapping to the NIST controls and how threat/risk would help realize those controls.
6.6.2 Optional support for conceptual model conceptual reference model ing and mapping Submissions may reference and/or define non-normative UML profiles and associated QVT (or other ways to express mapping logic) for conceptual model conceptual reference model ing and the mapping. Submitters are encouraged to follow the progress of and use as appropriate SMIF, ODM, MDMI, semantic web and other efforts to help define conceptual model conceptual reference model and mappings.	A UML profile corresponding to tThe UML profile defined in SMIF is included in section utilized .
6.6.3 Optional MOF representation Submissions may define A MOF metamodel that utilizes the conceptual model conceptual reference model and provides an XMI representation of Operational Threats and Risks.	As a UML model, a MOF representation is automatic.
6.6.4 Optional Integration with UPDM Submissions may define conceptual integration points with UPDM.	The Risk portion of the model references some DoDAF concepts but a complete DoDAF mapping and integration of concepts is not provided. Integration points with UPDM are not specified.

0.5 Resolution of Discussion Issues

6.7.1 Simulation Submissions shall discuss how the models could be used for simulation. The intent is to support the use of complex
--

simulation systems (e.g., Monte Carlo methods) to test multiple scenarios.

As a ~~conceptual model~~conceptual reference model the information is there to support simulation, this includes metrics and options. However there is no explicit support for simulation. A simulation engine would need to map the ~~conceptual model~~conceptual reference model to their internal simulation data structure. ~~This specification does not define how a mapping engine would implement this capability.~~

Formatted: English (United States)

6.7.2 Applicability

Submissions shall discuss the applicability of their approach to possible future efforts to embrace other domains, specifications or levels of detail related to threats and risks.

The foundational and general concepts in the ~~conceptual model~~conceptual reference model provide the foundation for threats and risks but are not threat and risk specific. ~~Threat and risk specific concepts use and specialize these more general concepts and are segregated into their own modules.~~ The ~~foundational and general concepts~~ may then be used as linking concepts to other domains and viewpoints. The general concepts are intended to be specialized and augmented for various domains. For these reasons the foundational concepts and concept library ~~would~~may make a viable foundation for a general purpose information sharing and federation model ~~in future efforts~~.

6.7.3 Design choices

Submissions shall discuss their design choices for level of detail.

~~We looked for the~~The level of detail that corresponds to information to be shared both across domains and disciplines. ~~provides guidance on the appropriate level of detail. It was not our goal to replicate detailed interactions within a discipline (e.g. between cyber experts) or within an organization but to enable communication between different domains and different organizations with shared concerns. This perspective provided the guidance for the level of detail included.~~

Formatted: English (United States)

1.1 Scope

Organizations (commercial, non-for-profit, or government) conduct business/mission operations and consider various threats and risks that may disrupt these operations. Threats and risks are increasingly multi-dimensional in nature – especially those spanning both physical and cyber space. Examples of areas of impact include: Critical infrastructure protection, counter terrorism, and public safety including threats from deadly pathogen, defense, intelligence, and economical infrastructure.

Historically, these communities of interest (COIs) have made significant technical and financial investments by developing processes, policies, systems, and formats to respond to threats within their communities.

However, the effectiveness of these investments may be limited by the organizational maturity of these communities, and the problems get even more pronounced when there is need to share information across these communities. Due to the complexity, connectivity, and global nature of threats faced by modern organizations, effective risk management and situational awareness depend on collaboration and information sharing. Federating information across multiple communities, irrespective of technical and political boundaries, will enable us to effectively mitigate multi-dimensional intentional threats, natural events, and system failures.

The operational threat and risk conceptual model includes and integrates concepts from multiple communities and established data formats, focusing on those concepts that are deemed to be of interest across these communities. This specification defines a conceptual model for threat and risk concepts as well as mappings to augment, and not replace, specific data formats to enable operational threat and risk information sharing, data federation, analytics, and simulation.

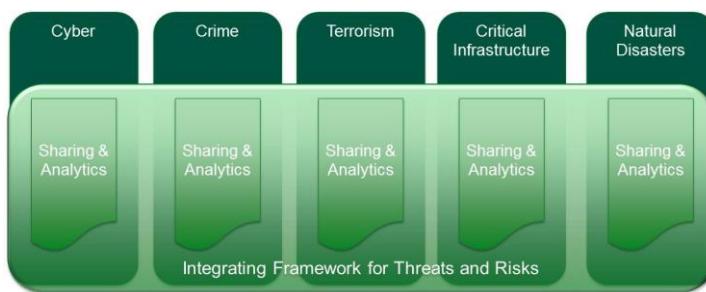


Figure 1. Integrating Framework

The ideal solution, illustrated above, shows an integrating framework that allows individual technologies and communities to evolve independently while providing the semantic definitions and mappings that enable broad-based information sharing and comprehensive analytics. This is being realized as a “conceptual model” (e.g., domain ontology) that captures common concepts – this conceptual model is then mapped to the various schemas/formats used in each community. This specification leverages concepts found in existing specifications, including but not limited to: NIEM, STIX, EDXL, NIST, OGC, and others. Machine executable mappings are then defined between the conceptual model and specific normative targets, including NIEM and STIX. The conceptual model and mappings are structured based on the Semantic Modeling for Information Federation [SMIF] draft submission, however these standards processes are independent.

The capabilities to federate information, analyze it and share across different formats will be provided by products and projects that leverage this specification.

2 Conformance

This specification defines the following conformance points (also referred to as conformance targets):

2.1 Canonical model conformance

Implementations claiming canonical model conformance shall be able to comprehend and represent data corresponding to the semantics of all of the concepts defined in the conceptual model/conceptual reference model. There is no specific technology, syntax, API, or representation requirement for canonical model conformance. Canonical model conformance must also include at least one conformant mapping as defined in sections 2.2 through 2.4.

While not required, canonical model conformant implementations are expected to provide a mechanism to produce or rationalize data in multiple formats, leading to developing capabilities like data federation or data transformation, and advanced features like simulations, metrics, and analytics.

2.2 Information model mapping conformance

A data format An information model mapping implementation may claim conformance provided it:

- Represents mappings in the same form as the normative mappings
- Maps to a subset of threat/risk concepts defined in the conceptual model/conceptual reference model where that subset enables a meaningful interaction between parties
- Fulfills either canonical model conformance or mapping conformance to one of the normative mappings: STIX or NIEM
- Demonstrates the Can input and/or output of data representing threat/risk concepts in any format

Note that the scope and depth of a mapping is dependent on the domain and domain requirements for information sharing and federation. As such, mappings are expected to fulfill a threat/risk requirement but there is no specific test or subset of concepts required.

2.3 STIX mapping conformance

A STIX mapping implementation may claim conformance provided it is able to:

- Parse STIX data in STIX format and comprehend that data define its semantics in terms of the conceptual model/conceptual reference model, or,
- Produce STIX data from information comprehended with semantics based on the conceptual Model/conceptual reference modelmodel
- Fulfills either canonical model conformance or conformance to another conformant mapping.

2.4 NIEM mapping conformance

A NIEM mapping implementation may claim conformance provided it is able to:

- Parse NIEM data in NIEM format and comprehend that data define its semantics in terms of the conceptual model/conceptual reference model, or,

- Produce NIEM data from information [comprehended-with semantics](#) based on the [conceptual Modelconceptual reference model](#)
- Fulfill either canonical model conformance or conformance to another conformant mapping.

2.5 OWL mapping conformance

[TODO] Reference to section TBD!

← Formatted: Body Text

2.6 Conceptual reference modeling profile conformance

A conceptual reference modeling profile implementation may claim conformance provided it is able to:

- [Read and write UML-XMI that utilizes the conceptual reference modeling profile](#)

3 References

3.1 Normative References

The following normative documents contain provisions which, through references in this text, constitute provisions of this specification. For dated references, subsequent amendments to or revisions of any of these publications do not apply.

The following normative documents contain provisions which, through reference in this text, constitute provisions of this specification. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply.

[UML]	OMG Unified Modeling Language (UML) Superstructure-v2.5 http://www.omg.org/spec/UML/2.5/
[OMG MDA Guide]	http://www.omg.org/cgi-bin/doc?ormsc/14-06-01
[BMM]	http://www.omg.org/spec/BMM/1.3/
[STIX]	https://stix.mitre.org/language/version1.2/index.html
[NIEM]	NIEM-UML 3 Specification [todo – final public link] http://www.omg.org/spec/NIEM-UML/3.0/Beta1
[EDXL]	http://docs.oasis-open.org/emergency/
[SI]	http://www.bipm.org/en/measurement-units/
[CVSS]	https://nvd.nist.gov/cvss.cfm
[CAP]	http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html
[CNSSI 4009]	https://www.cnss.gov/CNSS/issuances/instructions.cfm
[WGS-84]	http://earth-info.nga.mil/GandG/wgs84/
[OGC]	http://www.opengeospatial.org/
[NRC]	http://www.nrc.gov/
[DoDAF 2.0]	http://dodcio.defense.gov/Library/DoDArchitectureFramework.aspx
[ISO 73:2009]	ISO Guide 73:2009 provides the definitions of generic terms related to risk management. http://www.iso.org/iso/catalogue_detail?csnumber=44651
[NIST-SI]	http://physics.nist.gov/cuu/pdf/sp811.pdf

[NIST-UNITS] <http://www.nist.gov/pml/wmd/pubs/upload/AppC-12-hb44-final.pdf>

[NIST-800] <http://csrc.nist.gov/publications/PubsSPs.html>

[QODT] <http://www.qodt.org/>

[BFO] [Basic Formal Ontology](#)

<http://ifomis.uni-saarland.de/bfo/>

[FIBO]

[ISO/IEC
17027:2014]

[NIEM]

This section is being augmented based on references in the models

Formatted: Highlight

Formatted: English (United States), Highlight

3.2 Non-normative References

[DICTIONARY.COM] <http://dictionary.com>

[Firesmith 2003] <https://sites.google.com/a/firesmith.net/donald-firesmith/home/publications/publicationsbyyear/2003/CommonConcepts.pdf>

[SMIF] OMG Document [sysa/2016-12-01 and 02Ap/2016-05-02](#)

4 Terms and Definitions

For the purposes of this specification, the following terms and definitions apply:

Conceptual Model**Conceptual reference model**: A model of the concepts relative to a domain of interest. A **conceptual model****conceptual reference model** models the "real world" or "possible worlds", not data or technology.

Incident: Incidents are dangerous situation that is happening or has happened directly causing harm (detiment) to victims. Kinds of incidents include attacks, disasters, and accidents. Incidents are actualized risks.

Operational: A process or asset that supports the intended functioning of an organization or system.

Operational Risk: Operational risks are situations that may have a negative impact on an organization or company due to uncertainties related to possible breakdowns in a system or its environment via supply chain, injury to a person, or failure of a process resulting from intentional/malicious as well as unintentional/natural operational threats. One of the main impacts of operational risks is inability to conduct operations as planned.

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Operational Threat: Operational threats involve potential incidents or groups of incidents that may cause unwanted loss or harm to people or important assets or groups of assets. These incidents may be caused by threat actors, accidents, or natural phenomena. Examples include terrorist attacks, hurricanes, or an electrical grid failure.

Risk: [CNSSI 4009] Risk is a measure of the extent to which an entity [\[person, organization or system\]](#) is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

System: A system is a collection of parts and relationships among these parts organized to accomplish some purpose. Systems include organizations, governments, people, processes, communities, and information systems.

Threat: Any potential event or act – deliberate or accidental– or natural hazard that may lead to events that cause injury to people or assets, and thereby negatively affect the objectives of stakeholders.

Domain: A specific [sphere-area](#) of concern, activity or [knowledge-knowledge](#). Examples include [healthcare](#), [power distribution systems](#) and [shipping](#).

Cyber: of, relating to, or characteristic of computers, information technology, and virtual reality.

Fact: Facts are something that someone or something asserts to be true. The class of things that can be asserted are called “propositions” as they can be true or false. Once asserted these propositions are facts. [Of course](#) [Of course](#), the relevance, trust or belief in facts is open to interpretation.

Sign: Any symbol or syntactic structure that is used to identify some real or conceived entity or classification of entities.

Formatted: Font: Not Bold

Additional terms are defined in the model, clause [Error! Reference source not found.8](#) and [9](#).

5 Symbols and Notation

There are no symbols defined in this specification. The model specification uses standard UML notation with stereotypes as defined in the UML Profile for SMIF.

Commented [CC1]: Per MHause - add details on notation, particularly that in the generated sections as well as diagram coloring.

The following conventions are used in the UML diagrams:

- Classes that are referenced but not being defined in a section are unshaded whereas classes being defined are shaded.
- Diagrams that define a particular class or relationship will show all features that can be diagrammed. Higher level or summary diagrams may hide certain features, such as subsets or redefines, for readability. Associations are shown where they are relevant to the context being diagrammed.
- Certain stereotypes utilize a specific color for readability, the color is not required to read the diagrams.
 - Blue/grey for data types
 - Black for quantity kinds
- Generic building blocks are presented first, building to threat-risk specific concepts. Some readers may want to browse in the other direction.

Formatted: omg-body, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: omg-body, Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

Formatted: omg-body, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

6 Additional Information

6.1 Acknowledgments

Submitters

- Model Driven Solutions (<http://www.modeldriven.com>)
 - Cory Casanave
- KDM Analytics, Inc. (<http://www.kdmanalytics.com>)
 - Djenana Campara
 - Nick Mansourov
- International Business Machines, Inc. (<http://www.ibm.com>)
 - Bruce Douglass
- RSA, The Security Division of EMC (<http://www.rsa.com>)
 - Chris Hoover
- Lockheed Martin, Inc.
 - Ben Calloni
- Oracle Corporation
 - Pat Sack
 - Mark Tatum

Contributors & Supporters

- U.S. Information Sharing Environment PMO (<http://www.ise.gov>)
 - Kshemendra Paul
 - Vijay Mehra
- Demandware (<http://www.demandware.com/>)
 - Gerald Beuchelt
- U.S. Air Force
 - Harrell Van Norman
 - Kalabhi Patel
- U.S. Defense Security Services
 - Mark Nehmer
- California Public Safety (<http://www.Caloes.ca.gov>)
 - Nicole Meyer-Morse
 - Caroline Thomas Jacobs
- U.S. National Information Sharing Model PMO (<https://www.niem.gov/>)
 - Justin Stekervetz
- U.S. Pension Benefits Guaranty Corporation (<http://pbgc.gov/>)
 - Pamela Wise-Martinez
- Duke Energy

- Stuart Laval
- David Lawrence
- NSA/UCDMO
- NIST
 - Ron Ross
- INCOSE
 - Joe Weiss
- Integrated Networking Technologies, Inc.
 - Patrick Maroney

7 Operational Threat and Risk Guide (Non Normative)

7.1 Mission and purpose

Organizations (commercial, non-for-profit or government) conduct business/mission operations, and consider various threats and risks that may disrupt these operations. Threats and risks are increasingly multi-dimensional in nature – especially those spanning both physical and cyber space. Critical infrastructure protection, counter terrorism, public safety including threats from deadly pathogen, defense, intelligence, economical infrastructure are some key examples of areas of impact. Historically, related communities of interest (COIs) have made significant technical and financial investments if developing processes, policies, systems and formats to respond to threats within their communities. However, the effectiveness of these investments is also limited by the organizational maturity of these communities and the problems get even more pronounced when there is need to share information across these communities. Due to the complexity, connectivity and global nature of threats faced by modern organization, effective risk management and situational awareness depends on collaborations and information sharing. Federating information across multiple communities irrespective of technical and political boundaries will enable us to effectively counter multi-dimensional intentional threats, natural events and system failures.

The operational threat and risk conceptual model includes and integrates concepts from multiple communities and established data formats, focusing on those concepts that are deemed to be of interest *across* these communities or *across* disciplines. This specification defines a conceptual model for threat and risk concepts as well as mappings to augment, and not replace, specific data formats to enable operational threat and risk information sharing, data federation, analytics and simulation. Operational capabilities will be realized by products, projects or technologies that leverage this specification.

The current environment includes There are multiple risk and threat sharing and analytics capabilities in different domains, or communities, supporting different disciplines and using different data schema and technologies. While each of these provides value for its purpose, the community is missing the capability to consider information in context, in combination and with the added value of information from other communities and disciplines. The essential value of information dramatically increases as it is “rubbed together” with other information. What is *not needed* is yet another data structure that intends to be the one ring that binds them all. What *is needed* is the capability to federate and translate between different data structures, technologies, terminologies and human languages relating to risks and threats.

To meet these goals, we seek to define the semantics of ‘building blocks’ of general threat and risk concepts, leading to the semantics of threat and risk information sharing. It is the goal of the community forming around this standard to then build capabilities that are able to can leverage these models to provide advanced analytics, intelligent simulation, and dynamic information sharing.

While this specification is international in scope, statements at the highest levels of the U.S. government are informative. As stated in the recent executive order¹ of the President of the United States:

In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

The threat and risk specification provides the fundamental semantic underpinnings of this capability. It does so based on open standards, which are also specifically asked for in the executive order.

¹ <http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>

7.2 Technology capabilities

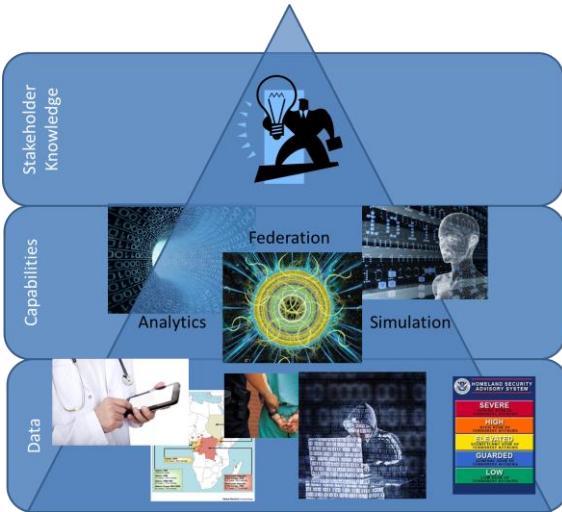
The technology capabilities that can leverage the threat and risk model are limited only to the imagination, creativity, and initiative of the community. The following represent a few ideas and examples related to possible capabilities that are envisioned that may frequently be combined in systems, tools, or products. Such tools and products are an essential part of building the capabilities and communities to achieve the impact envisioned in this specification and specified in section 7.

7.2.1 Federated analytics and simulation capabilities

Federated analytics and simulation ~~is-are~~ intended to pull information from multiple unrelated sources *and make sense of them together*. This includes “connecting the dots” use cases, fusion centers², enterprise threat management, etc. The essential goal is stakeholder knowledge, and intelligence derived from putting facts together. This includes (but is not limited to) products such as:

- Data federators and hubs
- Analytics tools
- Simulators
- Entity extraction
- Integrated threat management
- Federated query and graph databases

² Fusion centers operate as focal points for the receipt, analysis, gathering and sharing of threat related information.



Formatted: omg-body, Left

Figure 2 Federating Capabilities

The picture above illustrates the federation capability – multiple sources and forms of data are fed into a threat/risk based federation engine (an implementation of this specification). [The federation engine](#)[An implementation of this specification](#) will use the [conceptual model](#)[conceptual reference model](#) and mappings to unify the “facts” across these sources into a common semantic framework. Simulation and analytics tools can then leverage this federated information – present it in ways that are meaningful to a particular stakeholder as well as automate inferences across the federation to discover or suggest new information, not derivable from any one source.

7.2.2 Information Translating, Analytics, and Sharing capabilities

Information sharing capabilities focus on providing independent stakeholders with the ability to safely collaborate by exchanging information and services. In information sharing scenarios, data is “pumped in” from one or more data sources and translated to the vocabulary, structure, and data format of a data consumer. The [conceptual model](#)[conceptual reference model](#) provides the “pivot point” between the provider and consumer. Fundamental to this use case is the assumption that the data formats on either end are independently conceived and one will not be changed to the other. This also assumes that there is no one single format that everyone agrees to – an assumption that has proven true over and over. In the middle is the pivoting technology which does the semantic transforms. Technology capabilities in this family include but are not limited to:

- Data hubs

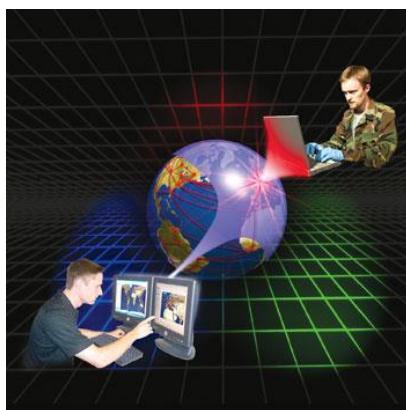


Figure 3 Information Sharing

- Publish/subscribe engines
- “Smart” enterprise service buses
- Secure endpoints with translation capability
- Model driven integration platforms
- Translators



The picture above illustrates independent information providers and consumers collaborating worldwide, with something in the middle (or on one side) that provides for the semantic translation of the data.

Translators are nothing new –Saint Jerome (4th Century) is considered the patron saint of translators and encyclopedists. The United Nations uses translators – human translators that understand how to express concepts in multiple languages. Likewise, an automated translator needs to understand how to express concepts in multiple languages – which means an understanding of both the concepts and how the languages express those concepts.

7.2.3 Risk Analytics Capabilities

Risk analytics capabilities enable an enterprise or government entity to identify, analyze, and evaluate its risks. Identification, analysis and evaluation of threats and risks and the corresponding vulnerabilities are required to understand and measure the impact of the risk involved and hence to decide on the appropriate measures and controls to manage them. The process of risk identification has to be systematic and comprehensive enough to ensure that no risk is unwittingly excluded. Having identified and evaluated the risks, the next step involves the identification of alternative appropriate actions for managing these risks, including:

Avoiding the risk by deciding to stop, postpone, cancel, divert or continue with an activity that may be the cause for that risk.

Sharing the risk with other parties facing the same risk (insurance arrangements and organizational structures such as partnerships and joint ventures can be used to spread responsibility and liability).

- Reducing the likelihood of risk.
- Reducing the impact of risk.
- Accepting the risk.

Collaboration and information sharing is an essential part of the risk analytics capability. Information about attacks, incidents and other undesired events involving ~~the-a~~ system or similar systems can be turned into sharable content and used to prevent similar incidents in the future. Such shareable content may include risk indicators, patterns, and effective courses of actions. Risk assessment process (indicated as #3 in the picture below) can be made efficient by importing the sharable content and using it to analyze the system at hand. ~~This will result in more efficient risk treatment actions – indicated as #4. The sharable content becomes an important part of the risk mitigation argument for the system at hand.~~

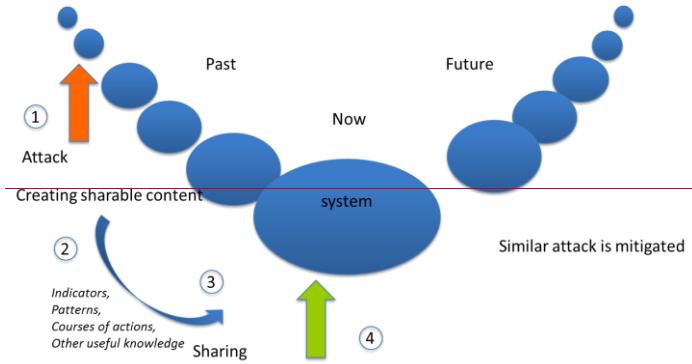


Figure 4. System in context of risk

Approaches [Evaluation of Alternatives to Federation](#) and [Integration](#)

Translating and federating can be done at different levels, broadly syntactic, canonical formats and semantic. The following section discusses the options and the justification for the [conceptual model](#)[conceptual reference model](#) approach.

7.2.4 Syntactic Federation and Translation

Most “data translator technologies” (e.g., XSLT) operate at the syntactic level. That is a specific syntax for some “fact” is recognized in a specific technical representation (e.g., a particular XML syntax and schema) and then converted to another specific syntax and schema (e.g., RDF using another schema) using a program of some sort. Such translators are inherently one-one, each format must be correctly interpreted and code written to translate to another format (which also must be correctly interpreted). Where there are specific systems to integrate or very well-defined and stable standards that fully cover all needs, this approach can be effective.

Where syntactic translation falls down is in any of the following scenarios:

- There are several different systems or organizations—each with their own formats and vocabularies.
- The meaning behind or details of the formats is fuzzy, leading to translation errors.
- Meaning is “hidden” behind non-standard or unrevealed encodings.
- There is change in any of the endpoints, requiring change in all others.
- Standards exist, but they are used inconsistently or missing needed capabilities.
- There is a need to federate or translate new information quickly and inexpensively.

Of course, these issues are common. Syntactic translation just does not scale to our federated dynamic and interconnected world.

Formatted: omg-body, Left, Don't keep with next

Formatted: omg-body, Left

Commented [CC2]: Consider redoing this section

7.2.5 Canonical data formats

Canonical data formats define a “one size fits all” data format (E.g., STIX or NIEM) as a de facto or de jure standard. Syntactic mapping is then used to translate data from another format (perhaps proprietary) into and out of the canonical format. Canonical formats attempt to remove the one-one limitations of direct mappings with mappings “through” the intermediate format. Canonical data formats work well when there is a well-defined community with strong leadership that can enforce the standard. Canonical formats have issues under the following conditions:

- Where different stakeholders have needs the canonical format can't handle—extensions are made that the community then does not understand. Extension mechanisms tend to be either missing or complex.
- Related communities need to share information but have not or cannot “buy in” to the others' standards.
- These formats tend to be locked to and very influenced by a specific technology, and the meanings get lost in the bits and bytes and potentially outmoded.
- It becomes very hard to change the technology to take advantage of new capabilities.
- It becomes hard to adapt to change the business needs.
- It can be time consuming, expensive and risky to implement adapters to and from the canonical format.
- The semantics of the format (on either end) are frequently ill-defined and translation errors or unintended data loss is frequent.
- It can be inefficient to go through an intermediate data format.

Canonical formats and standards have provided great value in specific communities, but as we expand across domains, disciplines, organizations, countries, and human languages they tend to show their limitations.

7.2.6 7.2.4 Semantic federation and translation/integration

The A semantic information federation approach is the one leveraged in this specification. A semantic approach focuses on concepts and their meaning, not how they are represented in any particular schema, syntax, vocabulary, or technology. Mappings then define how various data formats and vocabularies *represent* those concepts. Concepts are well defined in a conceptual modelconceptual reference model – a more precise way to define a vocabulary or taxonomy. Conceptual reference models may be called “ontologies”, or “abstract data models” but some ontologies or abstract data models are essentially programs and not conceptual.

The essential difference between a conceptual reference model and any of the syntactic forms abovea concrete application model is that it describes the real world things and their relationships as understood by stakeholders. It is a *model of the world*³, not a model of data or a system. When we have a concept like “Incident” in our model, “instances” of incidents are real things that happen – not a Java object or stream of XML. However, we may also have concepts of actual things, such as a specific incident.

³ Or more generally, real or possible worlds.

- A conceptual reference model is conceptual in that it is an expression and formalization of how a community conceives of their domain, problem area, business or environment. It is not a model of the solution or a technology.
- A conceptual reference model is a reference model in that it is intended to supply reference concepts for what information in various systems means, to “connect the dots” between application models. It is not intended as a concrete application or solution model in and of itself.

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

These real-world reference concepts are the pivot points between different ways to name, describe or talk about them the things we deal with every day. This “world of things” is what we understand – of course there can be many names for and descriptions of the same thing.

For example, we could have different ways to name the Eiffel tower or Colosseum – but they name the same thing.

Formatted: omg-body, Don't keep with next

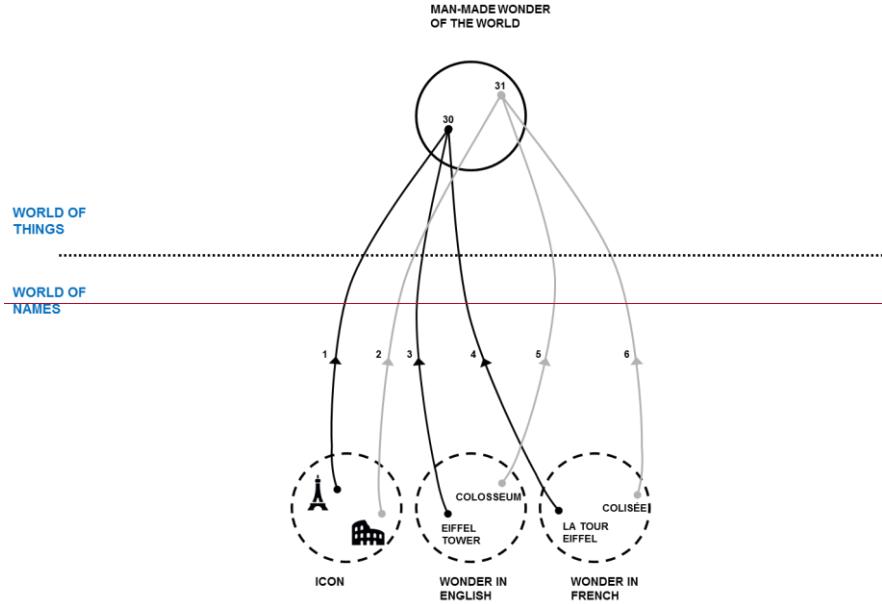


Figure 5. the World vs. Names

How do we know it's the same thing? IWhile in some cases we can describe something so precisely and mathematically that we can be sure, in many cases it is just a shared concept based on a definition and how that concept relates to other concepts. We allow for both precise and pragmatic definition of things.

In threat-risk scenarios we also have to be fully aware of how much we trust various information sources. It is common, if not the general rule, that different information sources will have conflicting information about the same things. How do we know what to trust? This specification provides the basis for trust, in capturing the provenance of information, but it leaves the evaluation of trust to the capabilities that utilize or analyze the information – or to the stakeholders who must make decisions based on it. This is a common pattern in this approach, providing the basis for decisions but not the specifics for how to make those choices.

A conceptual reference model has some similarities to a canonical data format in that it attempts to capture cross-stakeholder information needs – but it abstracts above the data format, technology, terminology and even the specific use case and structure for that information.

The conceptual approach has the following advantages:

- Conceptual models are very resilient to technology change, and mappings to new technologies can be added at any time.
- Conceptual models are more resilient to change in business needs, since the business vocabulary tends to have more stability – even when requirements change.
- Conceptual models provide unified pivot points that turn 1:1 mappings into 1:n mappings.
- Conceptual models can be very precise, with the semantics clear. This reduces the risk of translation errors.
- “Smart” technologies and rule engines can leverage the model semantics in multiple ways, providing advanced analytics and inference.
- Using Model Driven Architecture (MDA), conceptual models can be “provisioned” to an implementation technology or exchange format automatically, based on injecting the technology choices.
- Once the conceptual model foundation and supporting capabilities are in place, it is easy to add additional federation and translation capabilities.
- Conceptual models can be used to federate existing point and/or canonical data structures.

Formatted: omg-body, No bullets or numbering

Costs and concerns of a conceptual approach are:

- It is hard to start from scratch, as concepts tend to build on other concepts. Our mitigation of this issue is to provide such a foundation in this specification.
- The concepts of a domain are not always clear; it takes work to derive the conceptual model. Again, it is the intent of this specification to provide threat and risk concepts – ready to be leveraged.
- Conceptual technologies are less mature than syntactic ones. Our expectation is that expertise, tools, and technology development will be encouraged by having a standard.
- By reducing the time and cost for federation and integration, programmer jobs could be lost. Of course we hope there is better use for their time – perhaps leveraging the federated and shared data.
- Not everyone will agree on common definitions or models. There is no need for or expectation of universal agreement. There can be multiple conceptual models (even for the same data structures) and they can sometimes be used together by expressing mappings between them. Terminology differences can be integrated into the same model. As long as a conceptual model is useful for some universe of data, it has value. We hope this specification has such value within the threat and risk community.

Use of the Unified Modeling Language (UML)

UML is a standard for modeling with wide industry acceptance, multiple implementations, and supporting resources. UML has a heritage of being defined and used for “object modeling” at a level that is closer to implementing software systems than capturing concepts. UML has broadened and also addresses concerns such as processes, systems engineering, and others. In this specification UML is used as a conceptual modeling language. To use UML as a

conceptual modeling language certain extensions are made to UML using the built in extension mechanisms. These extensions are described in the Mapping Profile (section 12.7) as well as the in-process [SMIF] submission for this purpose.

7.3 Defining and Leveraging ~~Conceptual Model~~^{Conceptual reference models}

This section is intended to introduce the approach taken to express the risk and threat ~~conceptual model~~^{conceptual reference models} and how the concepts are layered, modularized and organized.

7.3.1 Expressing ~~conceptual model~~^{conceptual reference models}

As stated in [7.2.47.4.3](#), ~~conceptual model~~^{conceptual reference models} are models of the world – or at least how communities conceive ~~it~~^{of the world}. This is differentiated from models of data (e.g., an E/R model or XML Schema) or models of software (e.g., a Java program). In their pure definition, *Ontologies*⁴ are ~~conceptual model~~^{conceptual models}, however not all ontologies or ontology languages are conceptual ~~and many are intended for building semantic applications using specific “reasoning engines”, not as reference models. Ontology languages are typically optimized and restricted for their intended class of reasoning engine, not to capture domain concepts in general.~~

Of course, human natural languages are the most common way to express concepts. [Natural language is used in the definition of our concepts but those definitions are augmented with more formal assertions.](#)

There can be confusion between the language used to express a model and what it models. For example, while Entity-Relational (E/R) was designed for SQL data models it can be used conceptually. At the other end of the spectrum many ontology languages have been used to express data models or to support specific forms of inference based computation. *The language does not make a model conceptual* (or an ontology or a data model), *what is being modeled does*. Of course some languages are better than others for ~~conceptual model~~^{conceptual reference modeling and mapping} ~~than others, [SMIF] is used because it is designed for expressing conceptual reference models and mappings to various forms of data.~~⁷

Our goal in this specification is to utilize a [set of ~~conceptual model~~^{conceptual reference models}](#) as the pivot point between different data models and syntaxes for expressing information about real-world threats and risks. While using a ~~conceptual model~~^{conceptual reference model} in this way is not new, there has not been a well-accepted standard for doing so. None of the well accepted modeling languages are specifically designed for ~~conceptual model~~^{conceptual reference modeling and mapping} – most are designed for software modeling (data, procedural computation, or inference).

The Unified Modeling Language (UML) was originally designed for modeling object-oriented software, but is also used for other purposes and is easily extended with *profiles*. We are using a profile of UML based on [a standard in progress – Semantic Modeling for Information Federation \(SMIF\)](#). UML is a well-accepted modeling language with widely available resources – SMIF provides a standard way to use UML ([and other languages](#)) for the purpose of ~~conceptual model~~^{conceptual reference modeling and mapping}. The combination of UML and the SMIF profile provides an expressive, [well supported and automatable](#) way to express the ~~conceptual model~~^{conceptual reference models} and mappings. [The SMIF profile is included in this specification as a non-normative appendix and therefore does not depend on SMIF being standardized](#). Any standard conformant UML tool can import and manage the profile and the ~~conceptual model~~^{conceptual reference model} but special tooling is required to automate mappings.⁷

The intent of the ~~conceptual model~~^{conceptual reference model} and mappings is that a tool or infrastructure developer can take that model and interpret it and transform it as appropriate for their own technology stack and data formats. They may then use that technology stack to implement the information sharing and federation capabilities described conceptually. However, *this specification makes no assumption about what that implementing technology stack may be or how it is*

⁴ *Ontology*: 1 : a branch of metaphysics concerned with the nature and relations of being. 2 : a particular theory about the nature of being or the kinds of things that have existence. [www.merriam-webster.com]. However, ontologies have become associated with a particular branch of formal languages such as OWL and Common Logic that support logical inference.

implemented. In addition, this specification makes *no assumption about a new “intermediate data format”* based on the conceptual model~~conceptual reference model~~- the conceptual model~~conceptual reference model~~ has no normative data | format – it maps to multiple possible data formats that already exist. Keeping the “middle” conceptual and virtual is a way to help resolve the “data format wars” that plague many attempts to federate where yet another data format may be unwelcome.

Mapped data formats must, of course, be used in any implementation – ultimately you need an explicit data (or language) syntax to communicate and process data. Each of the mapped data formats such as STIX or NIEM may be used to express threat & risk data within their domains. There is also growing interest in the “Semantic Web⁵” which uses the “Resource Description Framework Schema” (RDFS) language as well as the “Web Ontology Language” (OWL) or the Simple Knowledge Organization System (SKOS) to describe the web of data on the internet. The semantic web technologies are well suited to data federation. The conceptual model~~conceptual reference model~~ can be mapped to semantic web technologies generated from the conceptual model~~operational threat and risk (OTR) conceptual reference model, using-based on~~ the SMIF specification. Conceive

Formatted: English (United States)

⁵ The term “Semantic Web” refers to W3C’s vision of the Web of linked data. Semantic Web technologies enable people to create data stores on the Web, build vocabularies, and write rules for handling data. Linked data are empowered by technologies such as RDF, SPARQL, OWL, and SKOS. [<http://www.w3.org/standards/semanticweb/>]

7.3.2 Pivoting through conceptual reference models

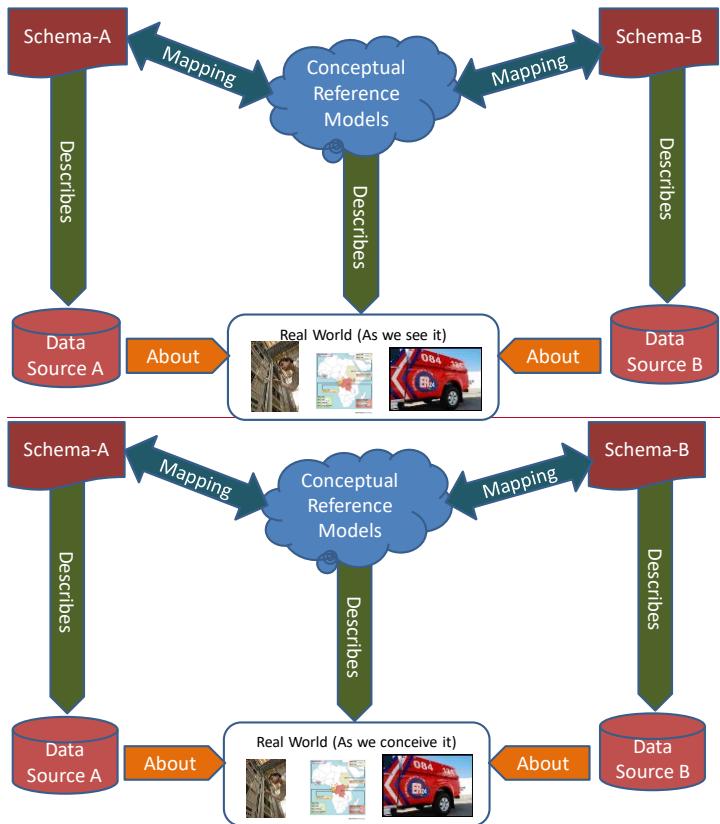


Figure 45 Illustration of pivoting through a conceptual reference model

The illustration above shows how conceptual reference models provide the “pivot point” between different schema for various data sources. The conceptual reference model describes the world (or a possible world) as we conceive it. Schema describe data, that data is about the same “real world”. Where schema elements are mapped to the same concepts their data can also be mapped or federated. Any number of schema (or other data descriptions) can pivot through the same concepts and thus provide for mappings between any combination of data sources.

7.3.3 Mapping to information and data models

Conceptual reference models are not intended to define data schema for specific applications, but to define the semantics behind those schema by mapping them to concepts. Each data schema to be mapped is imported into a model and a “[mapping model](#)” defines how the data structures in a concrete schema represent the common reference concepts. Only those concepts that need be shared or federated with other data schema need be mapped. An implementation of this specification is then able to map between and federate information in these different schema.

← Formatted: omg-body

Formatted: Font: Bold

7.3.37.3.4 Layering

Commented [CC3]: Put actual layer doc in separate document

Formatted: Normal

The conceptual model/conceptual reference model is actually multiple models, combined. Those models are layered and modularized. In that many of the concepts required for understanding threats and risk ([building blocks](#)) are more generic ([building than blocks](#)) than threats and risks, a framework of generic concepts is defined in a modular form separated into packages. These generic concepts are then used and specialized for the risk and threat domain. This layering makes it more practical to integrate threats and risks with related viewpoints and concerns, such as enterprise resource planning, law enforcement, software development or transportation. [Since the "edges" of threat and risk management are very fuzzy and information from other domains needs to be able to be integrated to "connect the dots". this layering provides for the needed integration points across diverse data sources.](#) The same layering [may](#) supports reuse of these more general concepts for other conceptual models;domains.



Figure 56 Conceptual Model/Conceptual reference model Layering

The above illustration shows the layering of the conceptual model/conceptual reference models.

- **Foundational Concepts:** The foundational concept library defines basic constructs for conceptual model/conceptual reference modeling such as ideas of entities, roles, types, and identifiers. [Any model is expected to use these concepts.—These very general concepts are defined in the SMIF specification and used as a foundation for OTR.](#)
- **Generic Concepts:** The generic library is a set of modules focused on a specific core concepts and other closely related concepts. More specific concepts can pick and choose what they need out of the concept library. Examples include “Person,” “Organization,” “Control,” “Location,” etc. Many library concepts are derived from NIEM and other sources,[but abstracted to their more general concept.](#)
- **Threat and Risk Specific Concepts:** These are the cross-cutting concepts within the threat-risk domain. These are also defined in focused modules such as “Risk”, “Incident”, or “Vulnerability.” These cross-cutting concepts form the basis of the threat/risk specific framework.

[Note that evolution of the conceptual modeling approach may allow for the foundational and generic concepts to be moved into their own specifications such that only the threat and risk specific concepts would be required to be included in a future version of this specification. However, at this time there are insufficient foundational and generic conceptual model standards for such reuse.](#)

7.3.47.3.5 Source of concepts

Multiple inputs have been considered in bringing together the conceptual model conceptual reference model. Primary inputs include:

Threat and risk specific sources

- NIEM
- STIX
- NIST 800 Series
- ISO 8000 and NIST Units
- EDXL
- [Firesmith Safety Model](#)
- Common Vulnerability Enumerations

Generic concepts

- ISO Specifications: 11179, 1087, 704, 11354, 18876, 24707
- [Dolce upper ontology](#)
- [OMG Unified Modeling Language](#)
- [Web Ontology Language](#)
- [OMG Date & Time Specification](#)
- [OMG Financial Business Ontology \(FIBO\)](#)
- [OMG Unified Modeling Framework \(UAF\)](#)
-

Due to the multiple inputs, none match exactly. Every effort has been made to retain the semantics of the concepts and synthesize them [together in an understandable way](#).

Top Level Concepts

Operational threat and risk builds on some of the “top level” concepts as defined in the SMIF specification. Concepts such as entities, situations and patterns are common and can be reused. SMIF also defines language specific concepts that may not be needed for threat and risk, but may be used to extend the OTR model for more specific purposes. Readers are encouraged to see the introduction to SMIF concepts for this foundation.

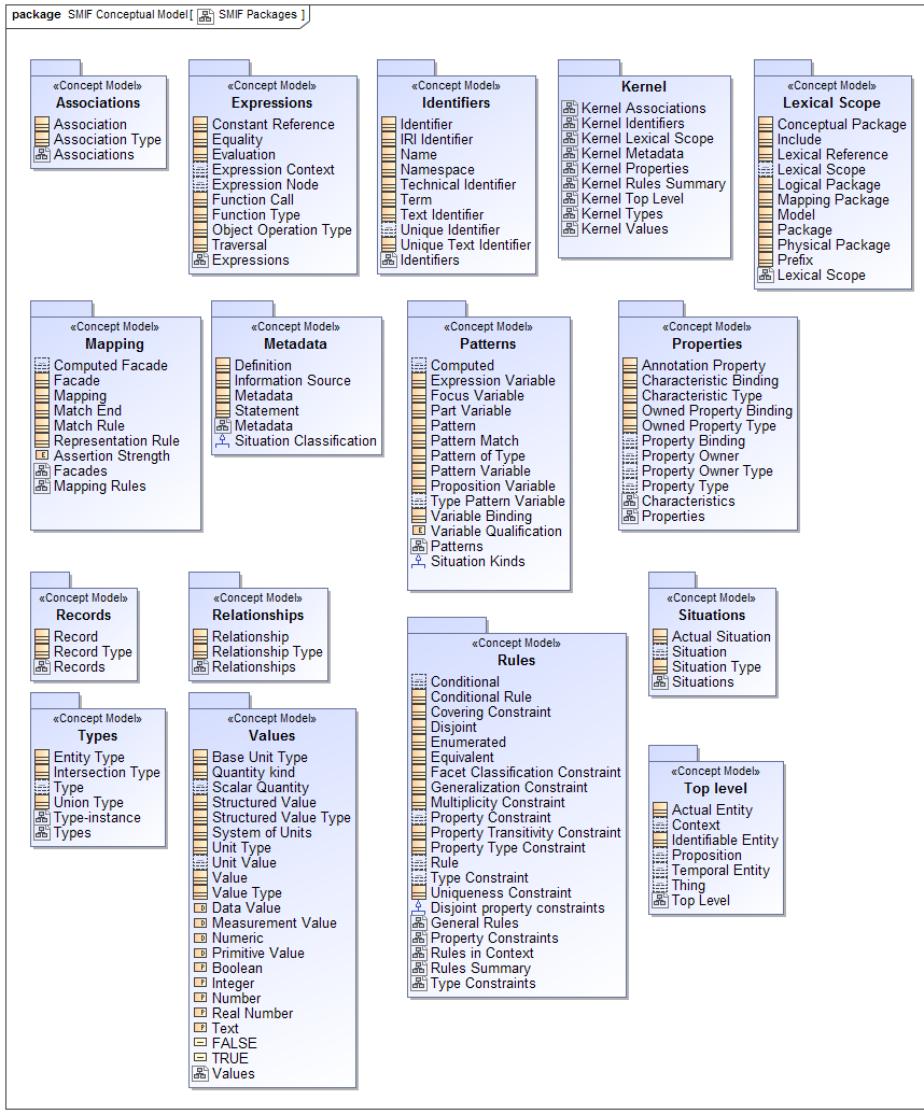


Figure 6 Concepts define in SMIF

Formatted: Caption

Building on the top-level concepts in SMIF is a library of general concepts that are needed for threat and risk information but not specific to it, this includes people, places and things. The general concept library is included as a separate section..

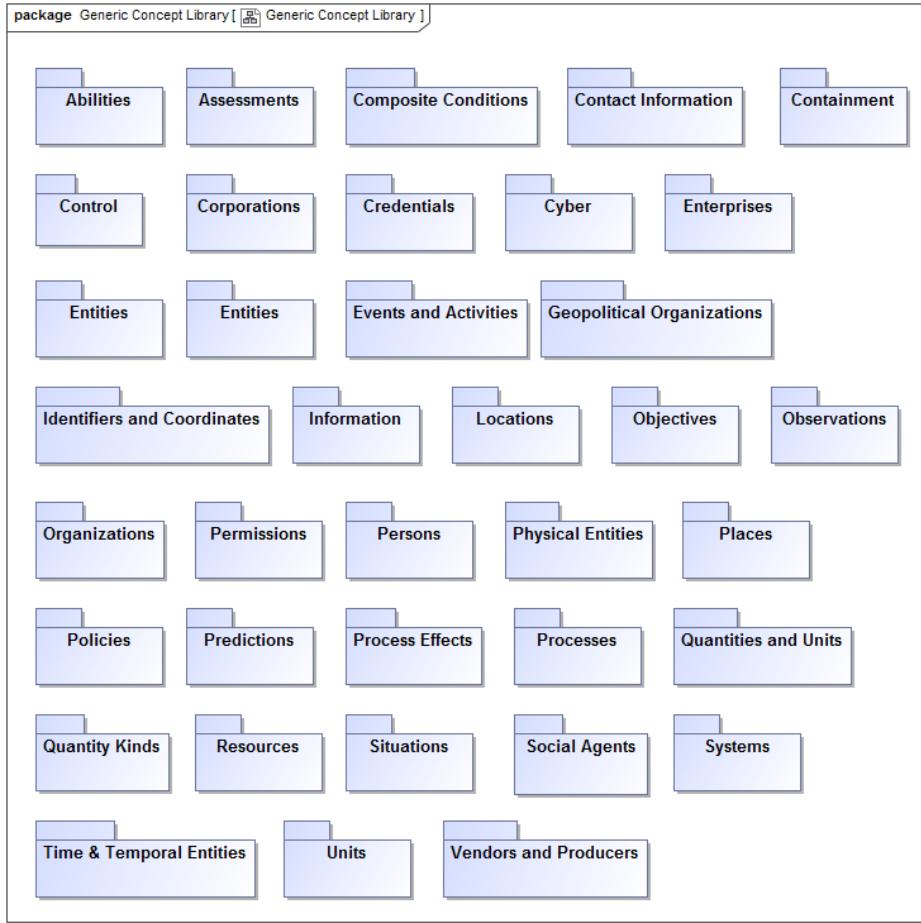


Figure 7 Generic Concept Library

Formatted: Caption

The packages defined in the concept library is shown above and documented in the appendix.

Threat and risk specific concepts then use and combine these general concepts for information sharing across domains that supports threat information sharing and risk analytics.

7.4 Modeling Style

Formatted: Heading 2,Title 2

There are two primary kinds of concepts defined in threat and risk – classes representing entities and relationships representing “connections” between entities. Each relationship concept defines what other concepts it relates to (which can be entity or relationship concepts). [When a concept is defined in a conceptual reference model they are defined as](#)

they are most generally understood, not how they may be used in a specific application context, this avoids redundancy and stovepiped models. All concepts can be organized into hierarchies. These hierarchies result in some “top level” concepts and more specialized and specific concepts.

We are used to hierarchies of entity concepts; e.g. an oak tree is a kind of tree, a tree is a kind of plant, etc. We also frequently see hierarchies of relationship concepts: e.g. ownership is a kind of control.

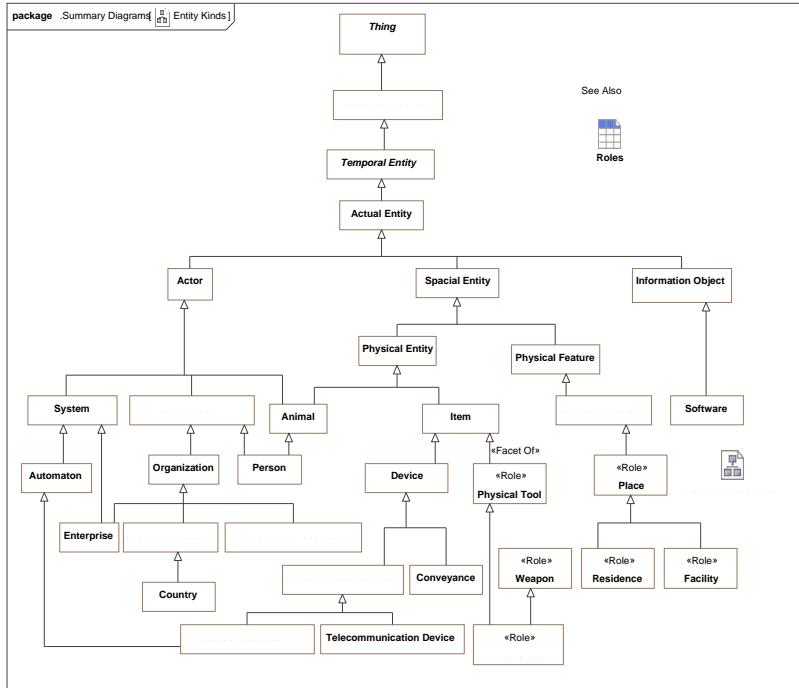


Figure 8 Example Entity Hierarchy

When a relationship concept (UML association) is defined in a conceptual model, concepts should be defined as they are most generally understood, not how they may be used in a specific context, this avoids redundancy and stovepiped models. It is possible to form hierarchies of concepts where it makes sense. So when a very general relationship concept (Shown as a UML Association Class) is being defined we connect it to the most general entity concept (Shown as a UML Class) which may be involved in that relationship. Such entity classes are frequently more general than the specific problem being solved at the moment. Many concepts important to threat and risk are of this more general nature. For example, that one situation may happen before another is important for threat management but also makes sense across domains – it is a general concept. Since “something happening after something else” is a general concept, the classes it relates are general concepts as well – a situation may happen before or after another situation. Properly representing these general concepts naturally introduces a hierarchy of other general concepts as are found in the generic concept library.

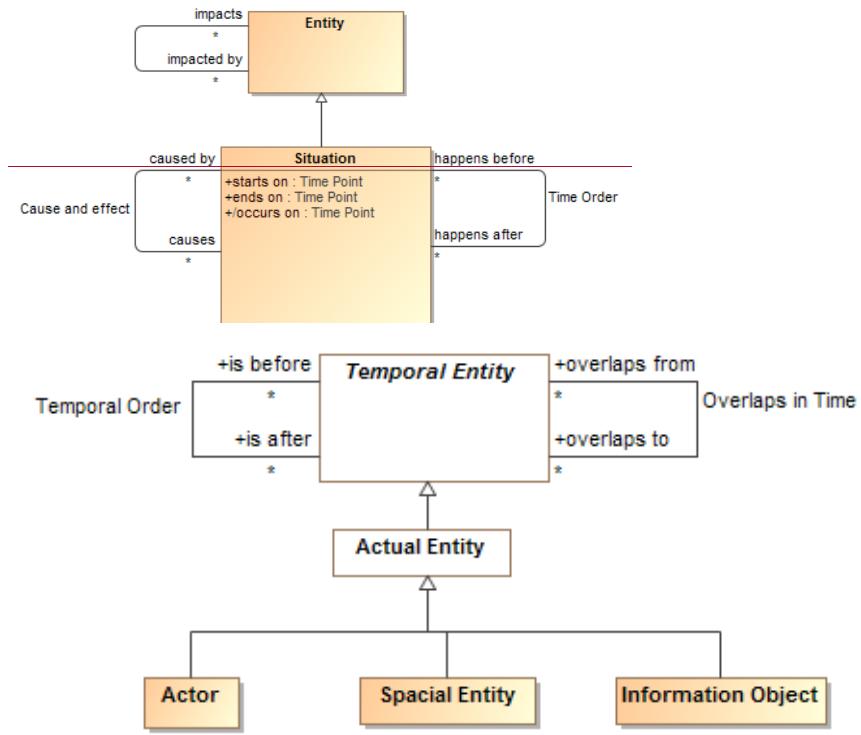


Figure 97. Example of Top Level Classes

The above example shows some of the top level classes **concepts** and the **associations** between them. These associations include the concepts that any situation may happen before or after any other situation or be caused by or cause another. It also shows that situations may have some impact on an entity – of course what that impact is will be more specific. Having these general relations both grounds more specific concepts and reduces the necessity for every class to have relations to every other class – as is frequently seen when there are no top level classes.

Each of these more general concepts may be specialized for more specific purposes, and many have been specialized for use within threat and risk. In many cases threat and risk specific terms are introduced as more specific terms for a general concept.

Formatted: omg-body, Left

Commented [CC4]: MHasue: Suggest making association classes.

Commented [CC5R4]: All classes are now association classe

The top level hierarchy

When such generic concepts are factored together a hierarchy emerges as can be seen below:

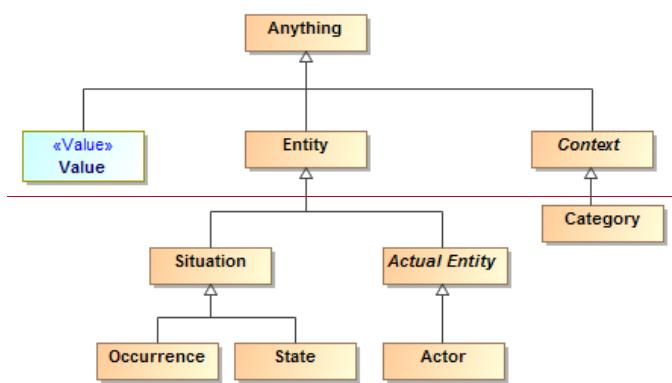


Figure 8. Top Level Classes

The figure above depicts some of the top level classes from which all other classes in the threat/risk model ultimately specialize. These are more thoroughly documented in 8.1, but are summarized here as an introduction. Each of these top-level classes has relations to other classes that are reused and specialized in other parts of the model. Some of the top-level concepts include:

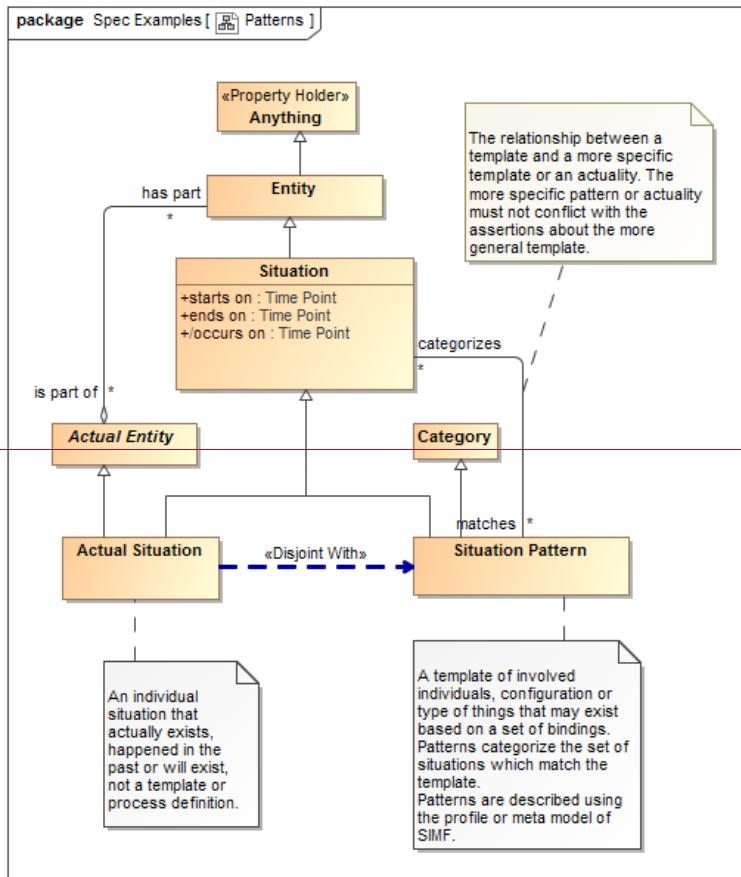
- **Anything**—the class that represents all things representable in models or as data.
- **Value**—values are text, quantities and other atomic data that do not change over time (E.g., the number 5 “just is”)—differentiated from entities. Values may be used as the types of properties.
- **Entity**—entities are any concept of a thing with a lifetime that may change over time—differentiated from values. Note that lifetimes may be very long or very short.
- **Situation**—situations are “configurations” of things or relations between things over a period of time. A situation could be as small as your weight at this moment or as large as the solar system. Subtypes of situations are occurrences (situations of things changing over time in some kind of process or event—e.g., running) and States (situations that are static for a period of time—e.g., the things on your desk right now).
- **Context**—a grouping of concepts contextualized in some way and with some common attributes facts and/or relations. Rules defined for a context are true for anything contextualized by that context. Note that anything may play the role of a context.
- **Category**—a category is any conception of how things may be grouped, typed, or segregated from other things. This includes types and taxonomies.

- **Actual Entity** — anything with individual identity and lifetime that is distinguished from others — this includes people, places, things, agreements, etc.
- **Actor** — anything that can take an active role in a process or behavior.

The full foundational model includes subtypes of the above, see the core concept library (8.1) for more detail. When reviewing more threat/risk specific concepts it should be recognized that properties and relations of a concepts supertype are part of that concepts definition.

← **Formatted:** omg-body

Templates and actual situations



Formatted: omg-body, Left

Figure 9. Situation Patterns

Fundamental concepts in the conceptual model/conceptual reference model are those of patterns and actual situations. An actual situation is something that is “real”, it has no variables and describes a particular situation or incident – like a specific laptop being stolen. A pattern is a template describing a set of situations based on that pattern. So a pattern could be the general pattern of theft – when that happens, what is stolen, etc. are “variables” of that pattern.

Formatted: omg-body

While patterns and actual situations are quite different, what can be said about them is very similar. While a pattern has variables it also has some constants – the things that are the same across all the actual situations that describe it.

An actual situation can describe its relationship to a pattern by “binding” the roles something plays in those situations or binding real people, places, things and values to the variables. For example, in an actual situation “A stolen laptop” may be bound to a specific laptop—Model xyz owned by Joe Smith. That specific laptop actuality (what actually happened) then matches the stolen laptop pattern.

~~Both actual situations and patterns are considered situations—so situations may be specific or general, real or possible.~~

Next level of the hierarchy

With the top-level concepts in place, we have the basis for a hierarchy of entities. This diagram shows more of the entities where more concrete concepts are introduced:

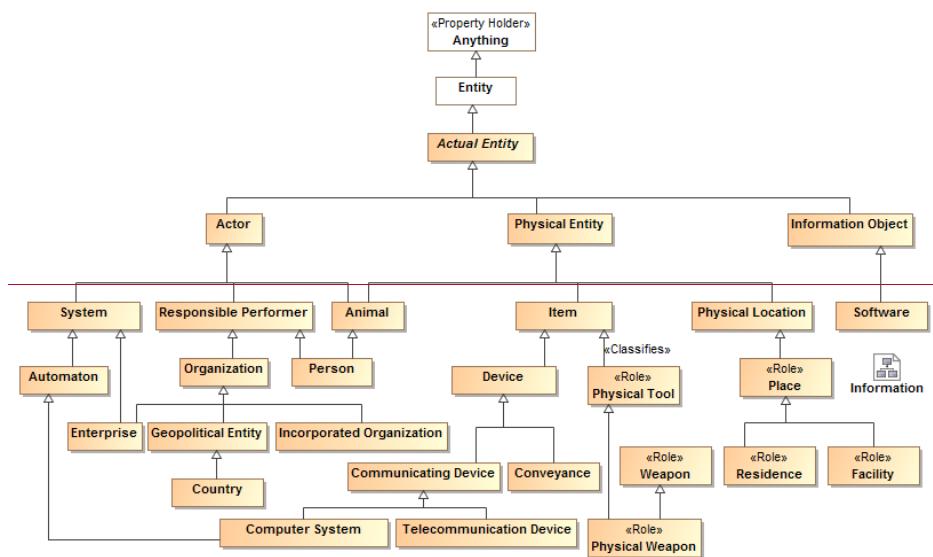


Figure 10. Entity Hierarchy

Note that many data models (such as NIEM) will start defining classes further down the hierarchy, such as with “Person” or “Item.”

Narrowing general concepts

For a particular use or data structure such general concepts will usually be narrowed. The mapping relations show how general concepts are mapped to more specific or restricted concepts in specific data structures. Specific structures may also ignore and not include concepts that are not important for their specific purpose—defining a concept in the conceptual model/conceptual reference model does not imply that it is or must be included in any particular data structure. This is one of the key ingredients to mapping across different structures and domains.

Formatted: omg-body, Left

Formatted: omg-body

7.47.4.1 Mixing Concepts with “multiple classification”

Formatted: Heading 3,Title 3

The [conceptual model](#) provides a way to classify and organize things, activities and relationships – a common idea in everyday life. Software professionals are used to “class hierarchies” in languages like Java and C# where a particular “object” is an “instance” of [a particular exactly one](#) class. In most software languages such an object can only be a member of one class and that class [is fixed](#) for the life of the object.

In the “real world” there are many ways to classify and consider something and those classifications can be contextual or change over time. The same individual can be a person, a citizen, an employee and an adult. At other times the same individual may be a child and a dependent. An attack on a facility may be considered an invasion [by](#) some and a defensive action by someone else.

Another primary use-case is “roles”. A role is a behavior, capability or responsibility that something “takes on”. For example, a person may assume the role of a police officer. Roles are frequently transient – they change over the lifetime of something or may even depend on the context in which it is considered. Another feature of roles is that they can [also](#) be combined, so that [an individual](#) police officer could also be in the role of a victim in [some an](#) incident [or the wife in a marriage](#).

The threat/risk [conceptual model](#) is about the real world, or world conditions we can conceive of. For this reason, the classifications defined in the [conceptual model](#) may be “mixed together” as required to define a particular thing, event or relationship. The technical term for this is “multiple classification”, however for most people it is just the normal way to describe something. Allowing for multiple classification makes the [conceptual model](#) simpler and more flexible.

There are times when it just doesn’t make sense for two or more [classifications classes](#) to be combined. E.g. something can’t be a truck and an incident, it just doesn’t make sense. For these cases such classes are marked as “disjoint” using either a UML dependency [as defined in SMIF](#) or generalization set.

Implementations of the threat/risk model must consider the multiple classification capability for which there are well known patterns to support it in various computer languages and data schema. When looking at the [conceptual model](#) don’t make the mistake of assuming that something can only be classified by just one class at a time.

8 Operational Threat and Risk Model Reference

8.1 Threat-risk-conceptual-model::Threat and Risk Specific Concepts

The risk and threat modules use and specialize more generic concepts to build the risk and threat information sharing and analytics framework.

All risks and threats involve an undesirable situation that is a real or possible situation with consequences that do harm | and impact the objectives of stakeholders. The same situation may, of course, not be considered a risk or threat to other stakeholders - some may consider such a situation an objective.

Formatted: Emphasis

This foundational information is then expanded with metrics and interrelationships such that threats and risks can be fully understood and dealt with. This includes chains of causation and dependency – such chains are frequently the point of attack that results in downstream harm.

Fundamental risk/threat specific concepts include:

- [Danger](#)
- [Risk](#)
- [Incident](#)
- [Indicator](#)
- [Vulnerability](#)

Note that these concepts use and build on more generic concepts that are not risk/threat specific such as "person", "organization", and "Intent".

All undesirable situations derived from the general concept of a "situation"; which is fundamental to this specification.

8.1.1 Diagram: Threat and Risk Specific Concepts

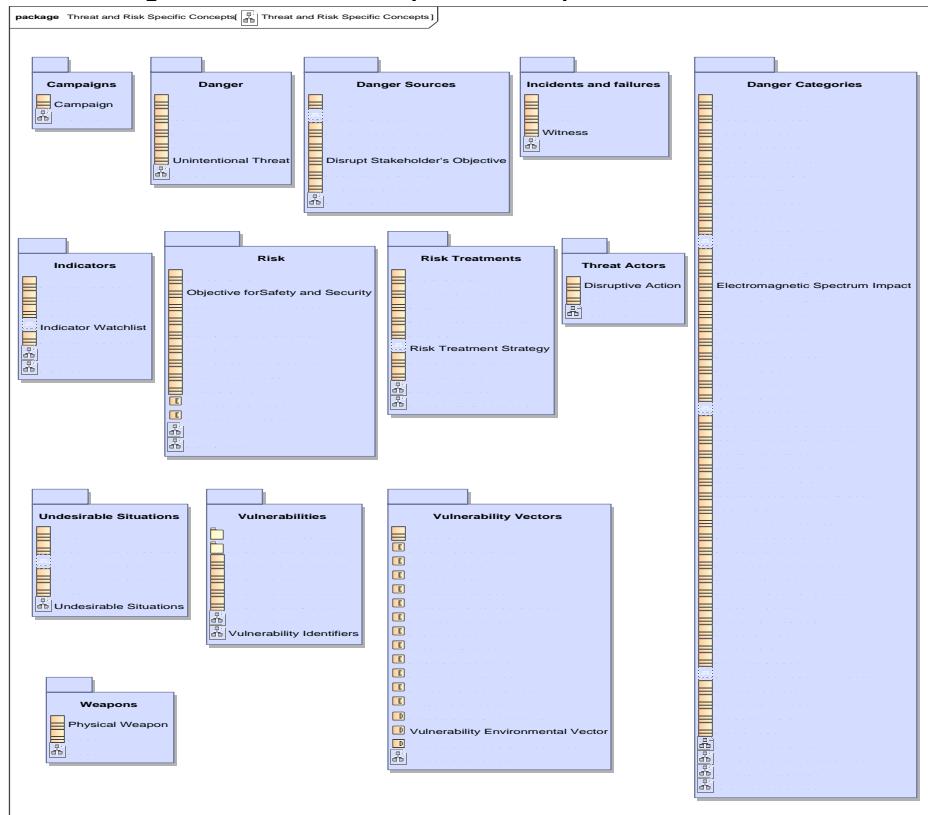


Figure 1. Threat and Risk Specific Concepts

8.2 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Summary Diagrams

8.2.1 Diagram: Entity Kinds

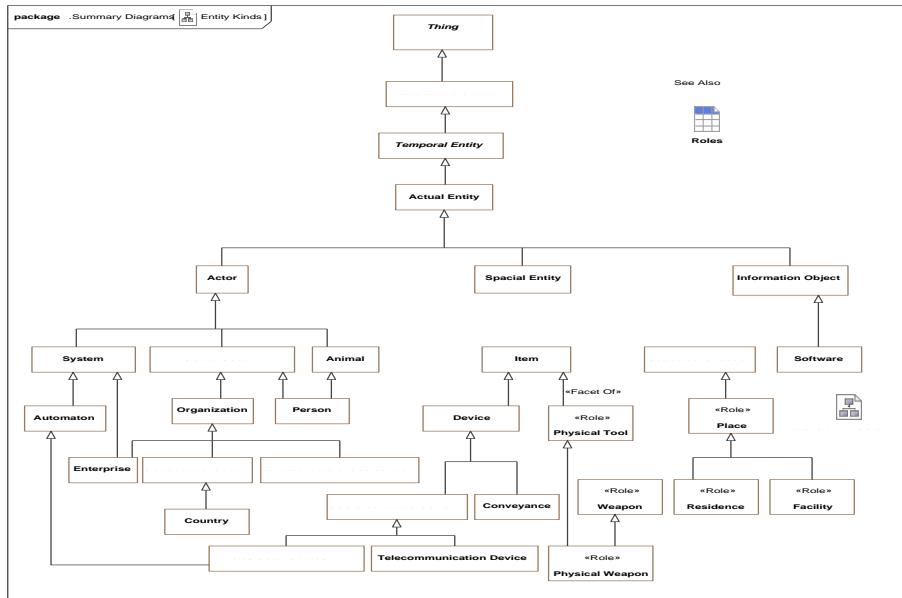


Figure 2. Entity Kinds

8.38.2 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Campaigns

Campaigns are ongoing activities in an organized and active way realizing a particular objective of stakeholders.

8.3.18.2.1 Diagram: Campaign

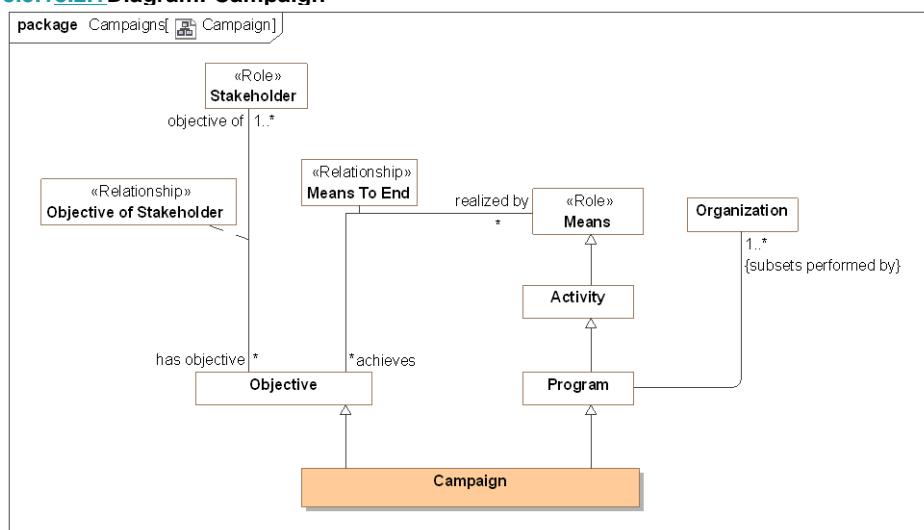


Figure 3_Figure 2_ Campaign

8.3.28.2.2 Class Campaign

Campaigns are ongoing work in an organized and active way toward a particular goal; typically a political, military, or social one. A campaign will typically have parts that are the specific activities of the campaign.

A Military campaign is a series of military operations intended to achieve a **particular objective**, confined to a **particular area**, or involving a specified type of fighting.

A campaign is also an objective for the activities supporting the campaign.

Direct Supertypes

[Objective](#), [Program](#)

8.48.3 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger

Concepts relative to threats. A threat is a situation that increases the likelihood of one or more related incidents.

8.4.18.3.1 Diagram: Danger

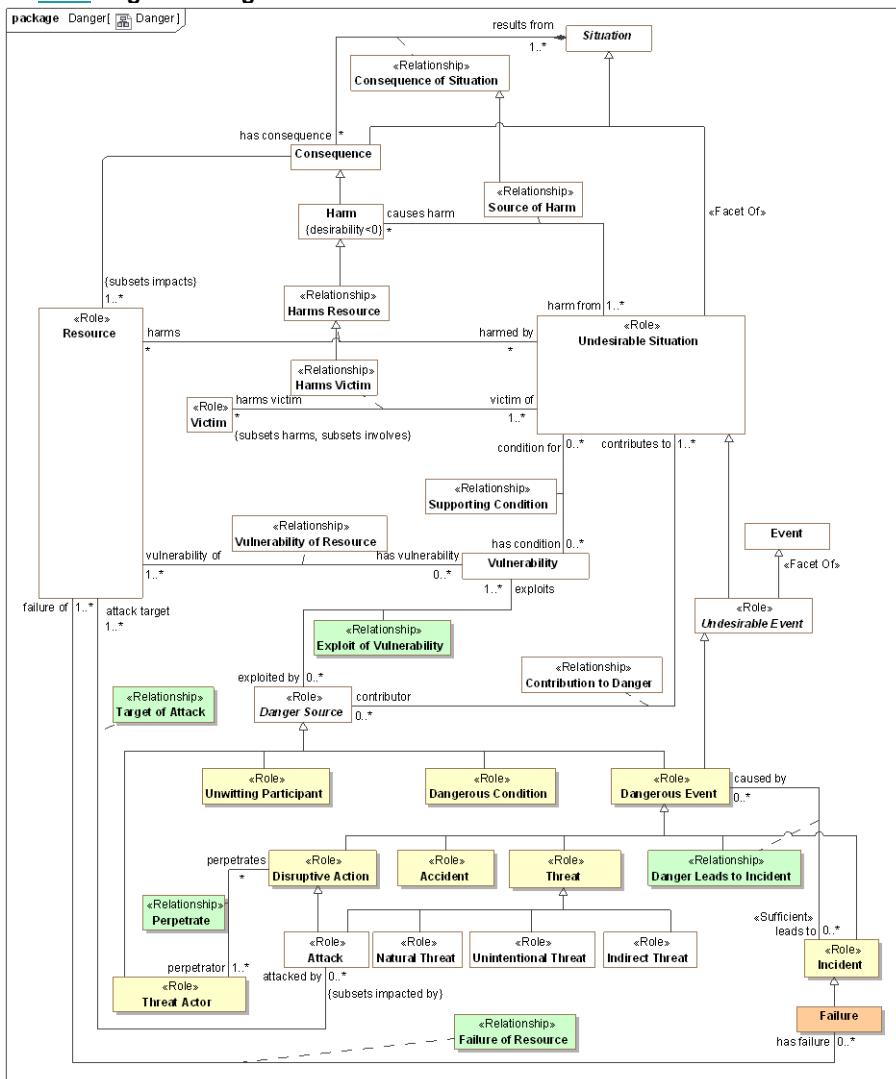


Figure 4-Figure 3. Danger

8.4.28.3.2 Class Attack <<Role>>

A dangerous activity that makes use of and derives benefit from a vulnerability and damages resources.

Direct Supertypes

[Activity Effecting Entity](#), [Disruptive Action](#), [Threat](#)

Associations

 attack target : [Resource](#) [1..*] Subsets: impacts:[Identifiable Entity](#)
through association: [Target of Attack](#)

A resource intended to be harmed by an attack.

8.4.38.3.3 Class Indirect Threat <<Role>>

A threat that does directly cause harm but may lead to other situations that will ultimately cause harm.

Direct Supertypes

[Threat](#)

8.4.48.3.4 Class Natural Threat <<Role>>

A threat from natural means.

Direct Supertypes

[Threat](#)

8.4.58.3.5 Association Class Target of Attack <<Relationship>>

Target of attack relates an attack to the resources attacked, the attack targets.

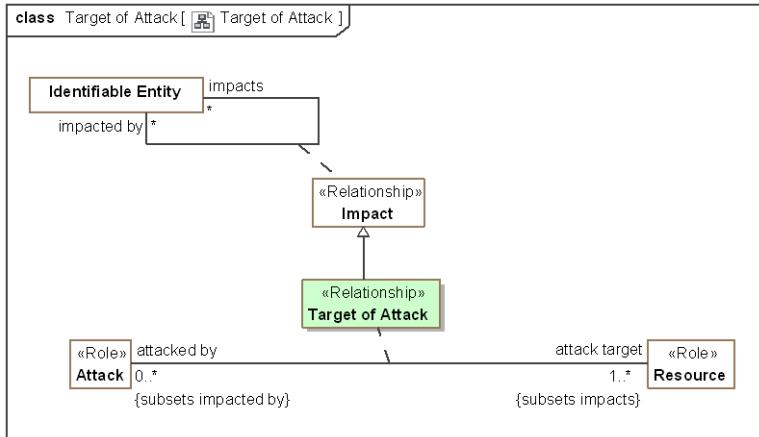


Figure 1. Target of Attack

Direct Supertypes

Impact

Association Ends

attack target : Resource [1..*] Subsets: impacts:Identifiable Entity

A resource intended to be harmed by an attack.

attacked by : Attack [0..*] Subsets: impacts:Identifiable Entity

Attack on a resource.

8.4.68.3.6 Class Threat <>Role>>

A threat is role of a situation that may lead to one or more related incidents or failures.

The threat consists of the existence of zero or more threat actors together with a set of one or more vulnerabilities. Thus, the threat of theft may result in an actual theft (attack), and threats correspond to attacks that are typically classified by attacker motivation (e.g., theft) as opposed to technique (e.g., spoofing). In some books and articles, the different but highly related terms “attack” and “threat” are sometimes confounded by being used as synonyms [Firesmith 03, Tulloch 03].

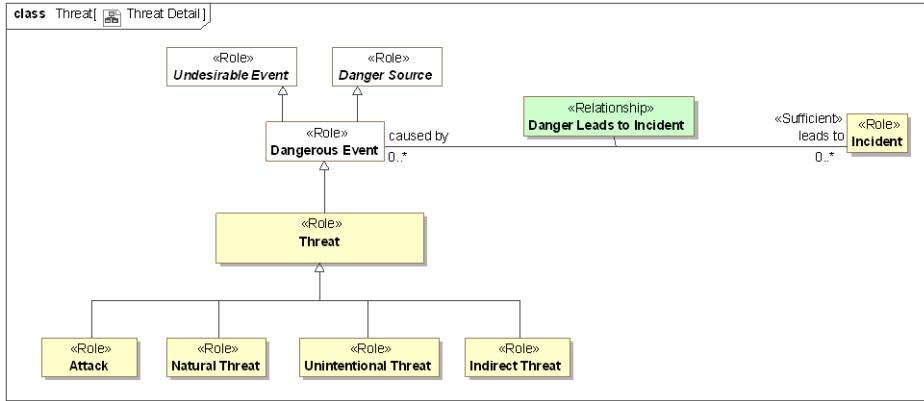


Figure 2. Threat Detail

Direct Supertypes

[Dangerous Event](#)

8.4.78.3.7 Class Unintentional Threat <<Role>>

A threat that is natural or not intended to cause harm.

Direct Supertypes

[Threat](#)

8.58.4 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger Categories

This package defines categories for risks and threats. These categories are not intended as exhaustive as others may be added. Categories may be combined.

8.5.18.4.1 Diagram: Danger Categories

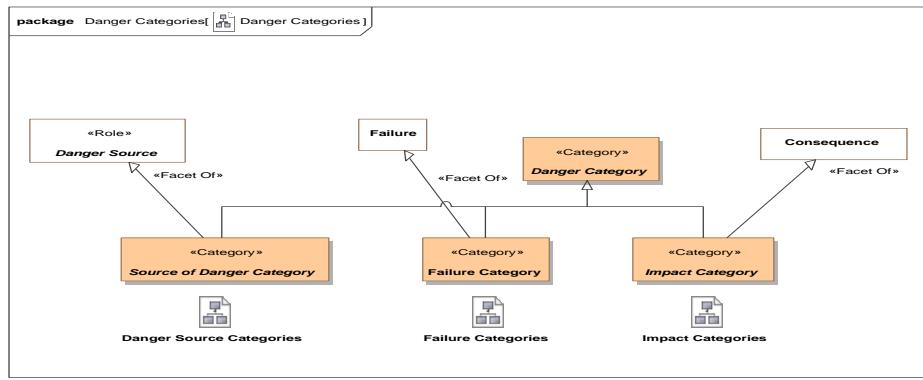


Figure 3. Danger Categories

8.5.28.4.2 Diagram: Danger Source Categories

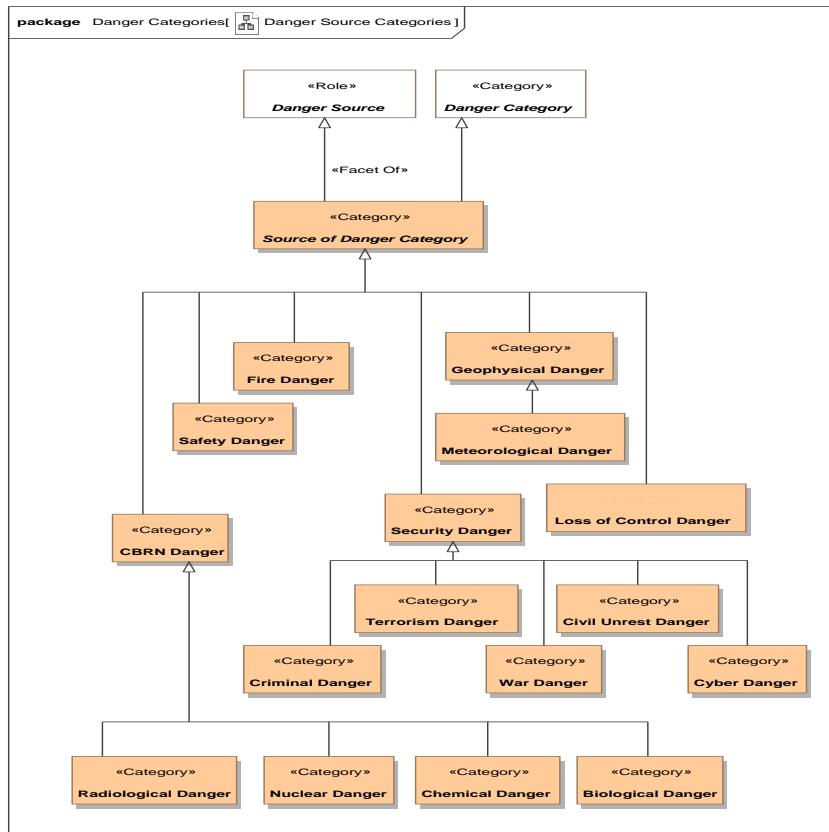


Figure 4. Danger Source Categories

8.5.38.4.3Diagram: Failure Categories

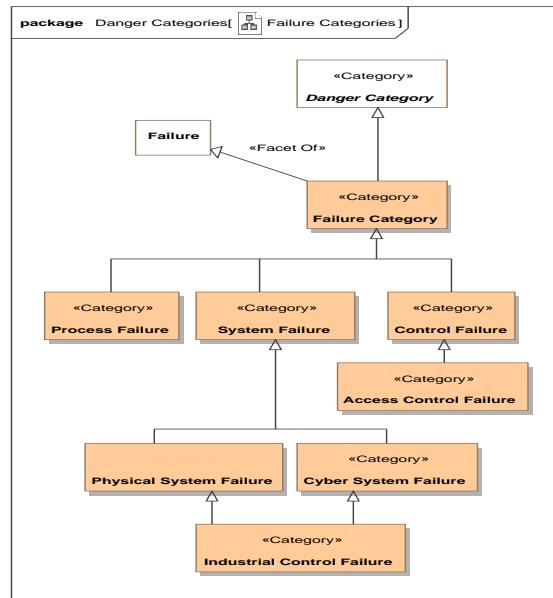


Figure 5. Failure Categories

8.5.48.4.4 Diagram: Impact Categories

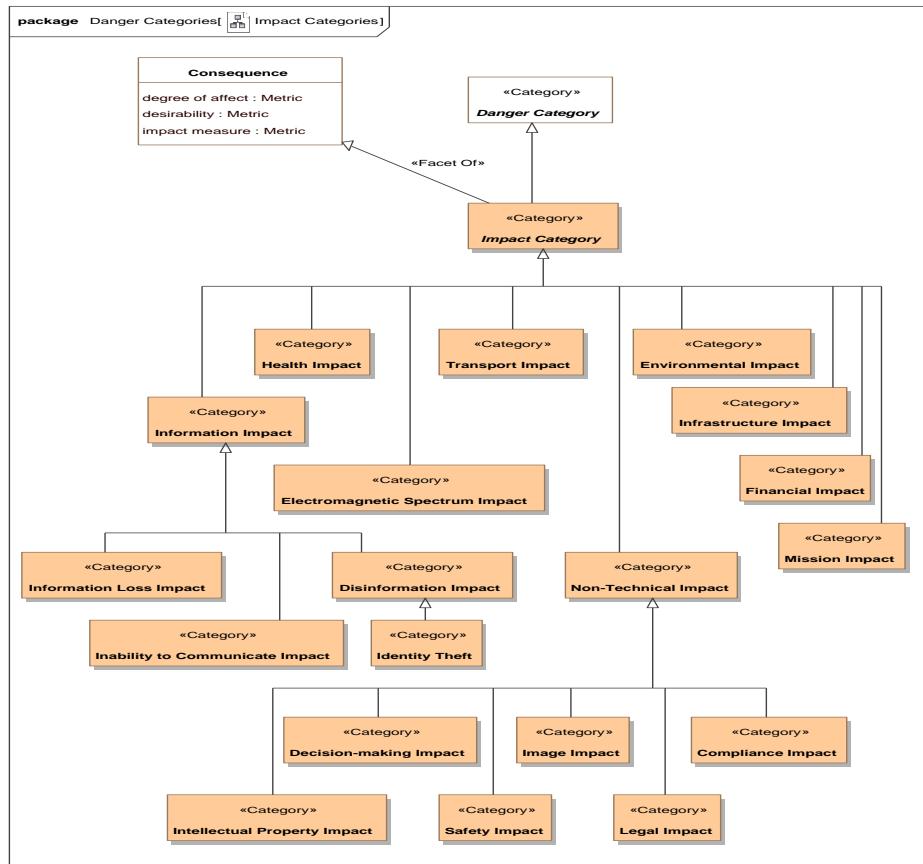


Figure 6. Impact Categories

8.5.58.4.5 Class Access Control Failure <<Category>>

Failure of permission controls to prevent unintended access.

Direct Supertypes

[Control Failure](#)

8.5.68.4.6Class Biological Danger <<Category>>

Any danger from a biological source.

Direct Supertypes

[CBRN Danger](#)

8.5.78.4.7Class CBRN Danger <<Category>>

A Chemical, biological, radiological or nuclear danger.

Direct Supertypes

[Source of Danger Category](#)

8.5.88.4.8Class Chemical Danger <<Category>>

A danger from a chemical.

Direct Supertypes

[CBRN Danger](#)

8.5.98.4.9Class Civil Unrest Danger <<Category>>

Danger resulting from the actions of a group of people causing disruption of the normal course of society.

Direct Supertypes

[Security Danger](#)

8.5.108.4.10Class Compliance Impact <<Category>>

Impact on the ability to comply with policies.

Direct Supertypes

[Non-Technical Impact](#)

8.5.148.4.11Class Control Failure <<Category>>

Failure of a policy or control process.

Direct Supertypes

[Failure Category](#)

8.5.128.4.12Class Criminal Danger <<Category>>

Danger from a criminal activity.

Direct Supertypes

[Security Danger](#)

8.5.138.4.13Class Cyber Danger <<Category>>

Danger related to computer systems and networks.

Direct Supertypes

[Security Danger](#)

8.5.148.4.14Class Cyber System Failure <<Category>>

Failure of any cyber system - hardware, software, or network to operate as intended.

Direct Supertypes

[System Failure](#)

8.5.158.4.15Class Danger Category <<Category>>

General category for dangers. Note that danger categories may be combined.

8.5.168.4.16Class Decision-making Impact <<Category>>

Impact on the ability to make informed decisions.

Direct Supertypes

[Non-Technical Impact](#)

8.5.178.4.17Class Disinformation Impact <<Category>>

Impact resulting from incorrect information.

Direct Supertypes

[Information Impact](#)

8.5.188.4.18Class Electromagnetic Spectrum Impact <<Category>>

Impact based on disruption in spectrum.

Direct Supertypes

[Impact Category](#)

8.5.198.4.19 Class Environmental Impact <<Category>>

A danger to the environment.

Direct Supertypes

[Impact Category](#)

8.5.208.4.20 Class Failure Category <<Category>>

A category of failure of a resource.

Direct Supertypes

[Danger Category, Failure](#)

8.5.218.4.21 Class Financial Impact <<Category>>

Impact resulting in loss of capital or the ability to obtain capital.

Direct Supertypes

[Impact Category](#)

8.5.228.4.22 Class Fire Danger <<Category>>

Danger from fire

Direct Supertypes

[Source of Danger Category](#)

8.5.238.4.23 Class Geophysical Danger <<Category>>

A danger resulting from the geography or movement of the earth.

Direct Supertypes

[Source of Danger Category](#)

8.5.248.4.24 Class Health Impact <<Category>>

A category of danger to people's health.

Direct Supertypes

[Impact Category](#)

8.5.258.4.25Class Identity Theft <<Category>>

A category of danger where an individual's identity is assumed by another...

Direct Supertypes

[Disinformation Impact](#)

8.5.268.4.26Class Image Impact <<Category>>

Impact to how an entity is viewed by others.

Direct Supertypes

[Non-Technical Impact](#)

8.5.278.4.27Class Impact Category <<Category>>

Categorization of the impact of dangers. Danger categories may be combined.

Direct Supertypes

[Consequence](#), [Danger Category](#)

8.5.288.4.28Class Inability to Communicate Impact <<Category>>

Category of impact to the ability to communicate.

Direct Supertypes

[Information Impact](#)

8.5.298.4.29Class Industrial Control Failure <<Category>>

A category of danger to the automated control of industrial systems.

Direct Supertypes

[Cyber System Failure](#), [Physical System Failure](#)

8.5.308.4.30Class Information Impact <<Category>>

A category of danger impact related to information - its unauthorized use or modification.

Direct Supertypes

[Impact Category](#)

8.5.348.4.31 Class Information Loss Impact <<Category>>

A category of danger impact where information becomes unavailable to the information owner.

Direct Supertypes

[Information Impact](#)

8.5.328.4.32 Class Infrastructure Impact <<Category>>

Classification of impact to infrastructure such that it is ~~not longer~~no longer available to fulfill objectives.

Direct Supertypes

[Impact Category](#)

8.5.338.4.33 Class Intellectual Property Impact <<Category>>

Category indicating a loss or compromise of intellectual property.

Direct Supertypes

[Non-Technical Impact](#)

8.5.348.4.34 Class Legal Impact <<Category>>

A categorization of impact to legal status or legal measures.

Direct Supertypes

[Non-Technical Impact](#)

8.5.358.4.35 Class Loss of Control Danger <<Category>>

Categorization of a danger resulting from the control of a system gained by parties not intended to have that control.

Direct Supertypes

[Source of Danger Category](#)

8.5.368.4.36 Class Meteorological Danger <<Category>>

Category of meteorological impact (e.g., ~~flood~~, flood).

Direct Supertypes

[Geophysical Danger](#)

8.5.378.4.37Class Mission Impact <<Category>>

Category of the impact on the ability to achieve a mission purpose.

Direct Supertypes

[Impact Category](#)

8.5.388.4.38Class Non-Technical Impact <<Category>>

Category representing the impact to something other than the ability to operate.

Direct Supertypes

[Impact Category](#)

8.5.398.4.39Class Nuclear Danger <<Category>>

Category of danger from a nuclear blast.

Direct Supertypes

[CBRN Danger](#)

8.5.408.4.40Class Physical System Failure <<Category>>

A category of danger of failure of any physical system.

Direct Supertypes

[System Failure](#)

8.5.418.4.41Class Process Failure <<Category>>

Categorization of a failure of a process to fulfill its objectives.

Direct Supertypes

[Failure Category](#)

8.5.428.4.42Class Radiological Danger <<Category>>

A categorization of danger from radiation.

Direct Supertypes

[CBRN Danger](#)

8.5.438.4.43Class Safety Danger <<Category>>

General emergency and public safety danger category. [CAP]

Direct Supertypes

[Source of Danger Category](#)

8.5.448.4.44Class Safety Impact <<Category>>

Category of impact to the safety of a resource.

Direct Supertypes

[Non-Technical Impact](#)

8.5.458.4.45Class Security Danger <<Category>>

[CAP] Danger category of “Security” - Law enforcement, military, homeland and local/private security.

Direct Supertypes

[Source of Danger Category](#)

8.5.468.4.46Class Source of Danger Category <<Category>>

A categorization of the source of dangers.

Direct Supertypes

[Danger Category, Danger Source](#)

8.5.478.4.47Class System Failure <<Category>>

Category of failure of a system - physical, financial, cyber, etc. such that the system is no longer available to serve its objectives.

Direct Supertypes

[Failure Category](#)

8.5.488.4.48Class Terrorism Danger <<Category>>

Category of danger from terrorism.

Direct Supertypes

[Security Danger](#)

8.5.498.4.49Class Transport Impact <<Category>>

[CAP] A category of impact to public or private transportation.

Direct Supertypes

[Impact Category](#)

8.5.508.4.50Class War Danger <<Category>>

A Category of danger from acts of war.

Direct Supertypes

[Security Danger](#)

8.6.18.5 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger Sources

A package categorizing source of dangers - natural, systematic, or intentional

8.6.18.5.1 Diagram: Danger Sources

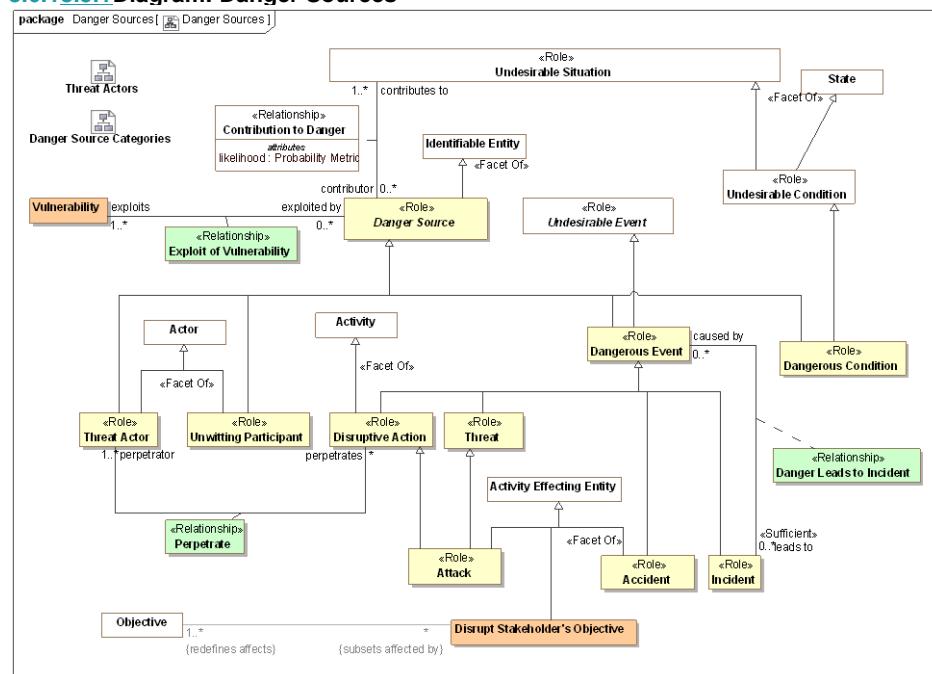


Figure 7. Danger Sources

8.6.28.5.2 Class Accident <>Role>

An unfortunate incident that happens unexpectedly and unintentionally, typically resulting in damage or injury. e.g. a child falling into an open well in a playground.

Direct Supertypes

[Activity Effecting Entity](#), [Dangerous Event](#)

8.6.38.5.3 Association Class Contribution to Danger <<Relationship>>

A relationship defining the undesirable situations a danger source contributes to.

Direct Supertypes

[Impact](#)

Association Ends

contributor : [Danger Source](#) [0..*] Subsets: impacts:[Identifiable Entity](#)

A danger source that can contribute to the possibility of an undesirable situation occurring.

contributes to : [Undesirable Situation](#) [1..*] Subsets: impacts:[Identifiable Entity](#)

Undesirable situation that is enabled by a danger source. e.g., an open well contributes to the danger of a child falling in that well.

Attributes

likelihood : [Probability Metric](#)

8.6.48.5.4 Class Danger Source <<Role>>

The source of any danger - natural, systematic, or intentional, where a danger is a situation (including events) that may lead to an incident that causes harm.

Direct Supertypes

[Identifiable Entity](#)

Associations

exploits : [Vulnerability](#) [1..*] Subsets: impacts:[Identifiable Entity](#)

through association: [Exploit of Vulnerability](#)

Vulnerability used by a danger source (intentionally or unintentionally) to directly or indirectly cause harm.

contributes to : [Undesirable Situation](#) [1..*] Subsets: impacts:[Identifiable Entity](#)

through association: [Contribution to Danger](#)

Undesirable situation that is enabled by a danger source. e.g., an open well contributes to the danger of a child falling in that well.

8.6.58.5.5 Class Dangerous Condition <<Role>>

A condition (not an event) that may directly or indirectly lead to harm. e.g. an open well in a playground.

Direct Supertypes

[Danger Source](#), [Undesirable Condition](#)

8.6.68.5.6 Class Dangerous Event <>Role>>

An event that is the source of danger - natural, systematic, or intentional, where a danger is a that may lead to an incident that causes harm.

Direct Supertypes

[Danger Source](#), [Undesirable Event](#)

Associations

 leads to : [Incident](#) [0..*] Subsets: causes:[Situation](#) contributes to:[Undesirable Situation](#)
through association: [Danger Leads to Incident](#)

Incident that is the result of a threat.

8.6.78.5.7 Class Disrupt Stakeholder's Objective

An action intended to harm the objectives of a stakeholder.

Direct Supertypes

[Activity Effecting Entity](#), [Disruptive Action](#)

Associations

 <>Restriction>> : [Objective](#) [1..*] Redefines: affects:[Identifiable Entity](#)

An objective that is disrupted by an intentional action.

8.6.88.5.8 Association Class Exploit of Vulnerability <>Relationship>>

Vulnerabilities that are leveraged by a danger source to cause or potentially cause harm.

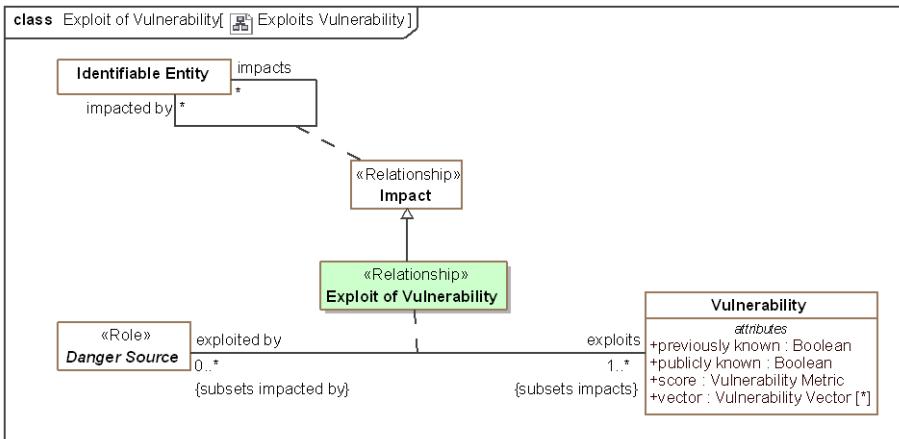


Figure 8. Exploits Vulnerability

Direct Supertypes

Impact

Association Ends

█ exploits : Vulnerability [1..*] Redefines: affects: Identifiable Entity

Vulnerability used by a danger source (intentionally or unintentionally) to directly or indirectly cause harm.

█ exploited by : Danger Source [0..*] Redefines: affects: Identifiable Entity

Danger source that can or did exploit a vulnerability such that it leads to an undesirable situation.

8.6.98.5.9 Class Objective to Disrupt

Something that efforts or actions are intended to attain such that it damages another in some way or obtains resources not intended for a threat actor.

Direct Supertypes

Objective

Associations

↙ <<Restriction>> : Disruptive Action [0..*] Subsets: realized by: Means

Objective of a threat actor to cause a system to fail.

↙ <<Restriction>> : Threat Actor [*] Redefines: Objective to Disrupt

8.6.108.5.10Class Unwitting Participant <>Role>>

An actor facilitating an activity or process without their prior knowledge or consent.

Direct Supertypes

[Actor](#), [Danger Source](#)

8.78.6 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents and failures

Concepts relating to incidents - undesired events that actually happen and impact victims.

8.7.18.6.1 Diagram: Incident

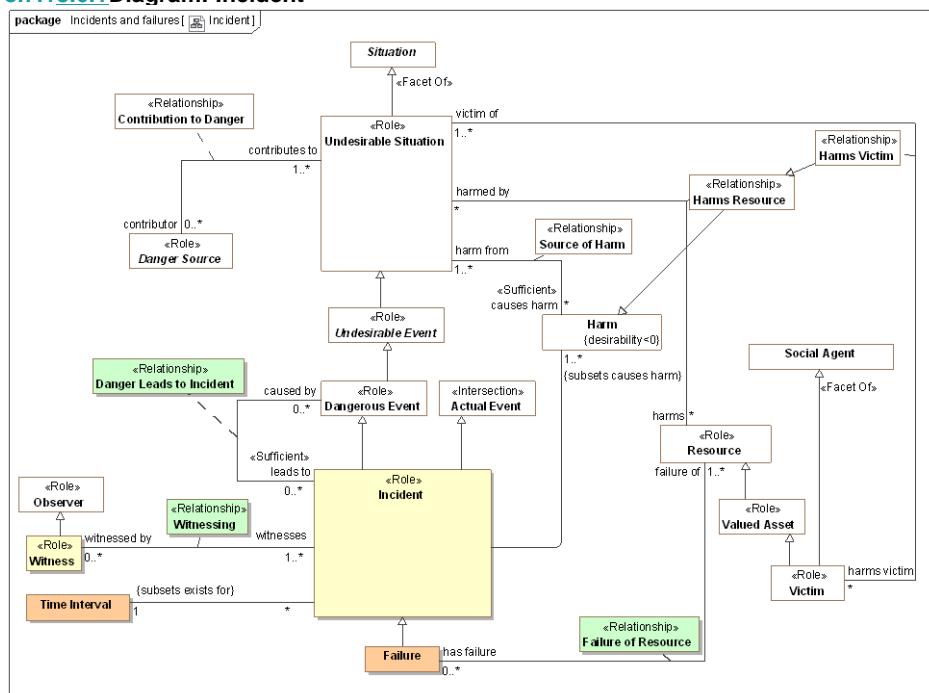


Figure 9. Incident

8.7.28.6.2 Association Class Danger Leads to Incident <<Relationship>>

The relationship between an incident and its causes, dangerous events.

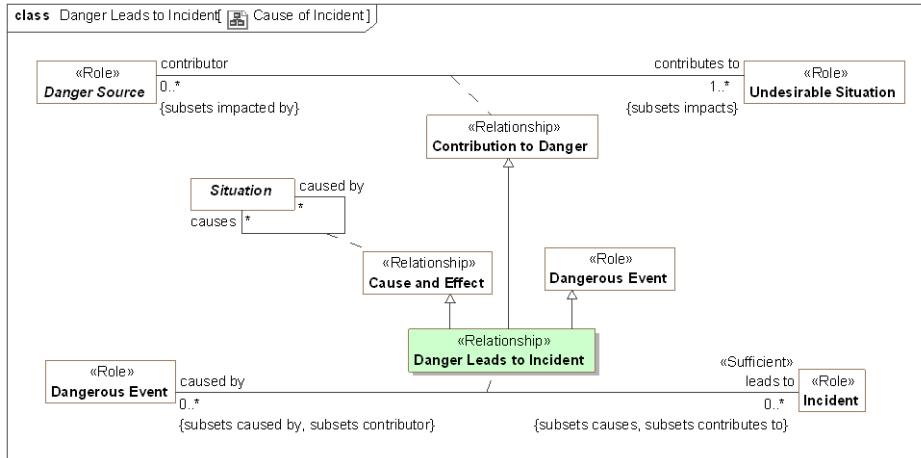


Figure 10. Cause of Incident

Direct Supertypes

[Cause and Effect](#), [Contribution to Danger](#), [Dangerous Event](#)

Association Ends

leads to : [Incident](#) [0..*] Redefines: : [Objective to Disrupt](#)

Incident that is the result of a threat.

caused by : [Dangerous Event](#) [0..*] Redefines: : [Objective to Disrupt](#)

Cause of an incident.

8.7.38.6.3 Class Failure

Failure is an incident which causes a resource to not fulfill its intended function.

Direct Supertypes

[Incident](#)

Associations

failure of : [Resource](#) [1..*] Subsets: impacts:[Identifiable Entity](#)
through association: [Failure of Resource](#)

Resource that fails in a failure event. The resource is no longer able to fulfill its function as intended.

8.7.48.6.4 Association Class Failure of Resource <<Relationship>>

Relationship between a failure event and the resources that have failed.

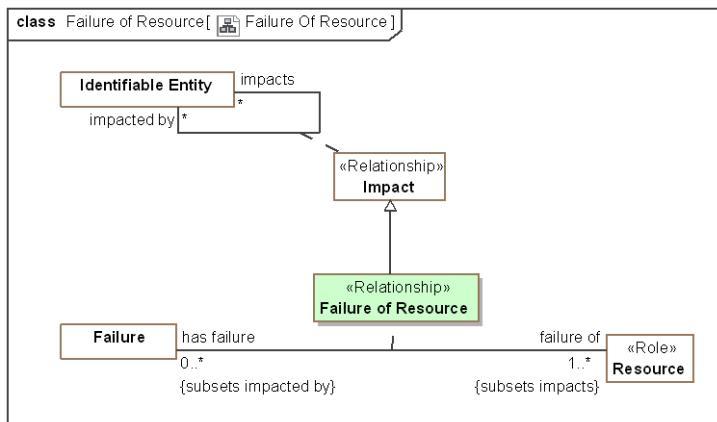


Figure 11. Failure Of Resource

Direct Supertypes

Impact

Association Ends

 has failure : [Failure](#) [0..*] Subsets: impacts:[Identifiable Entity](#)

Realized or potential failures of a resource.

failure of : Resource [1..*] Subsets: impacts:Identifiable Entity

Resource that fails in a failure event. The resource is no longer able to fulfill its function as intended.

8.7.58.6.5 Class Incident <<Role>>

An incident is a dangerous situation that is happening or has happened directly causing harm (detriment) to victims. Kinds of incidents include attacks, disasters, and accidents. Incidents are actualized risks.

Direct Supertypes

Actual Event, Dangerous Event

Associations

 caused by : [Dangerous Event](#) [0..*] Subsets: caused by:[Situation](#), contributor:[Danger Source](#)
through associations: [Danger Leads to Incident](#)

Cause of an incident.

- ✓ : [Harm](#) [1..*] Subsets: causes harm:[Harm](#)
- ✓ : [Time Interval](#) [1] Subsets: exists for:[Time Interval](#)
- █ witnessed by : [Witness](#) [0..*] Subsets: observed by:[Observer](#)
through association: [Witnessing](#)

Witnesses of an incident

[8.7.68.6.6 Class Witness <<Role>>](#)

Role of a person who observes an event, typically a crime or accident, take place.

Direct Supertypes

[Observer](#)

Associations

- █ witnesses : [Incident](#) [1..*] Subsets: observes:[Identifiable Entity](#)
through association: [Witnessing](#)

Incident observed by a witness.

[8.7.78.6.7 Association Class Witnessing <<Relationship>>](#)

Witnessing is the observation of an incident by a witness

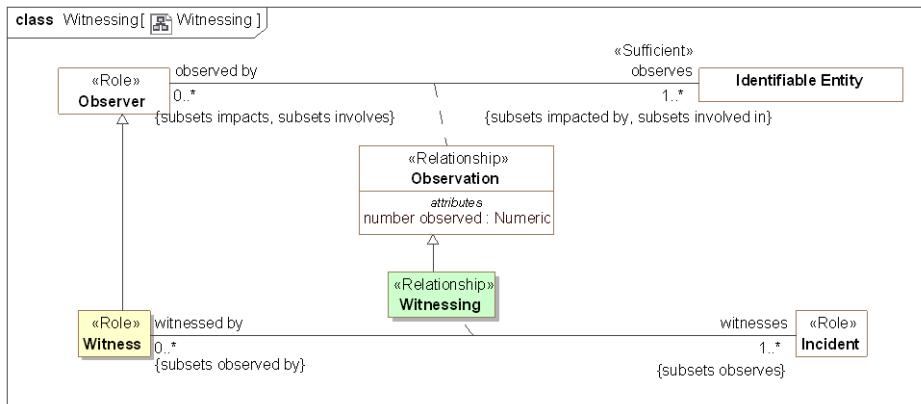


Figure 12. Witnessing

Direct Supertypes

Observation

Association Ends

 witnesses : [Incident](#) [1..*] Subsets: observes:[Identifiable Entity](#)

Incident observed by a witness.

 witnessed by : [Witness](#) [0..*] Subsets: observes:[Identifiable Entity](#)

Witnesses of an incident

8.88.7 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Indicators

Indicators are patterns of *situations* or lists of entities to watch out for that **indicate** a **situation** that may happen. An indicator may be scoped by an entity/situation, which contextualizes when it applies. When a situation matching an indicator is *observed* there is a *sighting* of that indicator which is then *evidence* for an *actual situation*, such as an *incident*. e.g., watch for these terrorists in airports.

A *sighting* is an *observation* that matches the pattern of an indicator. e.g., the terrorist Killer-Joe was seen at BWI on 12/11/2014 by a police officer Sam Shoe.

Indicators are not certain and may have a likelihood attached to the potential situations for which they are evidence.

Once a sighting flags an indicator, a *course of action* rule may be fired based on the indicated situation.

Specializations of indicator include indicator patterns (an arbitrary pattern of anything) and watch lists. Indicators may also be grouped.

8.8.18.7.1 Diagram: Indicator

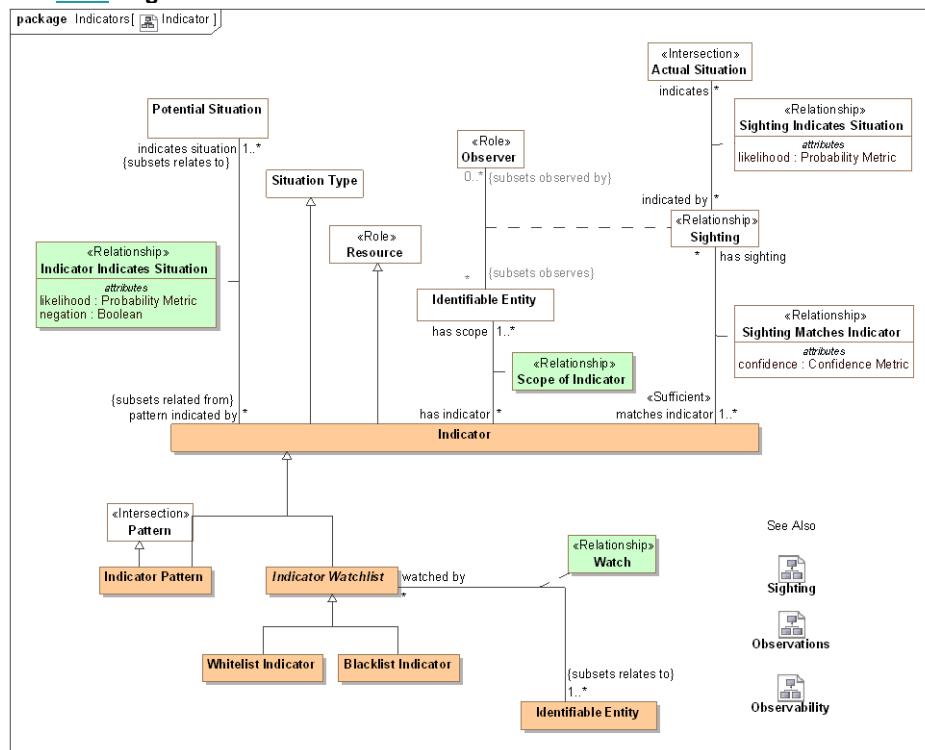


Figure 13. Indicator

8.8.28.7.2Diagram: Sighting

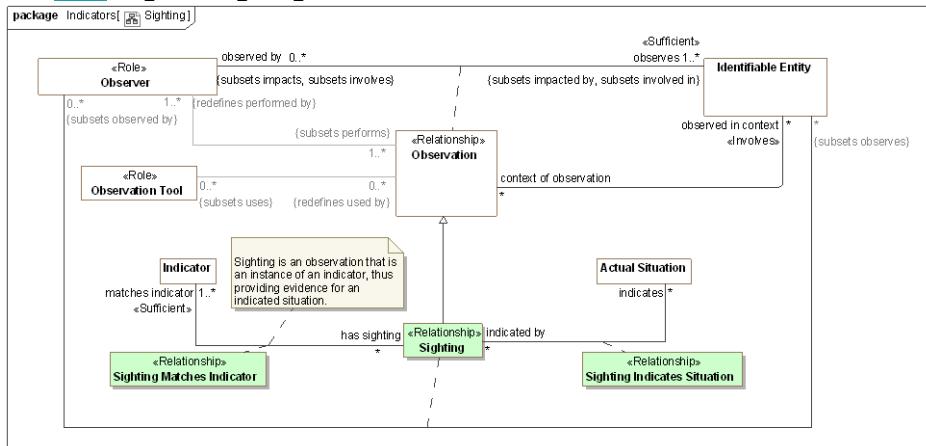


Figure 14. Sighting

8.8.38.7.3Class Blacklist Indicator

A list of watched entities that are assumed to pose a threat.

Direct Supertypes

[Indicator Watchlist](#)

8.8.48.7.4Class Indicator

An **indicator** is a predicate such that matching sightings are evidence for a possible situation. Sightings matching an indicator suggest further study or action based on a **course of action rule**.

Subtypes of indicator define what is watched for: a pattern, a watch list or some combination of other indicators. Indicators may be restricted to (relevant only within) a specific scope.

Direct Supertypes

[Resource](#), [Situation Type](#)

Associations

█ indicates situation : [Potential Situation](#) [1..*] Subsets: relates to:[Identifiable Entity](#)
through association: [Indicator Indicates Situation](#)

The situation pattern that may be inferred by a sighting matching the subject indicator.

 has sighting : [Sighting](#) [*] Subsets: has type:[Type](#)
through association: [Sighting Matches Indicator](#)

Sightings that match the subject indicator and may therefore imply the indicated situation.

 monitored by : [Monitoring Safeguard](#) [0..*] Subsets: used by:[Event](#)
through association: [Monitor](#)

Activities monitoring an indicator using a monitoring safeguard.

 : [Observer](#) [*] Redefines: can be utilized by:[Actor](#)
through association: [Observability](#)
 has scope : [Identifiable Entity](#) [1..*] Subsets: in context of:[Context](#)
through association: [Scope of Indicator](#)

An entity that defines a context for where an indicator is valid.

8.8.58.7.5 Association Class Indicator Indicates Situation <<Relationship>>

Relationship between an indicator that classifies some kind of situation and the kind of potential situation that the indicator suggests. The indicator is evidence for the indicated situation.

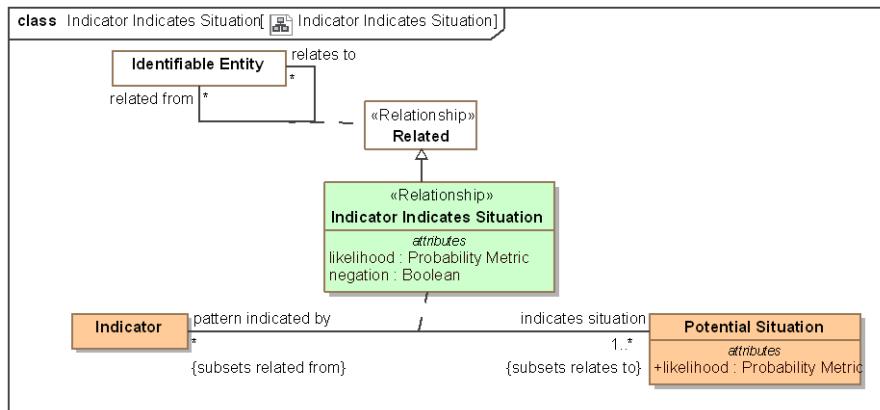


Figure 15. Indicator Indicates Situation

Direct Supertypes

[Related](#)

Association Ends

 indicates situation : [Potential Situation](#) [1..*] Subsets: in context of:[Context](#)

The situation pattern that may be inferred by a sighting matching the subject indicator.

 pattern indicated by : [Indicator](#) [*] Subsets: in context of: [Context](#)

Indicator that may be used as evidence that a potential situation has been realized by an actual situation.

Attributes

◊ likelihood : [Probability Metric](#)

The probability that the indication relationship actually indicates the situation. Note that likelihood may be negative, indicating that the indicator suggests the absence of the indicated pattern .

◊ negation : [Boolean](#)

[STIX] The negate field specifies the absence of the indicated pattern, inverting the sign of "likelihood".

8.8.68.7.6 Class Indicator Pattern

An indicator defined by a pattern. When the pattern is matched, the indicator "fires", indicating instances of the indicated potential situations.

Direct Supertypes

[Indicator](#), [Pattern](#)

8.8.78.7.7 Class Indicator Watchlist

An indicator defined by a set of entities (which can be individuals or situations) that should be watched for in a particular context. The members of the watch list are represented by "watches". When a watched individual is sighted, the indicator "fires", indicating instances of the indicated potential situations.

Direct Supertypes

[Indicator](#)

Associations

 watches : [Identifiable Entity](#) [1..*] Subsets: relates to: [Identifiable Entity](#)
through association: [Watch](#)

The entities (individuals, systems, situations, etc.) watched by a watch list.

8.8.88.7.8 Association Class Sighting <<Relationship>>

A sighting is a kind of observation that matches one or more indicators and that by matching indicators it increases the likelihood of the situation it <indicates>.

Sightings of indicators are not absolute. Both the matching of the sighting to the indicator and the indicated situation are qualified with a likelihood.

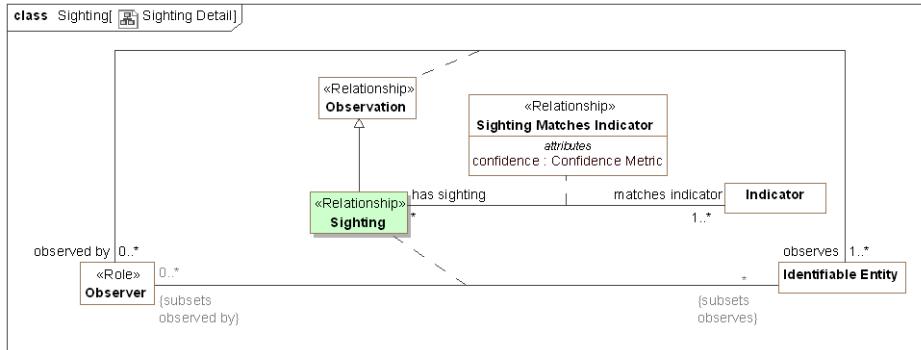


Figure 16. Sighting Detail

Direct Supertypes

[Observation](#)

Association Ends

- █ : [Identifiable Entity](#) [*] Subsets: relates to: [Identifiable Entity](#)
- █ : [Observer](#) [0..*] Subsets: relates to: [Identifiable Entity](#)

Associations

- █ indicates : [Actual Situation](#) [*] Subsets: relates to: [Identifiable Entity](#)
through association: [Sighting Indicates Situation](#)

Situation that is indicated by a sighting, the sighting is providing evidence for the situation.

- █ matches indicator : [Indicator](#) [1..*] Subsets: categorizes: [Thing](#)
through association: [Sighting Matches Indicator](#)

Indicator the subject sighting matches. The subject sighting will then provide evidence for an actual situation that is an instance of the potential situation of the indicator.

8.8.98.7.9 Association Class Sighting Indicates Situation <>Relationship>

Sightings provide evidence that the <indicates> situation may be occurring. This is based on the probability metric of the indicator the sighting is an instance of. Sighting Indicates Situation is derived from Indicator Indicates Situation where each potential situation indicated becomes a possible actual situation as evidenced by the sighting.

Similar to [SACM] AssertedEvidence: The AssertedEvidence association class records the declaration that one or more artefacts of Evidence (cited by ArtefactElementCitations) provide information that helps establish the truth of a Claim.
{AssertedEvidence references the record (artefacts) where as sightings are the actual event which may have record}

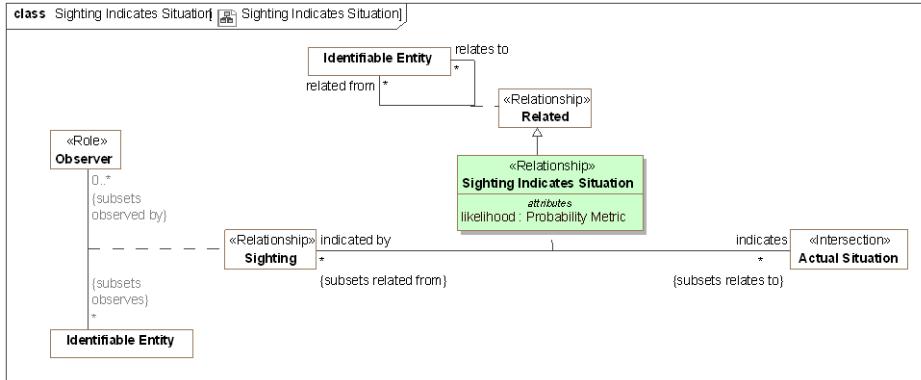


Figure 17. Sighting Indicates Situation

Direct Supertypes

[Related](#)

Association Ends

indicates : [Actual Situation](#) [*] Subsets: categorizes:[Thing](#)

Situation that is indicated by a sighting, the sighting is providing evidence for the situation.

indicated by : [Sighting](#) [*] Subsets: categorizes:[Thing](#)

Sightings that have been observed with respect to an actual situation, providing evidence of the situation.

Attributes

likelihood : [Probability Metric](#)

Probability that the specific sighting indicates the specific, actual situation referenced. In many cases this will be the same as the likelihood of the indicator's "Indicator Indicates Situation" likelihood, but specific conditions may increase or decrease that likelihood.

8.8.108.7.10 Association Class Sighting Matches Indicator <>Relationship>>

An assertion that a observation matches a particular indicator, thus classifying the observation as a sighting and providing evidence for situations the indicator, indicates.

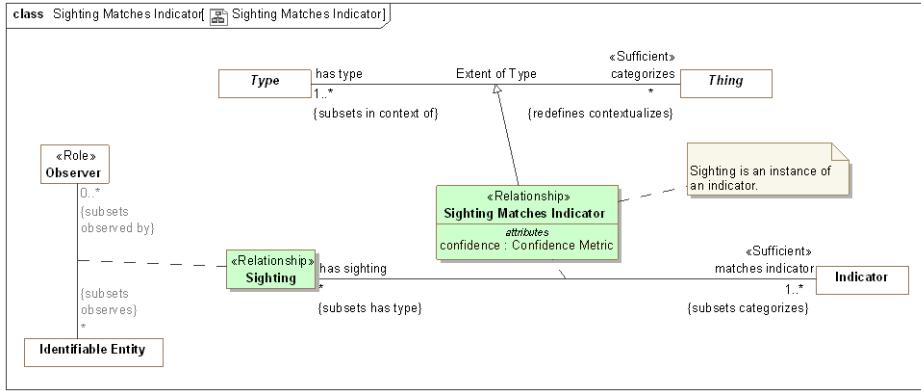


Figure 18. Sighting Matches Indicator

Direct Supertypes

[Extent of Type](#)

Association Ends

matches indicator : [Indicator](#) [1..*] Subsets: categorizes:[Thing](#)

Indicator the subject sighting matches. The subject sighting will then provide evidence for an actual situation that is an instance of the potential situation of the indicator.

has sighting : [Sighting](#) [*] Subsets: categorizes:[Thing](#)

Sightings that match the subject indicator and may therefore imply the indicated situation.

Attributes

confidence : [Confidence Metric](#)

Confidence that the observed sighting does actually match the pattern. e.g. The witness is 50% certain that the man in the airport had a gun.

8.8.118.7.11 Association Class Watch <>Relationship>>

Relationship defining that <watches> is on the <watched by> watch list.

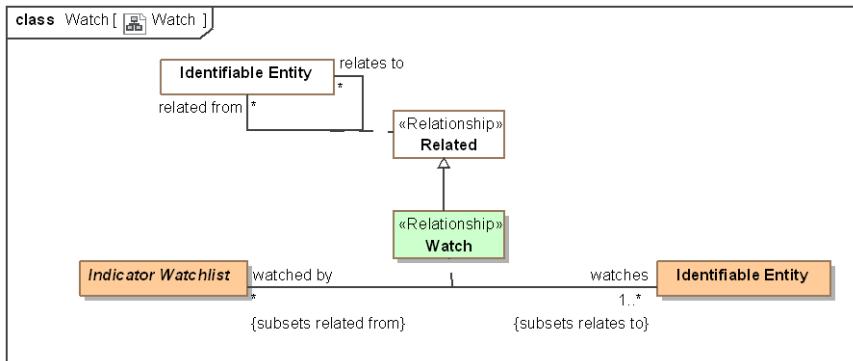


Figure 19. Watch

Direct Supertypes

[Related](#)

Association Ends

█ [watches](#) : [Identifiable Entity](#) [1..*] Subsets: categorizes:[Thing](#)

The entities (individuals, systems, situations, etc.) watched by a watch list.

█ [watched by](#) : [Indicator Watchlist](#) [*] Subsets: categorizes:[Thing](#)

Watch list the subject entity is listed in.

8.8.128.7.12 Class Whitelist Indicator

A list of watched entities that are assumed not to pose a threat.

Direct Supertypes

[Indicator Watchlist](#)

8.98.8 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk

Concepts relative to risk and risk analytics where risk is an assessment of the potential harm to resources important to a risk owner. At a high level risk is computed as the sum of the likelihood * impact for all resources valued by a risk owner.

8.9.18.8.1 Diagram: Risk

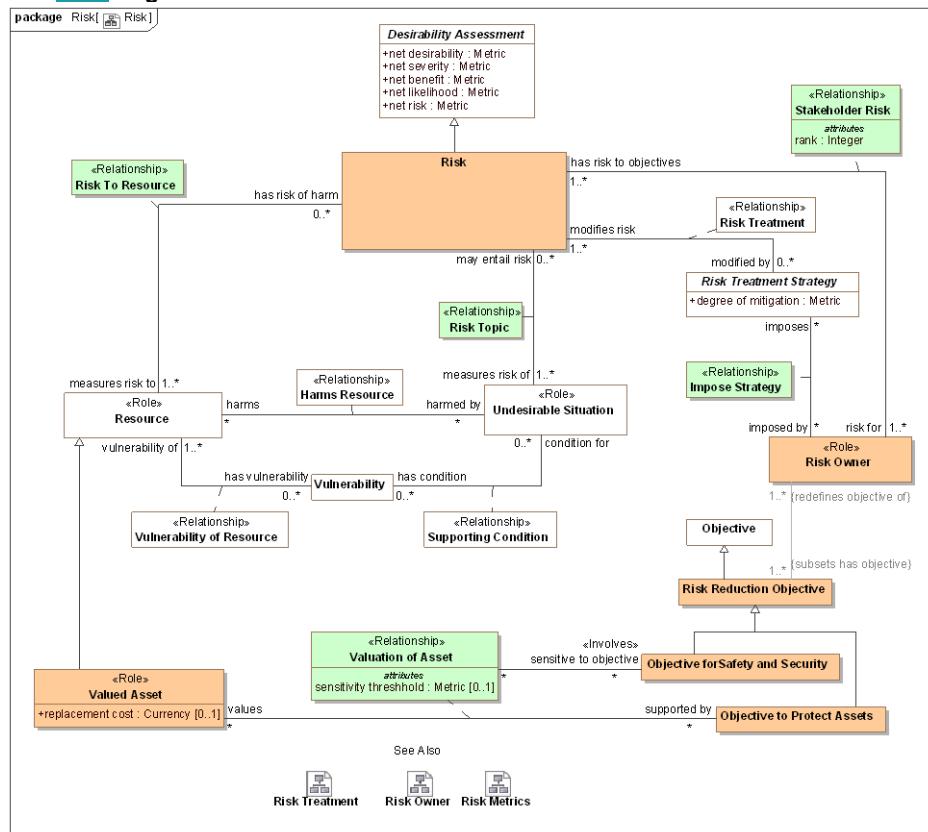


Figure 20. Risk

8.9.28.8.2Diagram: Risk Metrics

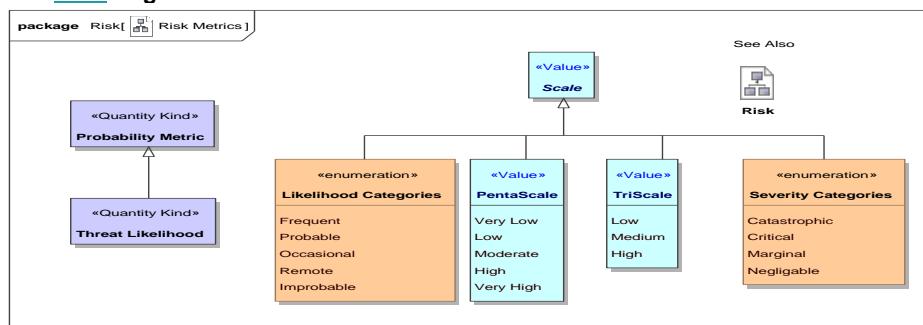


Figure 21. Risk Metrics

8.9.38.8.3Class Accept Risk

A strategy to live with the consequences of a risk and not mitigate it.

Direct Supertypes

[Risk Treatment Strategy](#)

Attributes

◆ risk level accepted : [Metric](#)

A metric representing the level of acceptable risk for the accept risk strategy.

8.9.48.8.4Association Class Impose Strategy <>Relationship>

A risk owner imposes a risk treatment strategy as a policy with the intent that the strategy reduces their risk to an acceptable level. The policy will be imposed in the entity that the policy <constraints>.

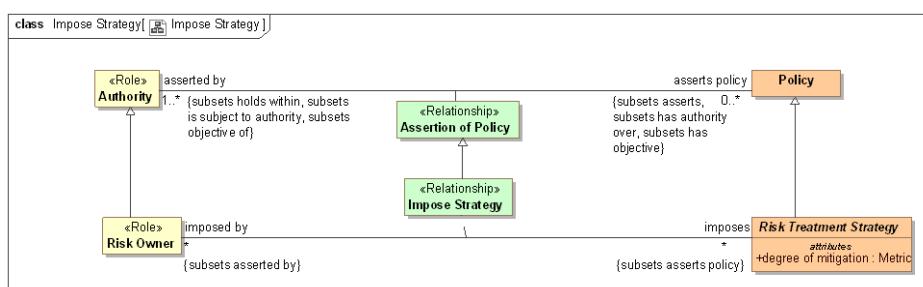


Figure 22. Impose Strategy

Direct Supertypes

[Assertion of Policy](#)

Association Ends

☒ imposes : [Risk Treatment Strategy](#) [*] Subsets: categorizes:[Thing](#)

Risk treatment strategy imposed by a risk owner to mediate the owners risk.

☒ imposed by : [Risk Owner](#) [*] Subsets: categorizes:[Thing](#)

Authority that imposes a risk strategy such that it is intended to reduce their risk.

8.9.58.8.5 Class Objective forSafety and Security

Classification of an objective related to the safety and security of a stakeholder. The protection from harm.

Direct Supertypes

[Risk Reduction Objective](#)

Associations

/ <<Involves>> : [Valuation of Asset](#) [*] Subsets: realized by:[Means](#)

8.9.68.8.6 Class Objective to Protect Assets

Objective of a stakeholder to protect an asset. To reduce the potential harm to valued assets.

Direct Supertypes

[Risk Reduction Objective](#)

Associations

☒ values : [Valued Asset](#) [*] Subsets: relates to:[Identifiable Entity](#)

through association: [Valuation of Asset](#)

An asset for which there is an objective to create, sustain, or protect the asset.

8.9.78.8.7 Class Risk

[CNSSI 4009] Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of Event.

[Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.]

Direct Supertypes

[Desirability Assessment](#)

Associations

 modified by : [Risk Treatment Strategy](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Risk Treatment](#)

A strategy to reduce the subject risk for the risk owner.

 risk for : [Risk Owner](#) [1..*] Subsets: impacts:[Identifiable Entity](#) assesses:[Assessed Entity](#)
through association: [Stakeholder Risk](#)

Owner of a risk. The risk owner has objectives to minimize the subject risk.

 measures risk of : [Undesirable Situation](#) [1..*] Subsets: assesses:[Assessed Entity](#)
through association: [Risk Topic](#)

Undesirable situations measured in terms of their risk of harming resources valued by a risk owner.

 measures risk to : [Resource](#) [1..*] Subsets: assesses:[Assessed Entity](#)
through association: [Risk To Resource](#)

Resources (aka assets) at risk.

8.9.88.8.8 Class Risk Mitigation Strategy

A plan which minimizes or eliminates the possibility or impact of a danger or risk.

Direct Supertypes

[Risk Treatment Strategy](#)

Associations

 leverages countermeasure : [Countermeasure](#) [1..*] Subsets: uses:[Resource](#)
through association: [Countermeasure for Strategy](#)

Countermeasure which serves a risk mitigation strategy.

8.9.98.8.9 Class Risk Owner <>Role>

A stakeholder with an objective to manage risk.

[ISO 73:2009] person or entity with the accountability and authority to manage a risk.

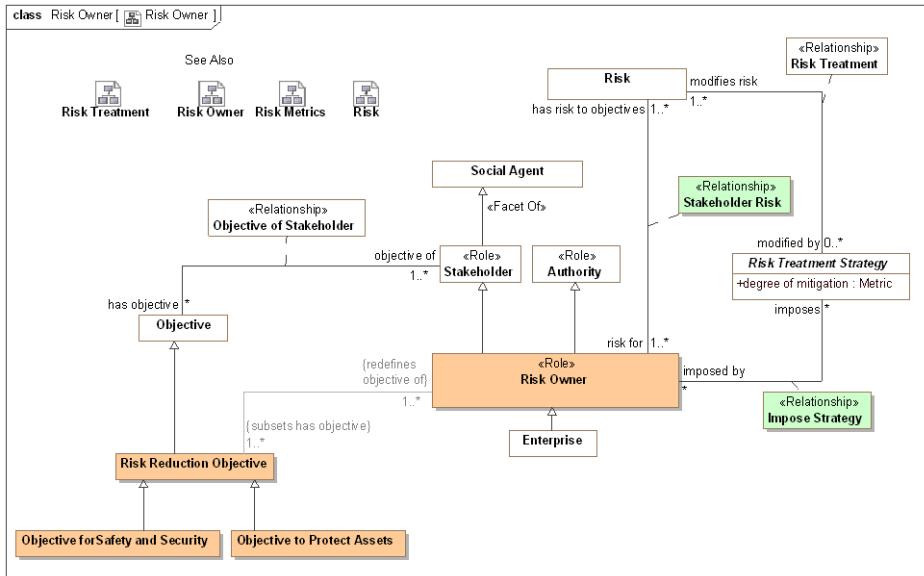


Figure 23. Risk Owner

Direct Supertypes

Authority, Stakeholder

Associations

- has risk to objectives : Risk [1..*] Subsets: impacted by:Identifiable Entity assessed by:Assessment through association: Stakeholder Risk

Risk owned by a risk owner such that the risk may impact the risk owners objectives.

- imposes : [Risk Treatment Strategy](#) [*] Subsets: asserts policy:[Policy](#) through association: [Impose Strategy](#)

Risk treatment strategy imposed by a risk owner to mediate the owners risk.

8.9.108.8.10 Class Risk Reduction Objective

An objective of a risk owner to reduce risk

Direct Supertypes

Objective

Associations

 <<Restriction>> : [Risk Owner](#) [1..*] Redefines: objective of: [Stakeholder](#)

8.9.118.8.11 Association Class Risk To Resource <<Relationship>>

The Risk to Resource relationship identifies the resources for which risk will be measured for the risk owner.

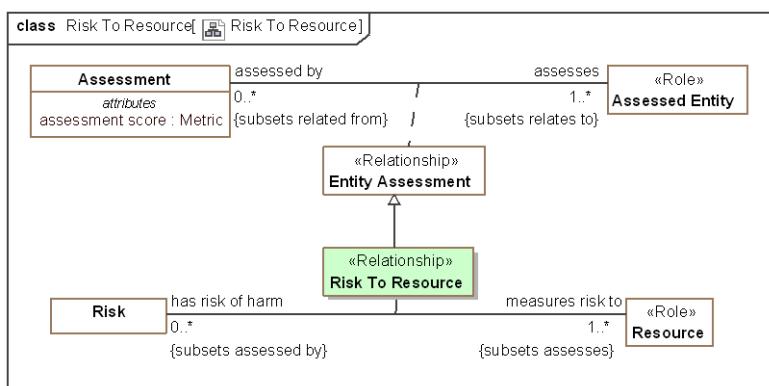


Figure 24. Risk To Resource

Direct Supertypes

[Entity Assessment](#)

Association Ends

 measures risk to : [Resource](#) [1..*] Redefines: objective of: [Stakeholder](#)

Resources (aka assets) at risk.

 has risk of harm : [Risk](#) [0..*] Redefines: objective of: [Stakeholder](#)

Potential risk to the subject resource.

8.9.128.8.12 Association Class Risk Topic <<Relationship>>

One or more undesirable situations that are assessed together in terms of their risk - the impact and likelihood that those situations will cause harm to resources valued by a risk owner.

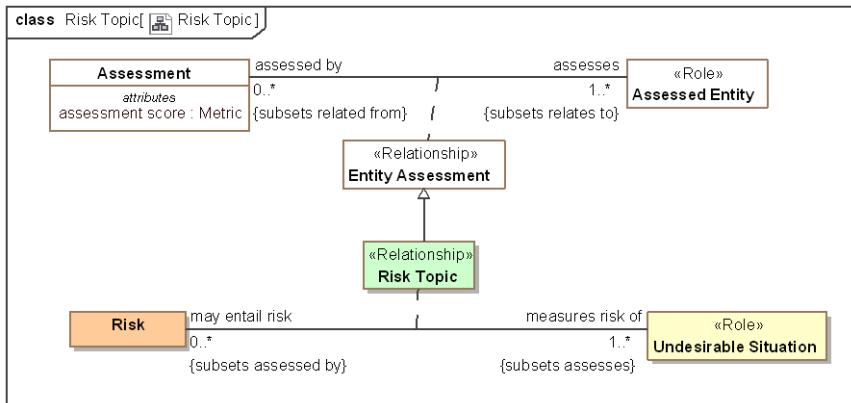


Figure 25. Risk Topic

Direct Supertypes

[Entity Assessment](#)

Association Ends

measures risk of : [Undesirable Situation](#) [1..*] *Redefines:* objective of: [Stakeholder](#)

Undesirable situations measured in terms of their risk of harming resources valued by a risk owner.

may entail risk : [Risk](#) [0..*] *Redefines:* objective of: [Stakeholder](#)

Risk resulting from a situation happening where the situation may cause harm to resources valued by a risk owner.

8.9.138.8.13 Association Class Stakeholder Risk <<Relationship>>

A relationship representing the impact of risk owned by a risk owner. The impact may be ranked as part of risk assessment.

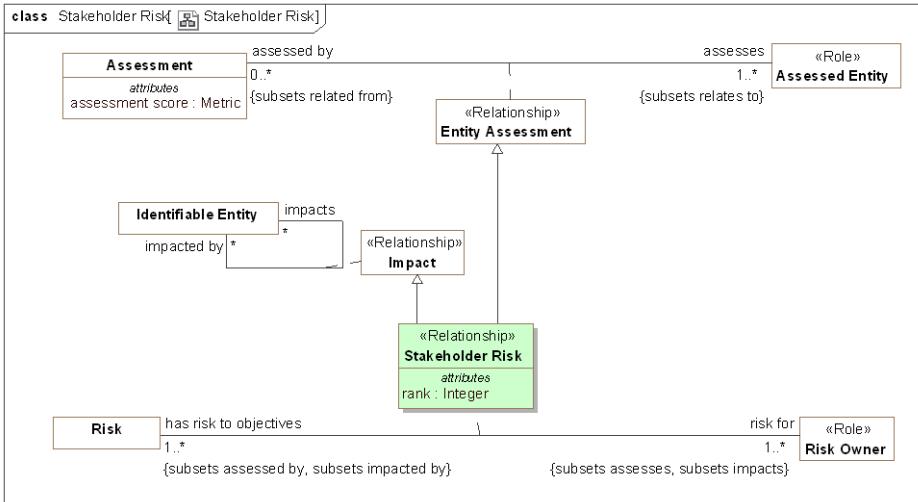


Figure 26. Stakeholder Risk

Direct Supertypes

[Entity Assessment](#), [Impact](#)

Association Ends

█ risk for : [Risk Owner](#) [1..*] *Redefines:* objective of: [Stakeholder](#)

Owner of a risk. The risk owner has objectives to minimize the subject risk.

█ has risk to objectives : [Risk](#) [1..*] *Redefines:* objective of: [Stakeholder](#)

Risk owned by a risk owner such that the risk may impact the risk owners objectives.

Attributes

◊ rank : [Integer](#)

An ordering of how important a risk is relative to all the risks of a risk stakeholder. How the rank is computed is usually determined by net risk but is not specified in this specification.

8.9.148.8.14 Class Threat Likelihood <<Quantity Kind>>

A metric representing the likelihood of a threat occurring.

Direct Supertypes

[Probability Metric](#)

8.9.158.8.15Association Class Valuation of Asset <<Relationship>>

A relationship representing the set of valued assets for a stakeholder's objectives.

Association Ends

 values : [Valued Asset](#) [*] Redefines: objective of: [Stakeholder](#)

An asset for which there is an objective to create, sustain, or protect the asset.

 supported by : [Objective to Protect Assets](#) [*] Redefines: objective of: [Stakeholder](#)

An objective that supports the creation, sustainment, or safety of a valued asset.

Attributes

 sensitivity threshhold : [Metric](#) [0..1]

A metric representing the threshold over which damage to an asset will be of concern to a risk stakeholder.

Associations

 <<Involves>> sensitive to objective : [Objective forSafety and Security](#) [*] Subsets: achieves:[Objective](#)

Objectives that directly justify the valuing of specific assets.

8.9.168.8.16Class Valued Asset <<Role>>

A system, organization, thing, process or person that is the direct concern of a stakeholder.

[BMM] Asset: something of value owned by the enterprise

Direct Supertypes

[Resource](#)

Attributes

 replacement cost : [Currency](#) [0..1]

Cost to replace the capability offered by the subject valued asset. This may or may not be the cost to replace the asset with an identical one.

Associations

 supported by : [Objective to Protect Assets](#) [*] Subsets: relates to:[Identifiable Entity](#)
through association: [Valuation of Asset](#)

An objective that supports the creation, sustainment, or safety of a valued asset.

8.9.1648.8.161Enumeration Likelihood Categories

A high-level scale of likelihood.

Direct Known Superclasses

Scale

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk  
public enum Likelihood Categories  
{Frequent, Probable, Occasional, Remote, Improbable}
```

Literals

- ◊ Frequent

Likely to occur often in the life of an item, with a probability of Event greater than 10:1 in that life.

- ◊ Probable

Will occur several times in the life of an item, with a probability of Event less than 10:1 but greater than 10:2 in that life.

- ◊ Occasional

Likely to occur sometime in the life of an item, with a probability of Event less than 10:2 but greater than 10:3 in that life.

- ◊ Remote

Unlikely but possible to occur in the life of an item, with a probability of Event less than 10:3 but greater than 10:6 in that life.

- ◊ Improbable

So unlikely, it can be assumed Event may not be experienced, with a probability of Event less than 10:6 in that life.

8.9.162**8.8.162**Enumeration Severity Categories

A high-level scale of severity.

Direct Known Superclasses

Scale

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk  
public enum Severity Categories  
{Catastrophic, Critical, Marginal, Negligible}
```

Literals

- ◊ Catastrophic

Could result in death, permanent total disability, loss exceeding \$1M, or irreversible severe environmental damage that violates law or regulation.

● Critical

Could result in permanent partial disability, injuries, or occupational illness that may result in hospitalization of at least three personnel, loss exceeding \$200K but less than \$1M, or reversible environmental damage causing a violation of law or regulation.

● Marginal

Could result in injury or occupational illness resulting in one or more lost work day(s), loss exceeding \$10K but less than \$200K, or mitigable environmental damage without violation of law or regulation where restoration activities can be accomplished.

● Negligible

Could result in injury or illness not resulting in a lost work day, loss exceeding \$2K but less than \$10K, or minimal environmental damage not violating law or regulation.

Known other enumerations

[Enumeration Likelihood Categories](#), [Enumeration Severity Categories](#)

8.108.9 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments

Concepts relative to risk treatment. Risk treatments lessen the likelihood or impact of undesirable situations.

8.10.18.9.1 Diagram: Risk Treatment

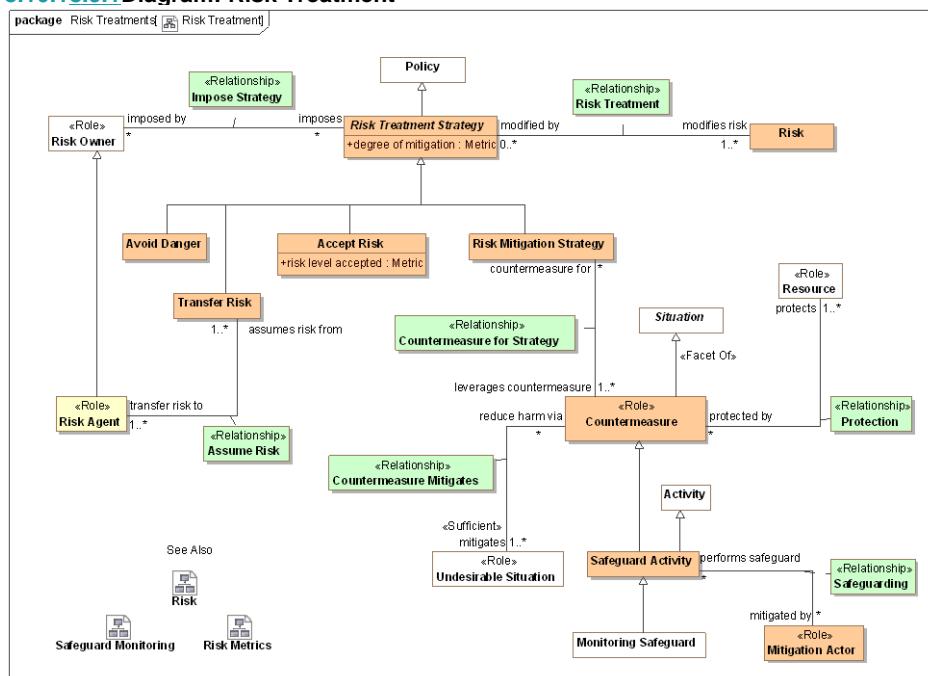


Figure 27. Risk Treatment

8.10.28.9.2Diagram: Safeguard Monitoring

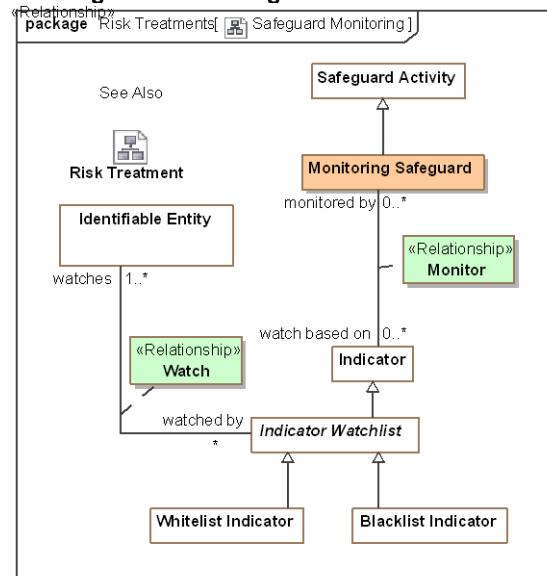


Figure 28. Safeguard Monitoring

8.10.38.9.3Association Class Assume Risk <<Relationship>>

A relationship defining the stakeholder assuming a risk for another as part of a risk transfer risk strategy.

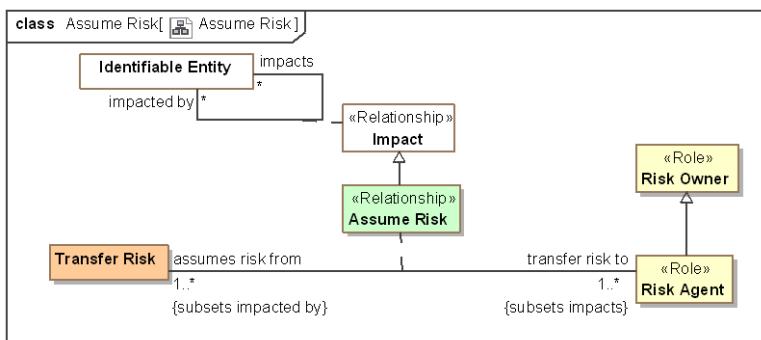


Figure 29. Assume Risk

Direct Supertypes

[Impact](#)

Association Ends

 transfer risk to : [Risk Agent](#) [1..*] Subsets: relates to:[Identifiable Entity](#)

Stakeholder that assumes a risk as the result of a transfer risk action.

 assumes risk from : [Transfer Risk](#) [1..*] Subsets: relates to:[Identifiable Entity](#)

The stakeholder that assumes a risk for another, such as an insurance company.

8.10.48.9.4 Class Avoid Danger

A likelihood reduction strategy whereby a stakeholder decides not to engage in a risky activity.

Direct Supertypes

[Risk Treatment Strategy](#)

8.10.58.9.5 Class Countermeasure <>Role>>

Countermeasure is a role of a situation to protect resources thus mitigating risk as part of a risk mitigation strategy.

Direct Supertypes

[Resource](#), [Situation](#)

Associations

 protects : [Resource](#) [1..*] Subsets: supports:[Resource](#)
through association: [Protection](#)

Resource protected by a countermeasure such that the risk to the resource is reduced. Note that resources include actors, people, organizations and things.

 <>Sufficient>> mitigates : [Undesirable Situation](#) [1..*] Subsets: impacts:[Identifiable Entity](#)
through association: [Countermeasure Mitigates](#)

Undesirable situation for which mitigation reduces the likelihood or impact.

 countermeasure for : [Risk Mitigation Strategy](#) [*] Subsets: used by:[Event](#)
through association: [Countermeasure for Strategy](#)

Mitigation strategy supported by a countermeasure.

8.10.68.9.6 Association Class Countermeasure for Strategy <>Relationship>>

Countermeasure for strategy defines a specific <leverages countermeasure> countermeasure that helps to mitigate risk as part of a <countermeasure for> risk mitigation strategy.

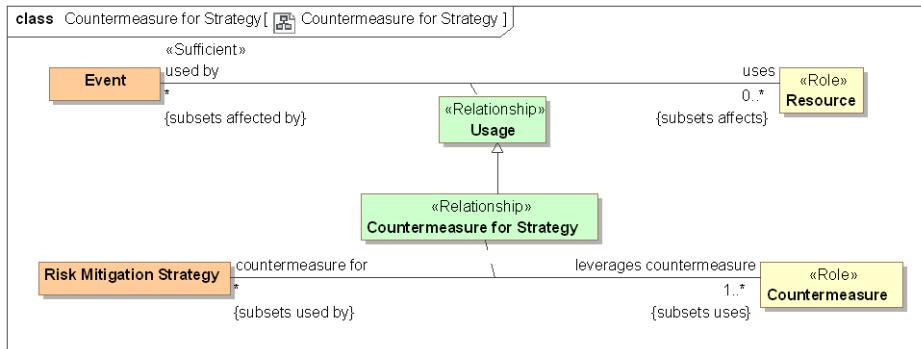


Figure 30. Countermeasure for Strategy

Direct Supertypes

Usage

Association Ends

█ leverages countermeasure : [Countermeasure](#) [1..*] Subsets: used by:[Event](#)

Countermeasure which serves a risk mitigation strategy.

█ countermeasure for : [Risk Mitigation Strategy](#) [*] Subsets: used by:[Event](#)

Mitigation strategy supported by a countermeasure.

8.10.78.9.7 Association Class Countermeasure Mitigates <>Relationship>>

Undesirable situations mitigated by a countermeasure.

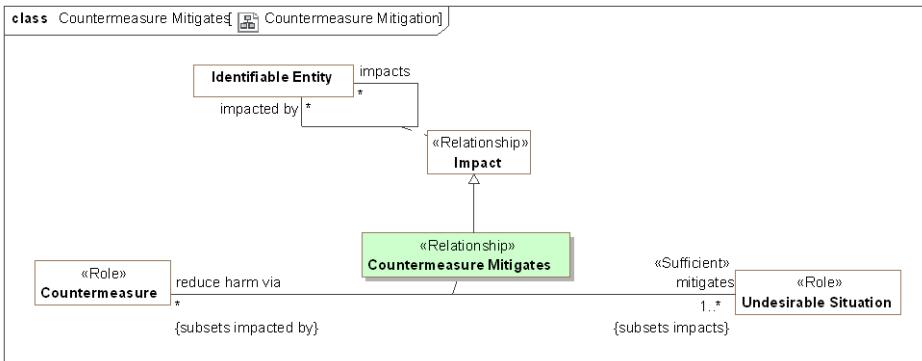


Figure 31. Countermeasure Mitigation

Direct Supertypes

[Impact](#)

Associations Ends

reduce harm via : [Countermeasure](#) [*] Subsets: used by:[Event](#)

An actual or potential response to a danger to minimize the impact of the subject undesirable situation.

mitigates : [Undesirable Situation](#) [1..*] Subsets: used by:[Event](#)

Undesirable situation for which mitigation reduces the likelihood or impact.

8.10.88.9.8 Class Mitigation Actor <<Role>>

Actor that performs a mitigation.

Direct Supertypes

[Actor](#), [Resource](#)

Associations

performs safeguard : [Safeguard Activity](#) [*] Subsets: performs:[Activity](#)
through association: [Safeguarding](#)

An activity a mitigation actor performs to protect resources identified by <protects>.

8.10.98.9.9 Association Class Monitor <<Relationship>>

Monitor relates the <monitored by> safeguard with a <watch based on> indicator such that the monitoring of the indicator becomes a safeguard that <protects> resources.

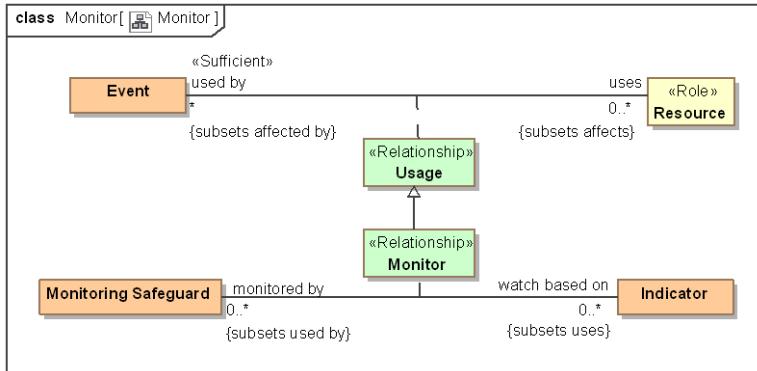


Figure 32. Monitor

Direct Supertypes

[Usage](#)

Association Ends

watch based on : [Indicator](#) [0..*] Subsets: performs:[Activity](#)

Indicators watched by the subject safeguard.

monitored by : [Monitoring Safeguard](#) [0..*] Subsets: performs:[Activity](#)

Activities monitoring an indicator using a monitoring safeguard.

8.10.108.9.10 Class Monitoring Safeguard

The action or process of observing something or someone based on well-defined indicators so as to mitigate risks.

Direct Supertypes

[Safeguard Activity](#)

Associations

watch based on : [Indicator](#) [0..*] Subsets: uses:[Resource](#)

through association: [Monitor](#)

Indicators watched by the subject safeguard.

8.10.1148.9.11 Association Class Protection <<Relationship>>

The protection of a resource by a countermeasure.

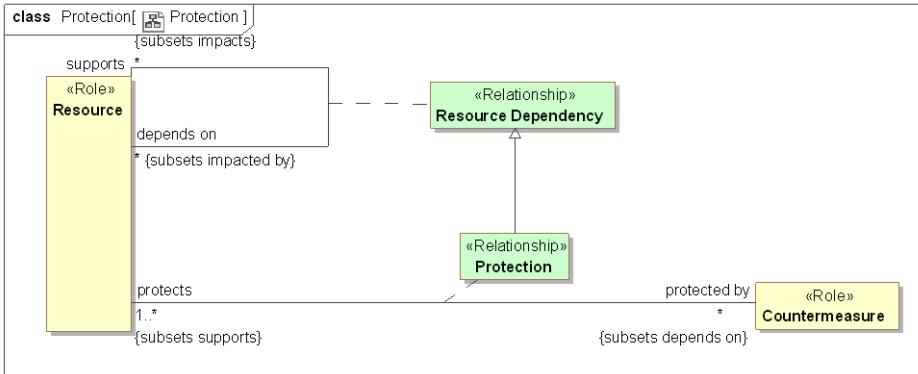


Figure 33. Protection

Direct Supertypes

[Resource Dependency](#)

Association Ends

protects : [Resource](#) [1..*] Subsets: uses:[Resource](#)

Resource protected by a countermeasure such that the risk to the resource is reduced. Note that resources include actors, people, organizations and things.

protected by : [Countermeasure](#) [*] Subsets: uses:[Resource](#)

Countermeasure that protects the subject resource.

8.10.428.9.12 Class Risk Agent <<Role>>

An entity that assumes risk on behalf of another. e.g. an insurance company.

Direct Supertypes

[Risk Owner](#)

Associations

assumes risk from : [Transfer Risk](#) [1..*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Assume Risk](#)

The stakeholder that assumes a risk for another, such as an insurance company.

8.10.138.9.13Association Class Risk Treatment <<Relationship>>

Risk treatment connects a <modified by> risk treatment strategy with the <modifies risk> Risk that it is intended to reduce.

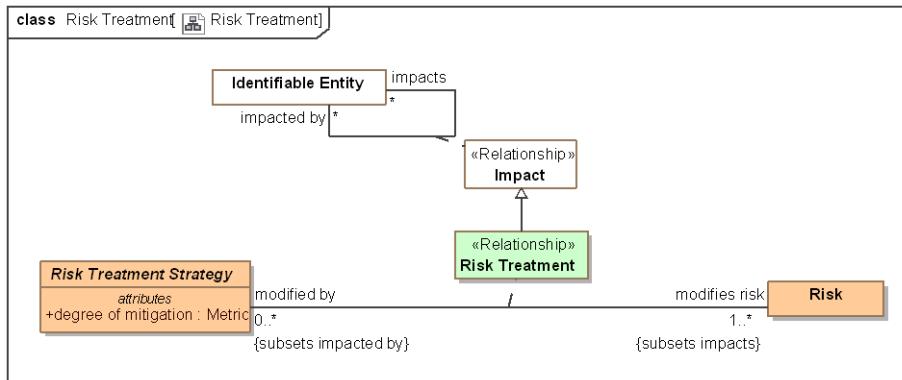


Figure 34. Risk Treatment

Direct Supertypes

[Impact](#)

Association Ends

[modifies risk](#) : [Risk](#) [1..*] Subsets: impacted by: [Identifiable Entity](#)

Risk that a risk treatment strategy reduces for the risk owner.

[modified by](#) : [Risk Treatment Strategy](#) [0..*] Subsets: impacted by: [Identifiable Entity](#)

A strategy to reduce the subject risk for the risk owner.

8.10.148.9.14Class Risk Treatment Strategy

A plan, method or process for dealing with risk by reducing the likelihood or impact.

Direct Supertypes

[Policy](#)

Attributes

[degree of mitigation](#) : [Metric](#)

A metric for how much a mitigation reduces the likelihood or impact of an undesirable situation.

Associations

[modifies risk](#) : [Risk](#) [1..*] Subsets: impacts: [Identifiable Entity](#)

through association: [Risk Treatment](#)

Risk that a risk treatment strategy reduces for the risk owner.

imposed by : [Risk Owner](#) [*] Subsets: asserted by:[Authority](#)
through association: [Impose Strategy](#)

Authority that imposes a risk strategy such that it is intended to reduce their risk.

8.10.158.9.15 Class Safeguard Activity

An activity of mitigating, or lessening the force or intensity of an undesired situation.

Direct Supertypes

[Activity](#), [Countermeasure](#)

Associations

mitigated by : [Mitigation Actor](#) [*] Subsets: performed by:[Actor](#)
through association: [Safeguarding](#)

The actor(s) that perform an activity to safeguard resources.

8.10.168.9.16 Association Class Safeguarding <<Relationship>>

The safeguarding relationship relates a <mitigated by> mitigation actor with a <performs safeguard> safeguard activity such that it <protects> resources.

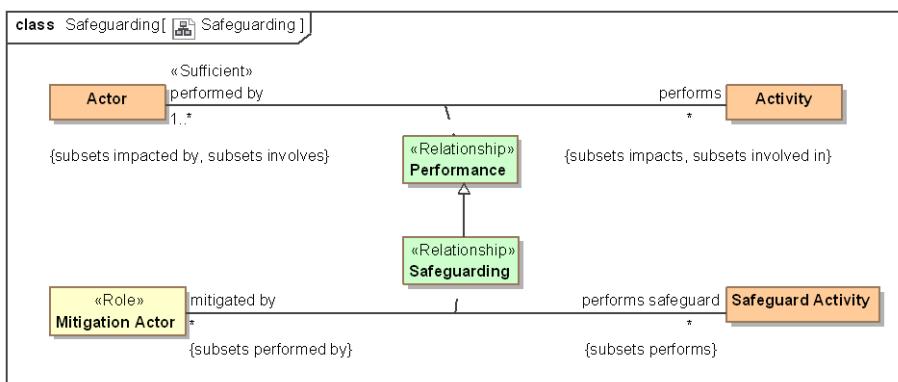


Figure 35. Safeguarding

Direct Supertypes

[Performance](#)

Association Ends

 performs safeguard : [Safeguard Activity](#) [*] Subsets: performed by:[Actor](#)

An activity a mitigation actor performs to protect resources identified by <protects>.

 mitigated by : [Mitigation Actor](#) [*] Subsets: performed by:[Actor](#)

The actor(s) that perform an activity to safeguard resources.

8.10.17 8.9.17 Class Transfer Risk

A strategy to cause another to assume the impact of a risk. e.g., insurance.

Direct Supertypes

[Risk Treatment Strategy](#)

Associations

 transfer risk to : [Risk Agent](#) [1..*] Subsets: impacts:[Identifiable Entity](#)
through association: [Assume Risk](#)

Stakeholder that assumes a risk as the result of a transfer risk action.

8.118.10 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Threat Actors

8.11.18.10.1 Diagram: Threat Actors

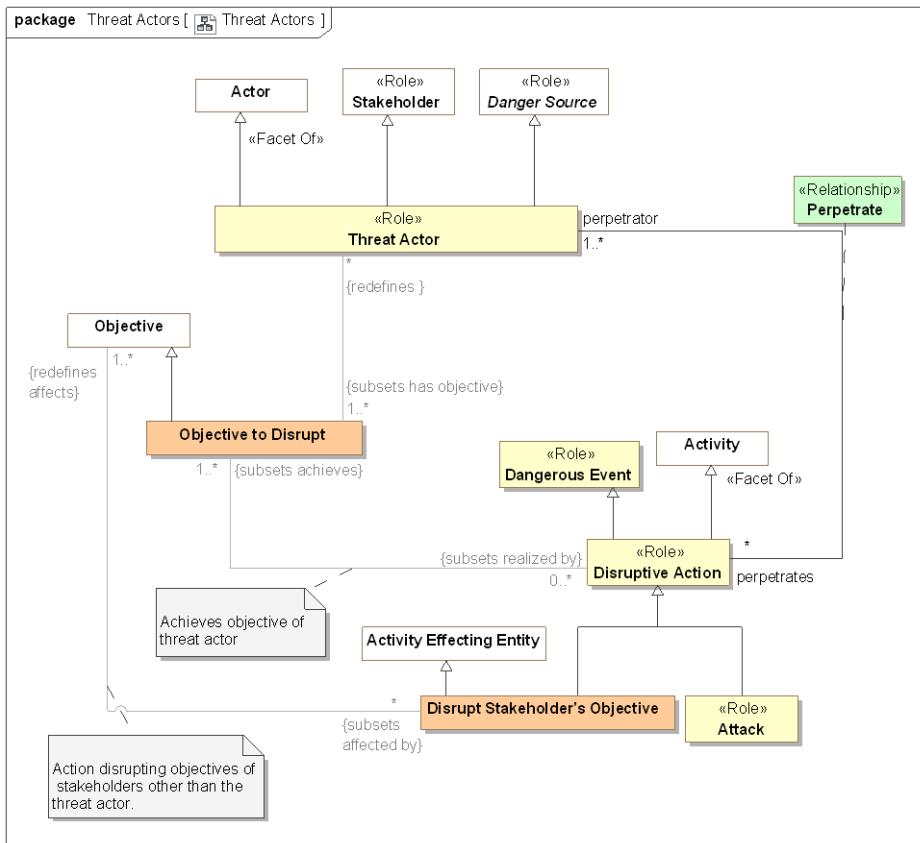


Figure 36. Threat Actors

8.11.28.10.2 Class Disruptive Action <>Role>>

An intentional activity that serves the objectives of a threat actor to cause harm. Some disruptive actions are threats.

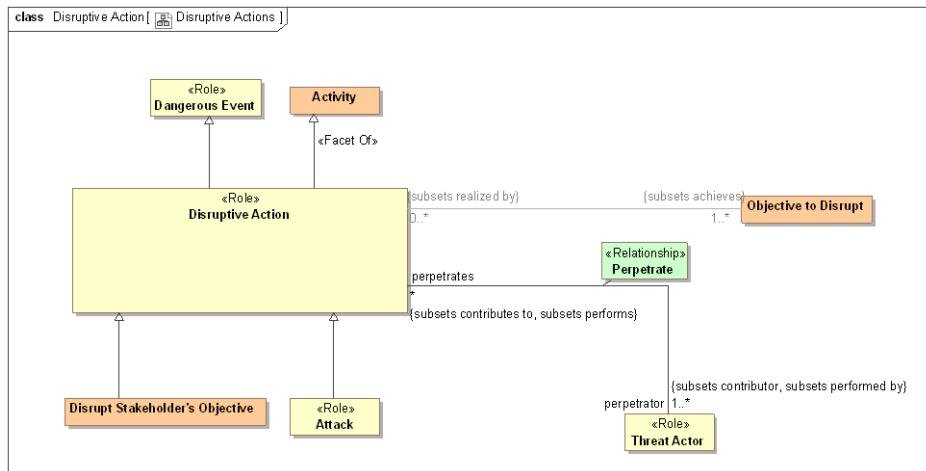


Figure 37. Disruptive Actions

Direct Supertypes

[Activity](#), [Dangerous Event](#)

Associations

<<Restriction>> : [Objective to Disrupt](#) [1..*] Subsets: achieves:[Objective](#).

A threat objective of a disruptive action.

perpetrator : [Threat Actor](#) [1..*] Subsets: performed by:[Actor](#) contributor:[Danger Source](#)
through association: [Perpetrate](#)

The threat actor performing an activity to cause or contribute to an attack.

8.11.38.10.3 Association Class Perpetrate <>Relationship>>

An actor involved in perpetrating an attack or other disruptive action.

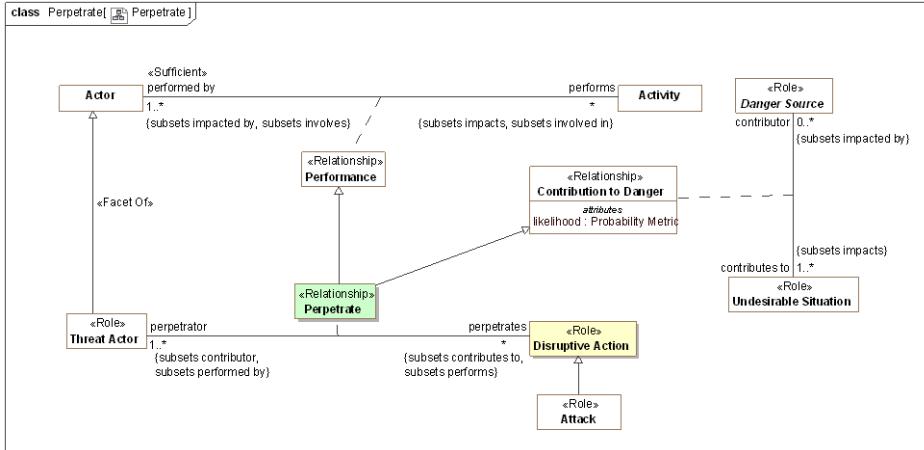


Figure 38. Perpetrate

Direct Supertypes

[Contribution to Danger](#), [Performance](#)

Associations Ends

perpetrates : [Disruptive Action](#) [*] Subsets: performed by:[Actor](#) contributor:[Danger Source](#)

The activity performed by a threat actor to cause or contribute to an attack.

perpetrator : [Threat Actor](#) [1..*] Subsets: performed by:[Actor](#) contributor:[Danger Source](#)

The threat actor performing an activity to cause or contribute to an attack.

8.11.48.10.4 Class Threat Actor <<Role>>

Role of an actor; all or partially responsible for some undesired situation - threat, risk, or attack. Threat actors have intent to do harm.

Direct Supertypes

[Actor](#), [Danger Source](#), [Stakeholder](#)

Associations

<<Restriction>> : [Objective to Disrupt](#) [1..*] Subsets: has objective:[Objective](#)

An objective that a threat actor intends to retain or achieve.

perpetrates : [Disruptive Action](#) [*] Subsets: performs:[Activity](#) contributes to:[Undesirable Situation](#)
through association: [Perpetrate](#)

The activity performed by a threat actor to cause or contribute to an attack.

8.128.11 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Undesirable Situations

Undesirable situations are a fundamentally concept that unifies the threat-risk framework. Undesirable situations classify a situation as one that causes harm to stakeholders (directly or indirectly). Undesirable situations are further specialized across three dimensions:

- Events Vs. Conditions - Events "happen" whereas conditions are a steady state for some period.
- Actual Vs. Potential.
- Intentional Vs. Natural or Systematic. Intentional dangers involve a "threat actor" whereas unintentional only involve weaknesses in resources.

The above are used to define more specific risk & threat concepts, such as:

- Incidents which are actual dangerous situations.
- Disasters and Accidents which are unintentional actual situation (no threat actor).
- Attacks which are actual situations perpetrated by a threat actor.
- Risks which are potential dangerous situations, thus having some level of uncertainty.
- Threats which are intentional risks from a threat actor.
- Hazards which are natural or systematic risks.

Resources also play an important role in the risk/threat framework in that resources are harmed by dangers but risks are also important for attackers to exploit vulnerabilities and for defenders to realize mitigations.

8.12.18.11.1 Diagram: Undesirable Situations

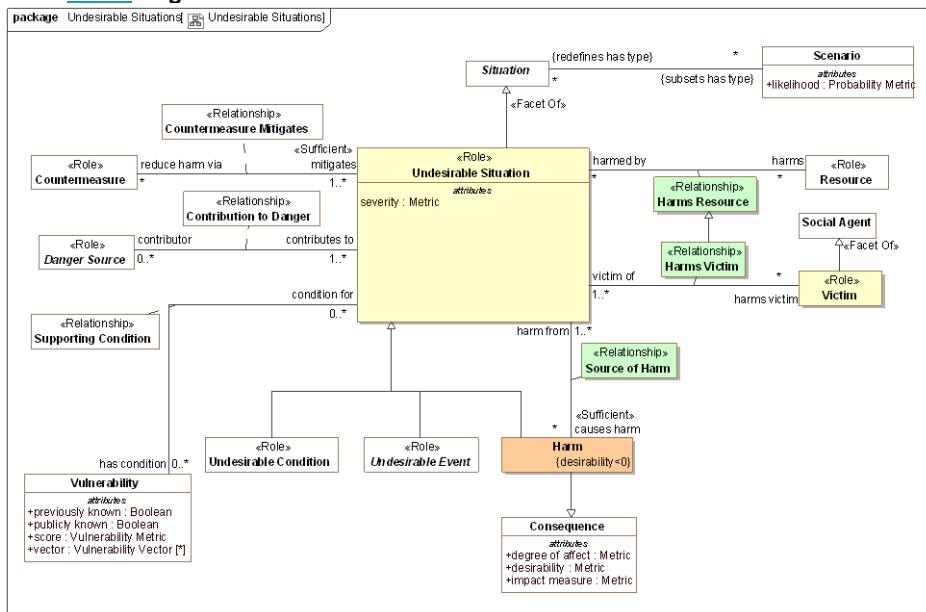


Figure 39. Undesirable Situations

8.12.28.11.2 Class Harm

Harm is a consequence of a situation that negatively impacts the objectives of stakeholders and therefore has negative desirability for those stakeholders.

[Firesmith 2003] Harm is a negative impact associated with an asset. Harm is due to an accident when dealing with safety requirements, is due to an attack when dealing with security requirements, and may be due to both accidents and attacks when dealing with survivability requirements.

[NIEM] Injury (More specific concept - Person specific).

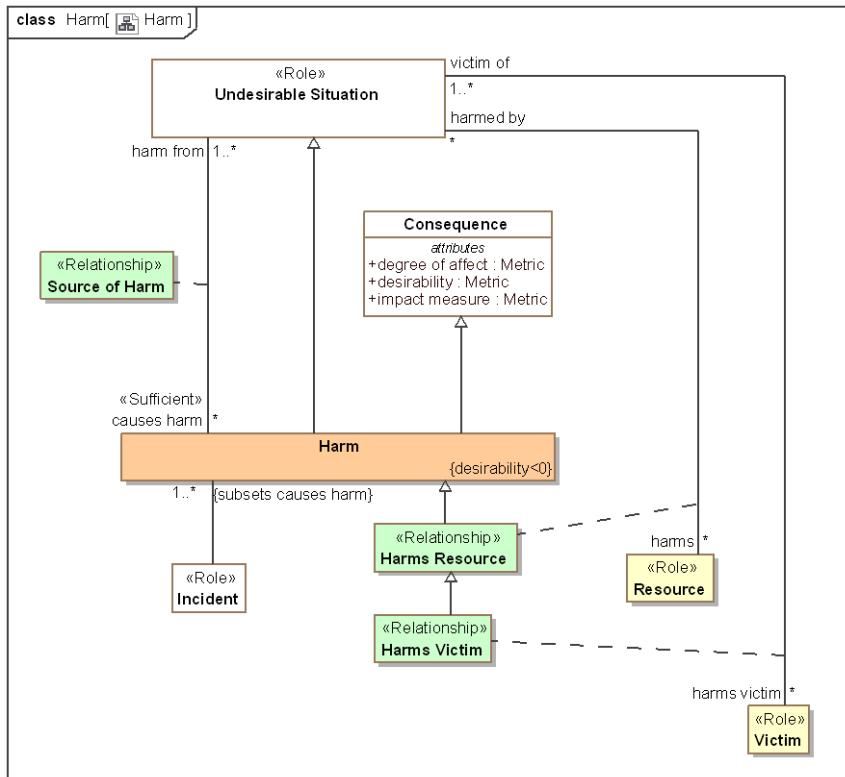


Figure 40. Harm

Direct Supertypes

[Consequence](#), [Undesirable Situation](#)

Associations

 harm from : [Undesirable Situation](#) [1..*] Subsets: results from:[Situation](#)
through association: [Source of Harm](#)

Situation which contributes to harm.

 : [Incident](#)

8.12.38.11.3 Association Class Harms Resource <<Relationship>>

Resources harmed or potentially harmed by an undesirable situation.

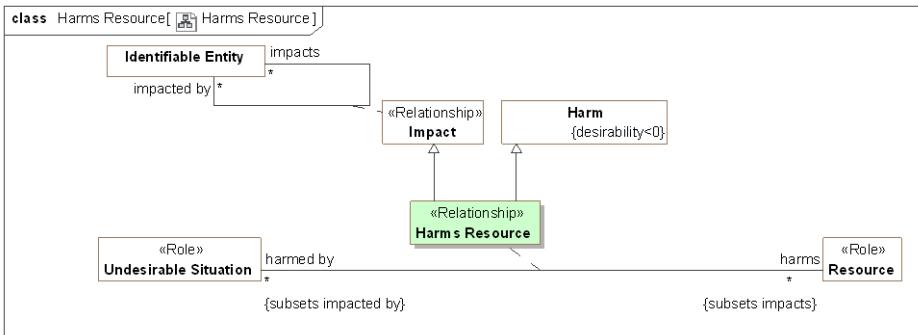


Figure 41. Harms Resource

Direct Supertypes

[Harm](#), [Impact](#)

Association Ends

- █ harms : [Resource](#) [*]
- █ harmed by : [Undesirable Situation](#) [*]

Attributes

- ◊ likelihood : [Probability Metric](#)

8.12.48.11.4 Association Class Harms Victim <>Relationship>>

People or organizations (social agents) harmed or potentially harmed by an undesirable situation.

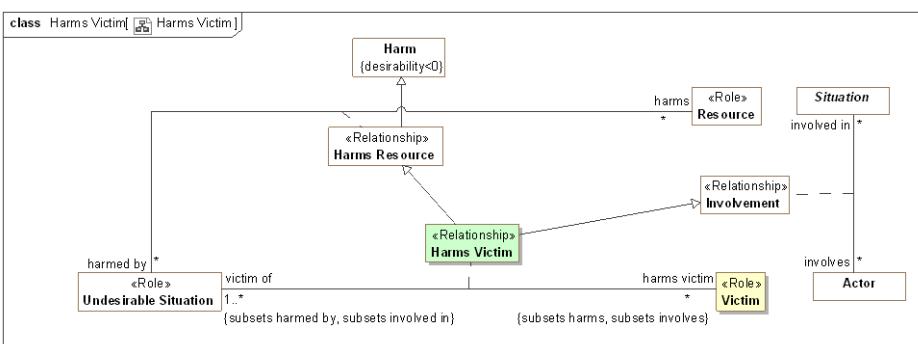


Figure 42. Harms Victim

Direct Supertypes

Harms Resource, Involvement

Association Ends

harms victim : [Victim](#) [*]

Victim harmed by a situation.

victim of : [Undesirable Situation](#) [1..*]

Situations for which the subject is a victim.

8.12.58.11.5 Association Class Source of Harm <>Relationship>>

Relationship describing the harm produced as a result of a situation.

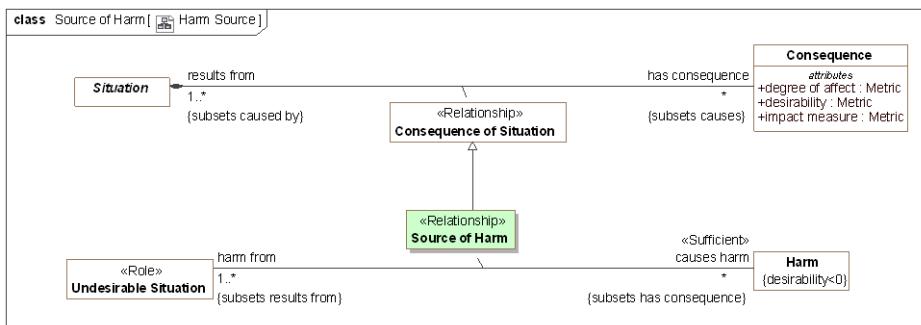


Figure 43. Harm Source

Direct Supertypes

Consequence of Situation

Association Ends

causes harm : [Harm](#) [*]

The harm to a resource caused by a undesirable situation.

harm from : [Undesirable Situation](#) [1..*]

Situation which contributes to harm.

8.12.68.11.6 Class Undesirable Condition <>Role>>

A role of a situation as an undesirable static situation (a condition, not something happening) that directly or indirectly does or may have detrimental consequences impacting the objectives of stakeholders.

Direct Supertypes

[State](#), [Undesirable Situation](#)

[8.12.78.11.7 Class Undesirable Event <>Role>>](#)

A role of an Event that may directly or indirectly cause harm.

Direct Supertypes

[Event](#), [Undesirable Situation](#)

[8.12.88.11.8 Class Undesirable Situation <>Role>>](#)

An undesirable situation is a role of a situation (condition or event) that has, is, or may cause harm (directly or indirectly). Undesirable situations negatively impact the objectives of stakeholders. An undesirable situation may be classified in the context of the impacted stakeholders - what is undesirable to one stakeholder may be desirable to another.

Direct Supertypes

[Situation](#)

Attributes

severity : [Metric](#)

A metric for the total harm caused by a undesirable situation.

Associations

causes harm : [Harm](#) [*] Subsets: has consequence:[Consequence](#)
through association: [Source of Harm](#)

The harm to a resource caused by a undesirable situation.

harms : [Resource](#) [*] Subsets: impacts:[Identifiable Entity](#)
through association: [Harms Resource](#)
harms victim : [Victim](#) [*] Subsets: involves:[Actor](#) harms:[Resource](#)
through association: [Harms Victim](#)

Victim harmed by a situation.

has condition : [Vulnerability](#) [0..*] Subsets: caused by:[Situation](#)
through association: [Supporting Condition](#)

A vulnerability as a condition for the a undesirable condition to occur.

<> reduce harm via : [Countermeasure](#) [*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Countermeasure Mitigates](#)

An actual or potential response to a danger to minimize the impact of the subject undesirable situation.

 may entail risk : [Risk](#) [0..*] Subsets: assessed by:[Assessment](#)
through association: [Risk Topic](#)

Risk resulting from a situation happening where the situation may cause harm to resources valued by a risk owner.

 contributor : [Danger Source](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Contribution to Danger](#)

A danger source that can contribute to the possibility of an undesirable situation occurring.

8.12.98.11.9 Class Victim <>Role>>

The role of any actor harmed by an incident.

Direct Supertypes

[Social Agent](#), [Valued Asset](#)

Associations

 victim of : [Undesirable Situation](#) [1..*] Subsets: involved in:[Situation](#) harmed by:[Undesirable Situation](#)
through association: [Harms Victim](#)

Situations for which the subject is a victim.

8.138.12 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

Vulnerabilities and weaknesses represent flaws or inherent qualities of some resource that can be the source of danger.

8.13.48.12.1 Diagram: Vulnerability

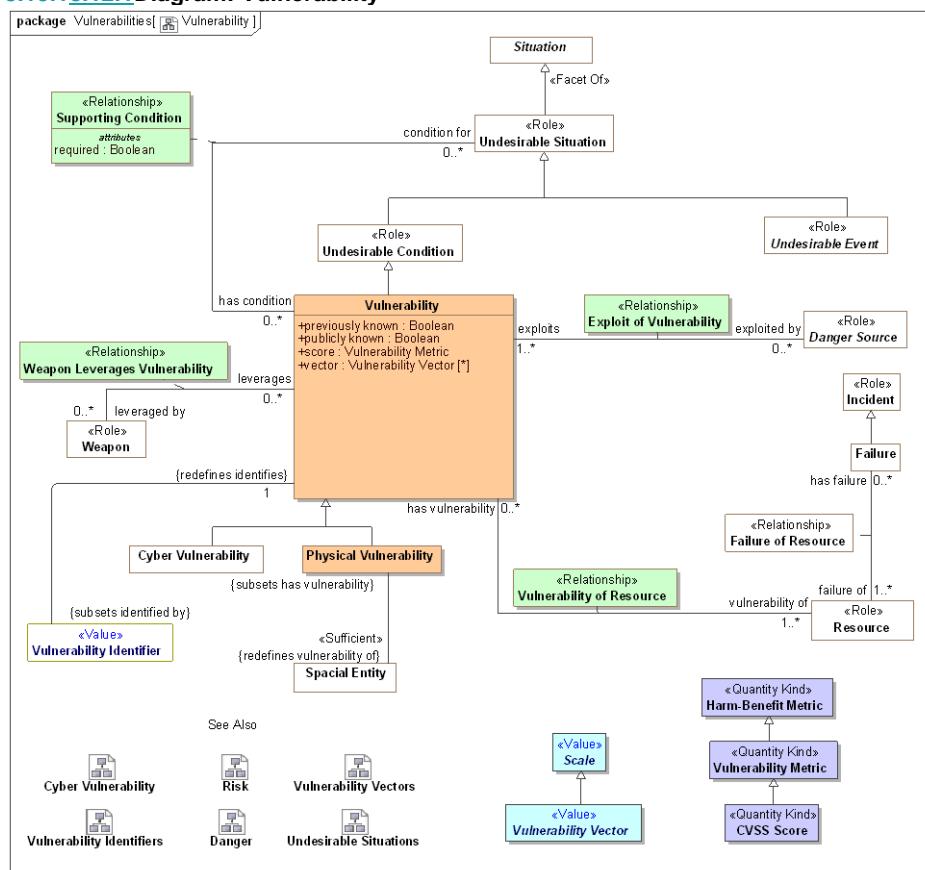


Figure 44. Vulnerability

8.13.28.12.2Diagram: Vulnerability Identifiers

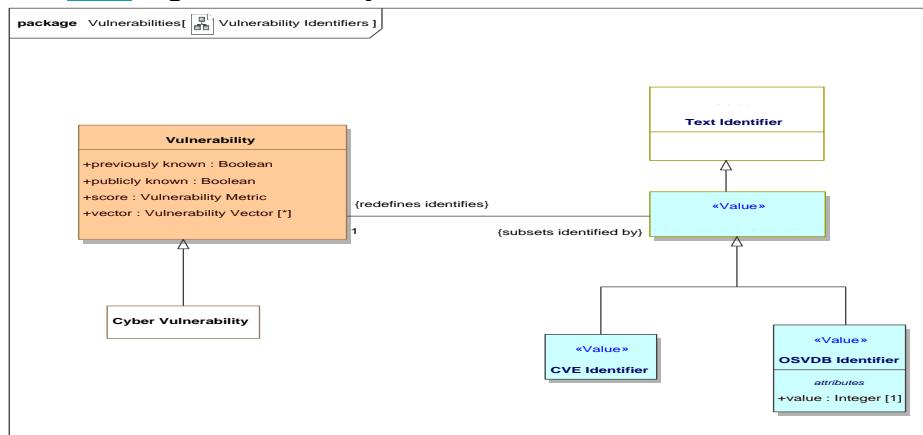


Figure 45. Vulnerability Identifiers

8.13.38.12.3Class Physical Vulnerability

A category of vulnerability of something to physical danger or attack.

Direct Supertypes

[Vulnerability](#)

Associations

/ <<Sufficient>> : Spacial Entity Redefines: vulnerability of:Resource

8.13.48.12.4Association Class Supporting Condition <<Relationship>>

Vulnerabilities required to exist for a threat to transition to an incident.

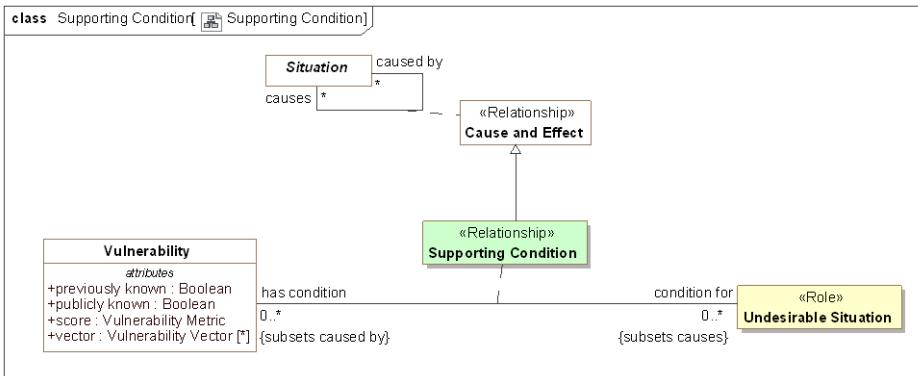


Figure 46. Supporting Condition

Direct Supertypes

[Cause and Effect](#)

Association Ends

condition for : [Undesirable Situation](#) [0..*] *Redefines:* vulnerability of: [Resource](#)

Incident or failure for which a vulnerability is a condition.

has condition : [Vulnerability](#) [0..*] *Redefines:* vulnerability of: [Resource](#)

A vulnerability as a condition for the a undesirable condition to occur.

Attributes

required : [Boolean](#)

True if the condition is required for the undesirable condition to occur, false if the condition is one of many conditions that may enable the undesirable situation.

8.13.58.12.5 Class Vulnerability

A Vulnerability (of an object and a cause of failure, i.e. attack, natural cause, mistake, natural cause, accidental cause, or indirect) is the set of conditions under which an object fails under the particular cause of failure.

This is consistent with NIST 800-30 (based on CNSSII 4009)

Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Direct Supertypes

[Undesirable Condition](#)

Attributes

- ◊ previously known : [Boolean](#)

At the time of the latest vulnerability characterization, true if the vulnerability had been previously reported, false if newly discovered or "zero day". Time is recorded in the "starts on" property of vulnerability.

- ◊ publicly known : [Boolean](#)

An assertion that the existence of vulnerability is public knowledge, not closely held within an organization.

- ◊ score : [Vulnerability Metric](#)

Score for the severity of the subject vulnerability - may use CVSS or other metrics.

- ◊ vector : [Vulnerability Vector](#) [*]

Factors influencing the subject vulnerability's score.

Associations

- / : [Vulnerability Identifier](#) Subsets: identified by:[Identifier](#)

- █ condition for : [Undesirable Situation](#) [0..*] Subsets: causes:[Situation](#)
through association: [Supporting Condition](#)

Incident or failure for which a vulnerability is a condition.

- █ vulnerability of : [Resource](#) [1..*] Subsets: impacts:[Identifiable Entity](#)
through association: [Vulnerability of Resource](#)

Resource the subject vulnerability may impact.

- █ exploited by : [Danger Source](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Exploit of Vulnerability](#)

Danger source that can or did exploit a vulnerability such that it leads to an undesirable situation.

- █ leveraged by : [Weapon](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Weapon Leverages Vulnerability](#)

Weapon that can leverage a vulnerability to help an actor take advantage of that vulnerability.

8.13.68.12.6 Class Vulnerability Identifier <>Value>>

An identifier for a vulnerability.

Direct Supertypes

[Text Identifier](#)

Associations

- / : [Vulnerability](#) [1] Redefines: identifies:[Identifiable Entity](#)

8.13.78.12.7 Class Vulnerability Metric <<Quantity Kind>>

A metric representing the overall impact of a vulnerability.

Direct Supertypes

[Harm-Benefit Metric](#)

8.13.88.12.8 Association Class Vulnerability of Resource <<Relationship>>

Relationship defining the resources that have a particular vulnerability.

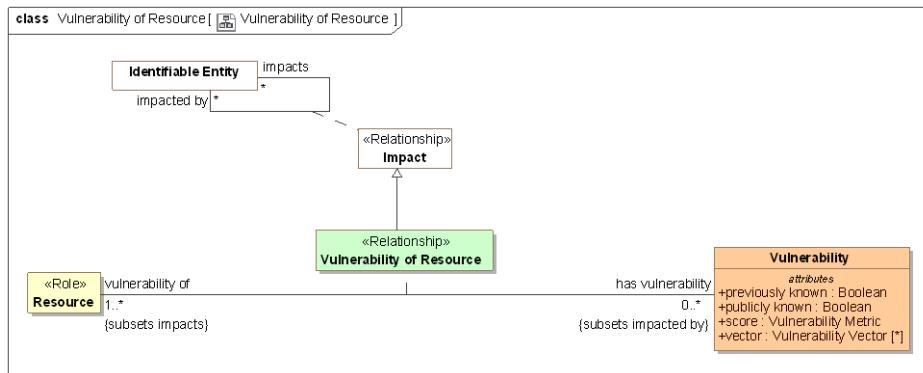


Figure 47. Vulnerability of Resource

Direct Supertypes

[Impact](#)

Association Ends

vulnerability of : [Resource](#) [1..*] *Redefines*: identifies: [Identifiable Entity](#)

Resource the subject vulnerability may impact.

has vulnerability : [Vulnerability](#) [0..*] *Redefines*: identifies: [Identifiable Entity](#)

Vulnerabilities of a resource, ways it may be compromised.

8.148.13 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Cyber Vulnerabilities

8.14.18.13.1 Diagram: Cyber Vulnerability

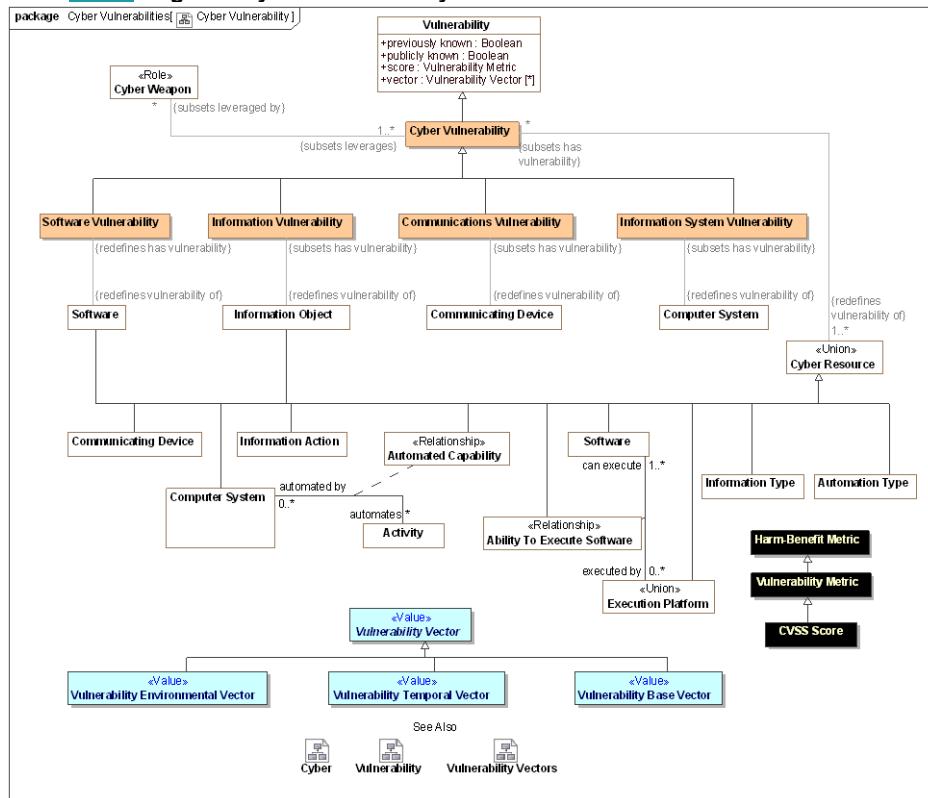


Figure 48. Cyber Vulnerability

8.14.28.13.2 Class Communications Vulnerability

A potential failure of a communications systems to restrict information flow to unintended parties.

Direct Supertypes

[Cyber Vulnerability](#)

Associations

/ <>Restriction>> : [Communicating Device](#) Redefines: vulnerability of:[Resource](#)

8.14.38.13.3 Class CVE Identifier <>Value>>

An identifier for Common Vulnerabilities and Exposures [<https://cve.mitre.org/>].

Direct Supertypes

[Vulnerability Identifier](#)

8.14.48.13.4 Class Cyber Vulnerability

A vulnerability of any cyber related resource.

Direct Supertypes

[Vulnerability](#)

Associations

/ <>Restriction>> : [Cyber Weapon](#) [*] Subsets: leveraged by:[Weapon](#)

/ <>Restriction>> : [Cyber Resource](#) [1..*] Redefines: vulnerability of:[Resource](#)

8.14.58.13.5 Class Information System Vulnerability

Category of vulnerability of a computer system and/or its network, software and execution of processes.

Direct Supertypes

[Cyber Vulnerability](#)

Associations

/ <>Restriction>> : [Computer System](#) Redefines: vulnerability of:[Resource](#)

8.14.68.13.6 Class Information Vulnerability

A category of vulnerability of information loss, misuse or corruption.

Direct Supertypes

[Cyber Vulnerability](#)

Associations

/ <>Restriction>> : [Information Object](#) Redefines: vulnerability of:[Resource](#)

8.14.78.13.7 Class OSVDB Identifier <>Value>>

OSVDB is an independent and open sourced web-based vulnerability database created for the security community.[<http://osvdb.org/>]. This package defines identifiers for referencing OSVDB.

Direct Supertypes

[Vulnerability Identifier](#)

Attributes

◊ value : [Integer](#) [1]

Index into the OSVDB database.

8.14.88.13.8 Class Software Vulnerability

A vulnerability of software such that the software such that the softwares operation is comprised.

Direct Supertypes

[Cyber Vulnerability](#)

Associations

/ <>Restriction>> : [Software](#) Redefines: vulnerability of:[Resource](#)

8.158.14 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability Vectors

[cvss] IT management must identify and assess vulnerabilities across many disparate hardware and software platforms. They need to prioritize these vulnerabilities and remediate those that pose the greatest risk. But when there are so many to fix, with each being scored using different scales, how can IT managers convert this mountain of vulnerability data into actionable information? The Common Vulnerability Scoring System (CVSS) is an open framework that addresses this issue. It offers the following benefits:

- Standardized Vulnerability Scores: When an organization normalizes vulnerability scores across all of its software and hardware platforms, it can leverage a single vulnerability management policy. This policy may be similar to a service level agreement (SLA) that states how quickly a particular vulnerability must be validated and remediated.
- Open Framework: Users can be confused when a vulnerability is assigned an arbitrary score. “Which properties gave it that score? How does it differ from the one released yesterday?” With CVSS, anyone can see the individual characteristics used to derive a score.
- Prioritized Risk: When the environmental score is computed, the vulnerability now becomes contextual. That is, vulnerability scores are now representative of the actual risk to an organization. Users know how important a given vulnerability is in relation to other vulnerabilities.

8.15.48.14.1Diagram: Vulnerability Vectors

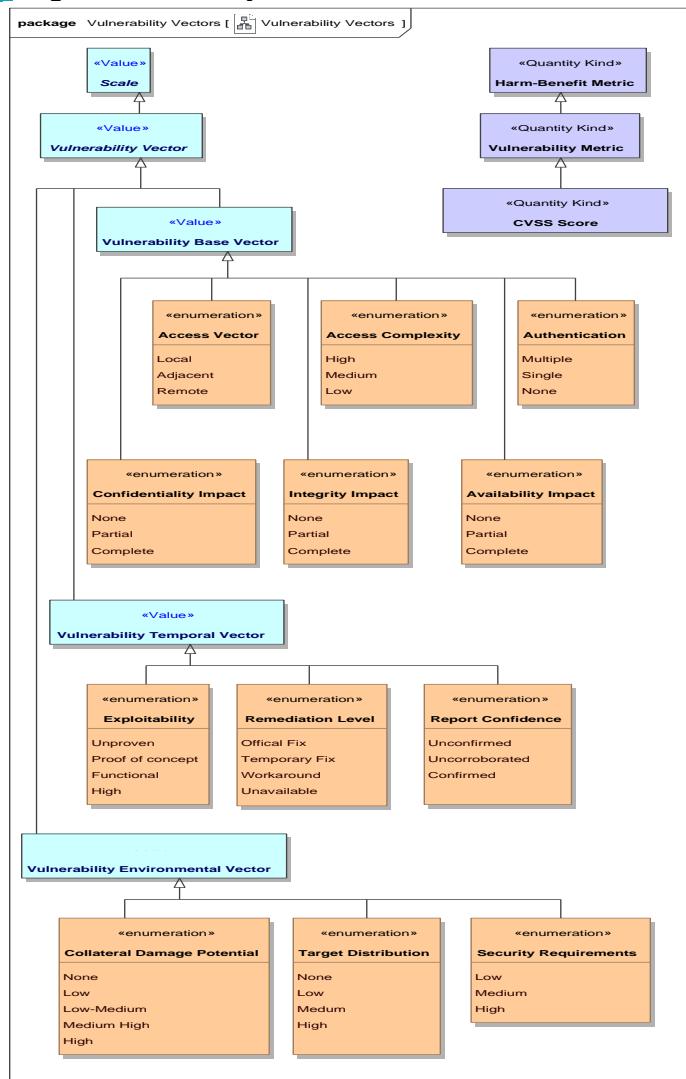


Figure 49. Vulnerability Vectors

8.15.28.14.2Class CVSS Score <<Quantity Kind>>

Common Vulnerability Scoring System. A number in the range of 0..10 representing a CVSS metric.
[CVSS]

Direct Supertypes

[Vulnerability Metric](#)

8.15.248.14.21Enumeration Access Complexity

[CVSS] This metric measures the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system. For example, consider a buffer overflow in an Internet service: once the target system is located, the attacker can launch an exploit at will. Other vulnerabilities, however, may require additional steps in order to be exploited. For example, a vulnerability in an email client is only exploited after the user downloads and opens a tainted attachment. The lower the required complexity, the higher the vulnerability score.

Direct Known Superclasses

[Vulnerability Base Vector](#)

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors
```

```
public enum Access Complexity  
{High, Medium, Low}
```

Literals

◎ High

Specialized access conditions exist. For example:

- In most configurations, the attacking party must already have elevated privileges or spoof additional systems in addition to the attacking system (e.g., DNS hijacking).
- The attack depends on social engineering methods that would be easily detected by knowledgeable people. For example, the victim must perform several suspicious or atypical actions.
- The vulnerable configuration is seen very rarely in practice.
- If a race condition exists, the window is very narrow.

◎ Medium

The access conditions are somewhat specialized; the following are examples:

- The attacking party is limited to a group of systems or users at some level of authorization, possibly untrusted.
- Some information must be gathered before a successful attack can be launched.
- The affected configuration is non-default, and is not commonly configured (e.g., a vulnerability present when a server performs user account authentication via a specific scheme, but not present for another authentication scheme).
- The attack requires a small amount of social engineering that might occasionally fool cautious users (e.g., phishing attacks that modify a web browser's status bar to show a false link, having to be on someone's "buddy" list before sending an IM exploit).

◎ Low

Specialized access conditions or extenuating circumstances do not exist. The following are examples:

- The affected product typically requires access to a wide range of systems and users, possibly anonymous and untrusted (e.g., Internet-facing web or mail server).
- The affected configuration is default or ubiquitous.
- The attack can be performed manually and requires little skill or additional information gathering.
- The “race condition” is a lazy one (i.e., it is technically a race but easily winnable).

[8.15.228.14.22](#) Enumeration Access Vector

[CVSS] This metric reflects how the vulnerability is exploited. The more remote an attacker can be to attack a host, the greater the vulnerability score.

Direct Known Superclasses

Vulnerability Base Vector

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors  
public enum Access Vector  
{Local, Adjacent, Remote}
```

Literals

⦿ Local

Local access to a vulnerable resource.

[cvss] A vulnerability exploitable with only local access requires the attacker to have either physical access to the vulnerable system or a local (shell) account. Examples of locally exploitable vulnerabilities are peripheral attacks such as Firewire/USB DMA attacks, and local privilege escalations (e.g., sudo).

⦿ Adjacent

A resource vulnerable to an attacker with have access adjacent to the vulnerable resource.

[cvss] Adjacent Network. A vulnerability exploitable with adjacent network access requires the attacker to have access to either the broadcast or collision domain of the vulnerable software. Examples of local networks include local IP subnet, Bluetooth, IEEE 802.11, and local Ethernet segment.

⦿ Remote

A vulnerability that does not require physical or virtual proximity.

[cvss] Network: A vulnerability exploitable with network access means the vulnerable software is bound to the network stack and the attacker does not require local network access or local access.

Such a vulnerability is often termed “remotely exploitable”. An example of a network attack is an RPC buffer overflow.

[8.15.238.14.23](#)Enumeration Authentication

[CVSS] This metric measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability. This metric does not gauge the strength or complexity of the authentication process, only that an attacker is required to provide credentials before an exploit may occur. The fewer authentication instances that are required, the higher the vulnerability score.

It is important to note that the Authentication metric is different from Access Vector. Here, authentication requirements are considered once the system has already been accessed. Specifically, for locally exploitable vulnerabilities, this metric should only be set to “single” or “multiple” if authentication is needed beyond what is required to log into the system. An example of a locally exploitable vulnerability that requires authentication is one affecting a database engine listening on a Unix domain socket (or some other non-network interface). If the user must authenticate as a valid database user in order to exploit the vulnerability, then this metric should be set to “single.”

Direct Known Superclasses

Vulnerability Base Vector

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors  
public enum Authentication  
{Multiple, Single, None}
```

Literals

◎ Multiple

Exploiting the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time. An example is an attacker authenticating to an operating system in addition to providing credentials to access an application hosted on that system.

◎ Single

One instance of authentication is required to access and exploit the vulnerability.

◎ None

Authentication is not required to access and exploit the vulnerability.

[8.15.248.14.24](#)Enumeration Availability Impact

[CVSS] Impact affecting the availability of a resource for its intended use.

Direct Known Superclasses

Vulnerability Base Vector

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors  
public enum Availability Impact  
{None, Partial, Complete}
```

Literals

◊ None

[cvss] There is no impact to the availability of the system.

◊ Partial

[cvss] There is reduced performance or interruptions in resource availability. An example is a network-based flood attack that permits a limited number of successful connections to an Internet service.

◊ Complete

[cvss] There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.

8.15.258.14.25 Enumeration Collateral Damage Potential

[CVSS] This metric measures the potential for loss of life or physical assets through damage or theft of property or equipment. The metric may also measure economic loss of productivity or revenue. Naturally, the greater the damage potential, the higher the vulnerability score.

Direct Known Superclasses

Vulnerability Environmental Vector

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors
```

```
public enum Collateral Damage Potential
```

```
{None, Low, Low-Medium, Medium High, High}
```

Literals

◊ None

[cvss] There is no potential for loss of life, physical assets, productivity, or revenue.

◊ Low

[cvss] A successful exploit of this vulnerability may result in slight physical or property damage. Or, there may be a slight loss of revenue or productivity to the organization.

◊ Low-Medium

[cvss] A successful exploit of this vulnerability may result in moderate physical or property damage. Or, there may be a moderate loss of revenue or productivity to the organization.

◊ Medium High

[cvss] A successful exploit of this vulnerability may result in significant physical or property damage or loss. Or, there may be a significant loss of revenue or productivity.

⊕ High

[cvss] A successful exploit of this vulnerability may result in catastrophic physical or property damage and loss. Or, there may be a catastrophic loss of revenue or productivity.

[8.15.268.14.26](#) Enumeration Confidentiality Impact

[CVSS] This metric measures the impact on confidentiality of a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. Increased confidentiality impact increases the vulnerability score.

Direct Known Superclasses

[Vulnerability Base Vector](#)

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors  
public enum Confidentiality Impact  
{None, Partial, Complete}
```

Literals

⊕ None

[cvss] There is no impact to the confidentiality of the system.

⊕ Partial

[cvss] There is considerable informational disclosure. Access to some system files is possible, but the attacker does not have control over what is obtained, or the scope of the loss is constrained. An example is a vulnerability that divulges only certain tables in a database.

⊕ Complete

[cvss] There is total information disclosure, resulting in all system files being revealed. The attacker is able to read all of the system's data (memory, files, etc.)

[8.15.278.14.27](#) Enumeration Exploitability

This metric measures the current state of exploit techniques or code availability. Public availability of easy-to-use exploit code increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability.

Initially, real-world exploitation may only be theoretical. Publication of proof of concept code, functional exploit code, or sufficient technical details necessary to exploit the vulnerability may follow. Furthermore, the exploit code available may progress from a proof-of-concept demonstration to exploit code that is successful in exploiting the vulnerability.

consistently. In severe cases, it may be delivered as the payload of a network-based worm or virus. The more easily a vulnerability can be exploited, the higher the vulnerability score.

Direct Known Superclasses

Vulnerability Temporal Vector

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors
```

```
public enum Exploitability
```

```
{Unproven, Proof of concept, Functional, High}
```

Literals

- ◊ Unproven

[cvss] No exploit [code] is available, or an exploit is entirely theoretical.

- ◊ Proof of concept

[cvss] Proof-of-concept exploit [code] or an attack demonstration that is not practical for most systems is available. The code or technique is not functional in all situations and may require substantial modification by a skilled attacker.

- ◊ Functional

[cvss] Functional exploit [code] is available. The [code/exploit] works in most situations where the vulnerability exists.

- ◊ High

[cvss] Either the vulnerability is exploitable by functional mobile autonomous code, or no exploit is required (manual trigger) and details are widely available. The code works in every situation, or is actively being delivered via a mobile autonomous agent (such as a worm or virus).

8.15.288.14.28 Enumeration Integrity Impact

[CVSS] This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and guaranteed veracity of information. Increased integrity impact increases the vulnerability score.

Direct Known Superclasses

Vulnerability Base Vector

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors
```

```
public enum Integrity Impact
```

```
{None, Partial, Complete}
```

Literals

- ◊ None

[cvss] There is no impact to the integrity of the system.

- ◊ Partial

Control over the system is partially comprised.

[cvss] Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited. For example, system or application files may be overwritten or modified, but either the attacker has no control over which files are affected or the attacker can modify files within only a limited context or scope.

- ◊ Complete

[CVSS] There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.

[8.15.298.14.29](#) Enumeration Remediation Level

[CVSS] A way to express the degree of remediation that can be provided.

Direct Known Superclasses

[Vulnerability Temporal Vector](#)

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors
```

```
public enum Remediation Level
```

```
{Official Fix, Temporary Fix, Workaround, Unavailable}
```

Literals

- ◊ Official Fix

[cvss] A complete vendor solution is available. Either the vendor has issued an official patch, or an upgrade is available.

- ◊ Temporary Fix

[cvss] There is an official but temporary fix available. This includes instances where the vendor issues a temporary hotfix, tool, or workaround.

- ◊ Workaround

[cvss] There is an unofficial, non-vendor solution available. In some cases, users of the affected technology will create a patch of their own or provide steps to work around or otherwise mitigate the vulnerability.

- ◊ Unavailable

[cvss] There is either no solution available or it is impossible to apply

[8.15.2108.14.210](#)Enumeration Report Confidence

[CVSS] Confidence in a report.

Direct Known Superclasses

[Vulnerability Temporal Vector](#)

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors
```

```
public enum Report Confidence
```

```
{Unconfirmed, Uncorroborated, Confirmed}
```

Literals

○ Unconfirmed

[cvss] There is a single unconfirmed source or possibly multiple conflicting reports. There is little confidence in the validity of the reports. An example is a rumor that surfaces from the hacker underground.

○ Uncorroborated

[cvss] There are multiple non-official sources, possibly including independent security companies or research organizations. At this point there may be conflicting technical details or some other lingering ambiguity.

○ Confirmed

[cvss] The vulnerability has been acknowledged by the vendor or author of the affected technology. The vulnerability may also be “Confirmed” when its existence is confirmed from an external event such as publication of functional or proof-of-concept exploit code or widespread exploitation.

[8.15.2118.14.211](#)Enumeration Security Requirements

[CVSS] These metrics enable the analyst to customize the CVSS score depending on the importance of the affected IT asset to a user’s organization, measured in terms of confidentiality, integrity, and availability. That is, if an IT asset supports a business function for which availability is most important, the analyst can assign a greater value to availability, relative to confidentiality and integrity. Each security requirement has three possible values: “low,” “medium,” or “high.” The full effect on the environmental score is determined by the corresponding base impact metrics. That is, these metrics modify the environmental score by reweighting the (base) confidentiality, integrity, and availability impact metrics. For example, the confidentiality impact (C) metric has increased weight if the confidentiality requirement (CR) is “high.” Likewise, the confidentiality impact metric has decreased weight if the confidentiality requirement is “low.” The confidentiality impact metric weighting is neutral if the confidentiality requirement is “medium.” This same logic is applied to the integrity and availability requirements.

Note that the confidentiality requirement will not affect the environmental score if the (base) confidentiality impact is set to “none.” Also, increasing the confidentiality requirement from “medium” to “high” will not change the environmental score when the (base) impact metrics are set to “complete.”

This is because the impact sub score (part of the base score that calculates impact) is already at a maximum value of 10. The greater the security requirement, the higher the score (remember that “medium” is considered the default).

Direct Known Superclasses

[Vulnerability Environmental Vector](#)

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors  
public enum Security Requirements  
{Low, Medium, High}
```

Literals

➊ Low

[cvss] Loss of [confidentiality | integrity | availability] is likely to have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).

➋ Medium

[cvss] Loss of [confidentiality | integrity | availability] is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).

➌ High

[cvss] Loss of [confidentiality | integrity | availability] is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers)

[8.15.2428.14.212 Enumeration Target Distribution](#)

[CVSS] This metric measures the proportion of vulnerable systems. It is meant as an environment-specific indicator in order to approximate the percentage of systems that could be affected by the vulnerability.
The greater the proportion of vulnerable systems, the higher the score.

Direct Known Superclasses

[Vulnerability Environmental Vector](#)

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability  
Vectors  
public enum Target Distribution  
{None, Low, Medium, High}
```

Literals

➊ None

[cvss] No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting. Effectively 0% of the environment is at risk.

➋ Low

[cvss] Targets exist inside the environment, but on a small scale. Between 1% - 25% of the total environment is at risk.

● Medium

[cvss] Targets exist inside the environment, but on a medium scale. Between 26% - 75% of the total environment is at risk

● High

[cvss] Targets exist inside the environment on a considerable scale. Between 76% - 100% of the total environment is considered at risk.

[8.16.15 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Weapons](#)

[8.16.18.15.1 Diagram: Weapons](#)

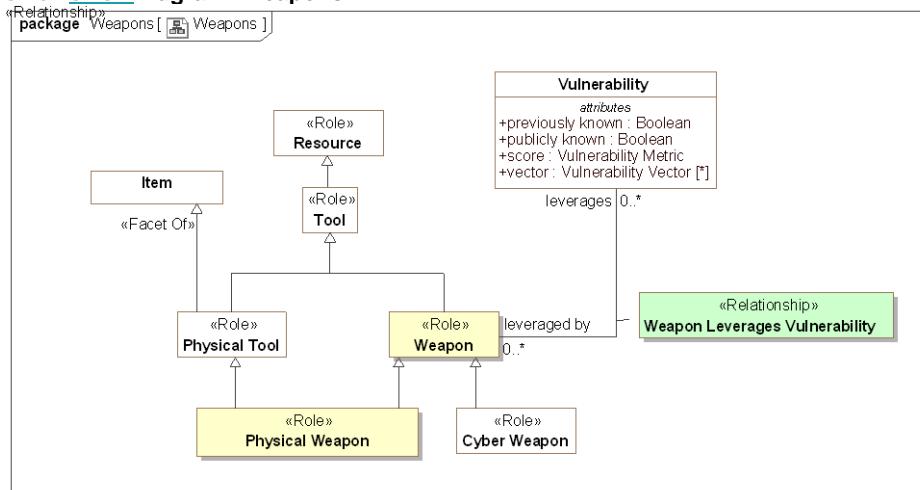


Figure 50. Weapons

[8.16.28.15.2 Class Physical Weapon <<Role>>](#)

A physical item intended to exploit a vulnerability and cause harm to some class of entities.

Direct Supertypes

[Physical Tool](#), [Weapon](#)

[8.16.38.15.3 Class Weapon <<Role>>](#)

Role of something used by an actor to cause harm by exploiting vulnerabilities.

Direct Supertypes

[Tool](#)

Associations

leverages : [Vulnerability](#) [0..*] Subsets: impacts:[Identifiable Entity](#)
through association: [Weapon Leverages Vulnerability](#)

Vulnerability that a weapon helps an actor take advantage of.

8.16.48.15.4 Association Class Weapon Leverages Vulnerability <<Relationship>>

Relationship defining the weapons that can leverage (exploit) a vulnerability.

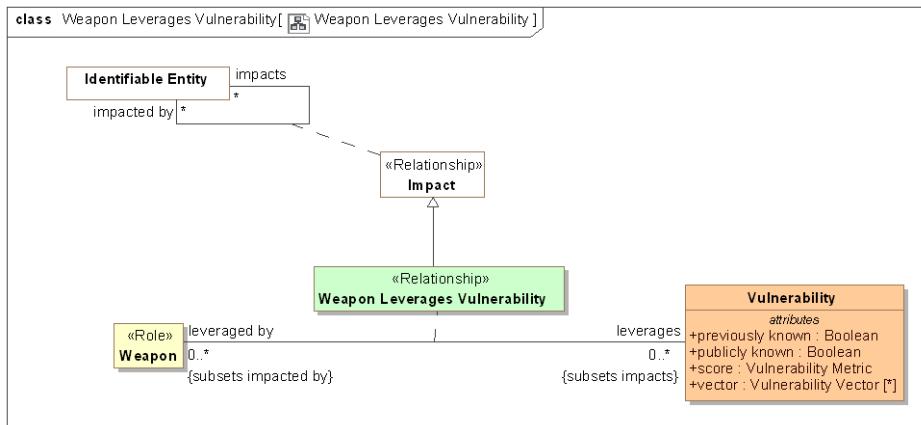


Figure 51. Weapon Leverages Vulnerability

Direct Supertypes

[Impact](#)

Association Ends

leverages : [Vulnerability](#) [0..*] Subsets: impacts:[Identifiable Entity](#)

Vulnerability that a weapon helps an actor take advantage of.

leveraged by : [Weapon](#) [0..*] Subsets: impacts:[Identifiable Entity](#)

Weapon that can leverage a vulnerability to help an actor take advantage of that vulnerability.

9 Generic Concept Library (Normative)

9.1 Threat-risk-conceptual-model::Generic Concept Library

Concepts that are common across many domains and purposes such that they may be used as needed to federate and translate information into a threat, risk or other domain. Also known as "Micro theories" in logic.

9.1.1 Diagram: Generic Concept Library

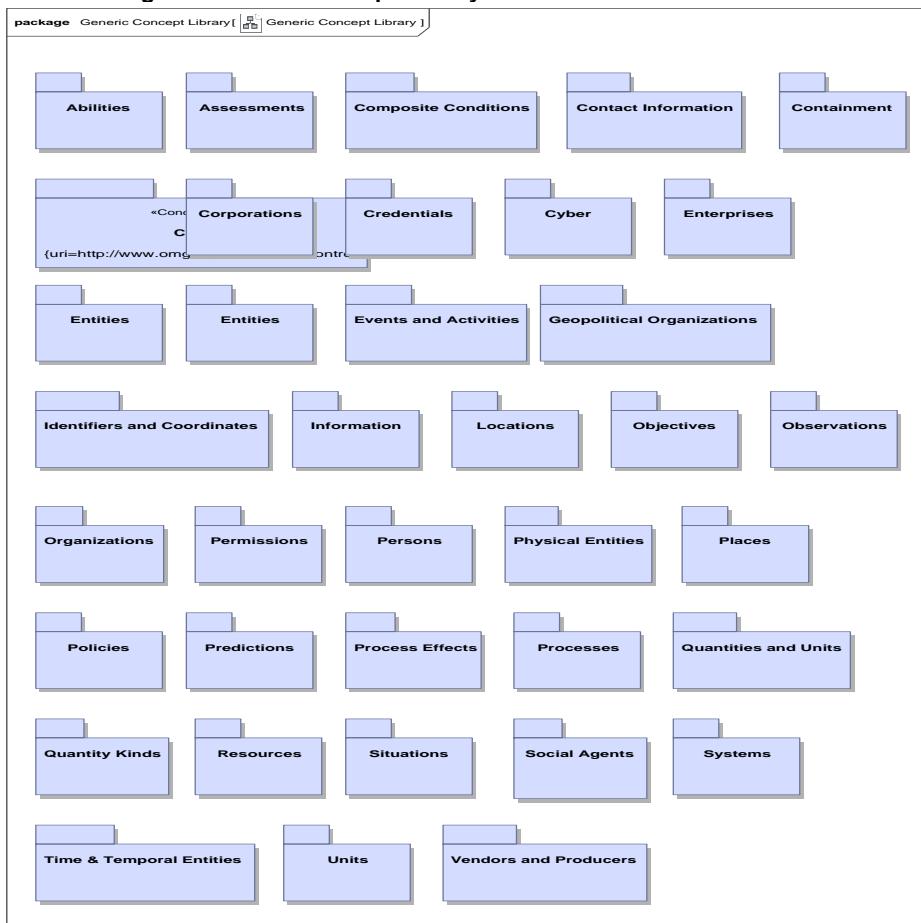


Figure 52. Generic Concept Library

Modules (as UML packages) defined as generic concepts under threat & risk. Each module focuses on a particular concept with dependencies on other modules. This forms a graph of "micro theories" that can be independently utilized.

9.2 Threat-risk-conceptual-model::Generic Concept Library::Abilities

The Ability module defines the basic concept of an *Ability* as the availability of a resource to an actor. The resource may be specific, such as \$5000, a weapon, or general, such as the ability to teach math. Each Ability is a state indicating that it has a lifetime and can participate in all the state/situation and entity relations. *Credentials* may be physical or virtual and attest to the Ability.

Abilities may be created, enhanced, diminished, or eliminated with an *Alter Ability* Event. When an actor alters an Ability (of themselves or others) they are playing the role of a *Facilitator* who performs an *Alter Capacity*.

9.2.1 Diagram: Ability

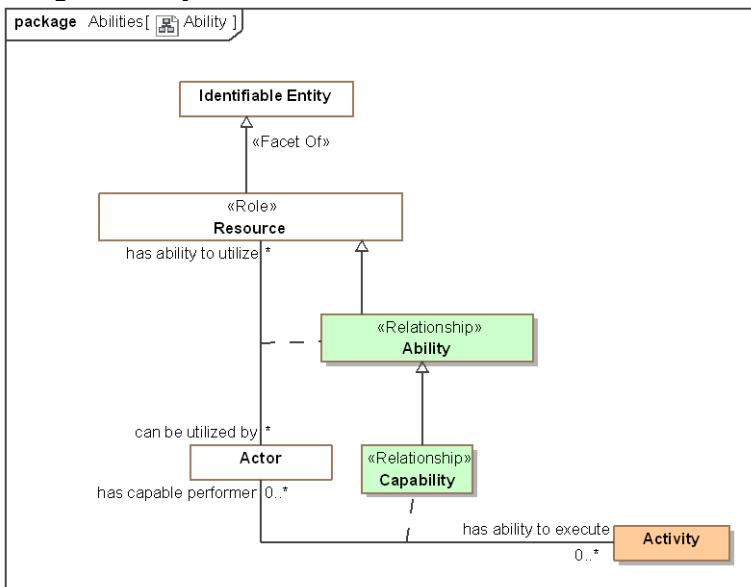


Figure 53. Ability

9.2.2 Diagram: Alter ability or control

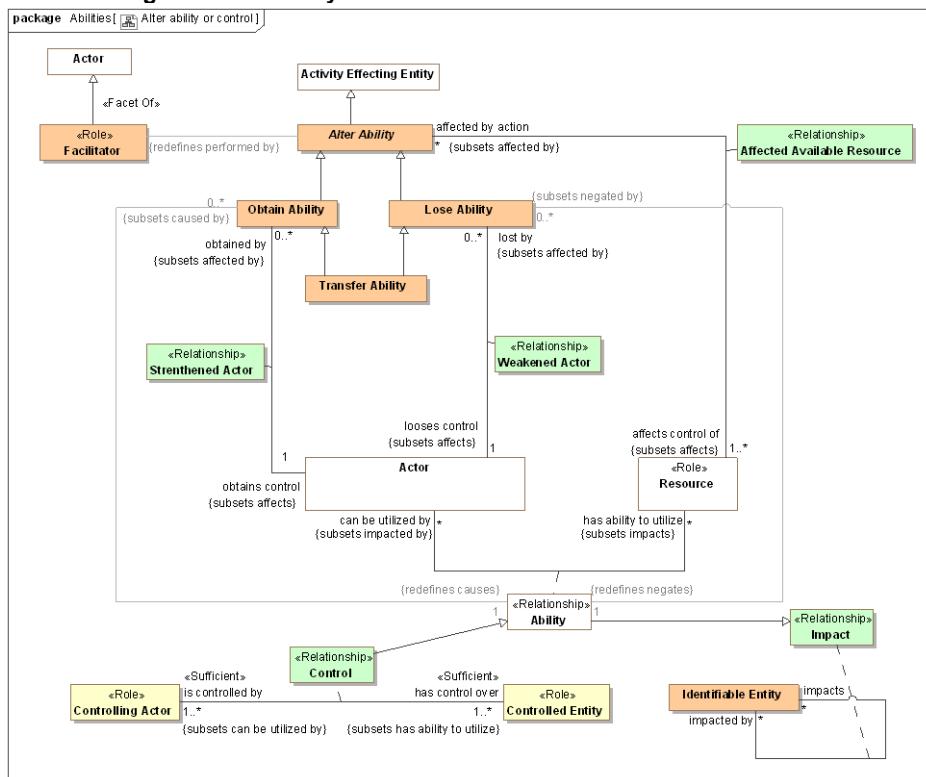


Figure 54. Alter ability or control

9.2.3 Association Class Ability <<Relationship>>

An Ability is the availability of a resource to an actor to perform activities.

Note that as with any entity, an Ability can also be categorized as a resource and thus the subject of other relationships..

Note that resources can be physical (such as a hammer), activities, virtual or more abstract such as training or experience.

[ISO/IEC 17027:2014] ability: capacity to perform an activity

[NIEM] CapabilityType:

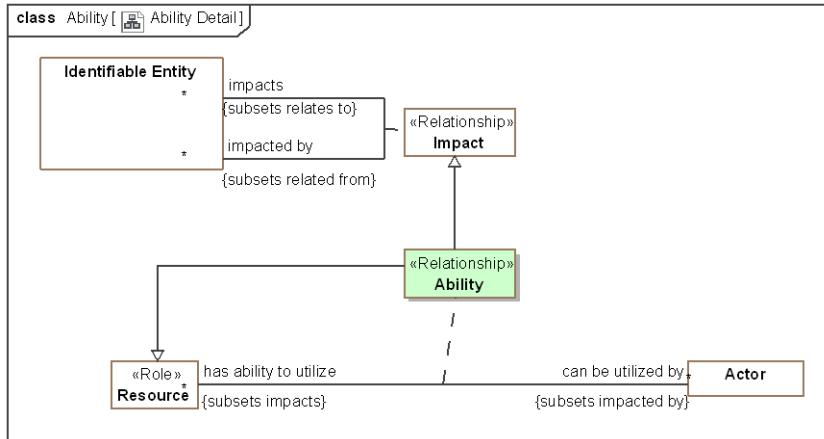


Figure 55. Ability Detail

Direct Supertypes

[Impact](#), [Resource](#)

Association Ends

can be utilized by : [Actor](#) [*]

The actor having the ability to utilize a resource for a purpose.

has ability to utilize : [Resource](#) [*]

A resource an actor can employ as part of a capability.

Associations

<<Restriction>> : [Lose Ability](#) [0..*] Subsets: negated by:[Situation](#)

<<Restriction>> : [Obtain Ability](#) [0..*] Subsets: caused by:[Situation](#)

has credential : [Credential](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)

through association: [Attest to Ability](#)

A physical or logical record of an assertion that a particular actor has a particular ability.

9.2.4 Association Class Affected Available Resource <<Relationship>>

An alter ability action affects an actors control over one or more resources. This relationship defines the set of resources impacted by an alter ability action.

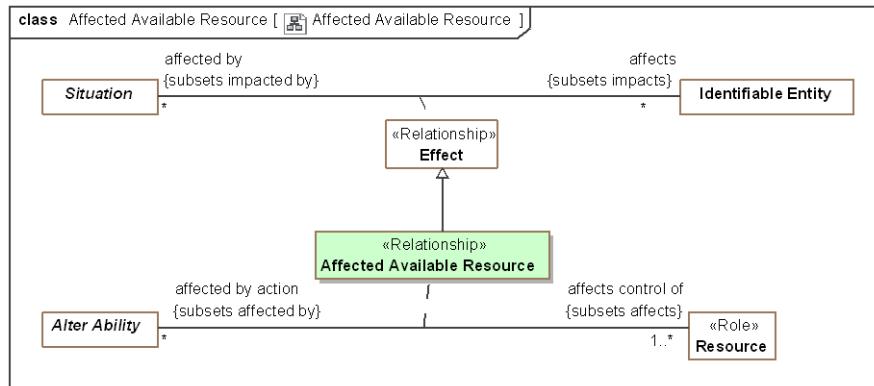


Figure 56. Affected Available Resource

Direct Supertypes

[Effect](#)

Associations

affects control of : [Resource](#) [1..*] Subsets: impacted by:[Identifiable Entity](#)

Resource that an alter ability action impacts in terms of its availability to actors.

affected by action : [Alter Ability](#) [*] Subsets: impacted by:[Identifiable Entity](#)

Actions which impact the availability of a resource to actors.

9.2.5 Class Alter Ability

The Event of providing or removing abilities (including control) by impacting the resources available to an actor.

Direct Supertypes

[Activity Effecting Entity](#)

Associations

<<Restriction>> : [Facilitator](#) Redefines: performed by:[Actor](#)

affects control of : [Resource](#) [1..*] Subsets: affects:[Identifiable Entity](#)

through association: [Affected Available Resource](#)

Resource that an alter ability action impacts in terms of its availability to actors.

9.2.6 Association Class Capability <>Relationship>>

A capability is the ability of an actor to have an effect by performing or enacting a process realized through the use of resources. Capability may lead to performance of the activity.

[FIBO] Capability: A capability represents the ability to perform a particular type of work and may involve people with particular skills and knowledge, intellectual property, defined practices, operating facilities, tools and equipment.

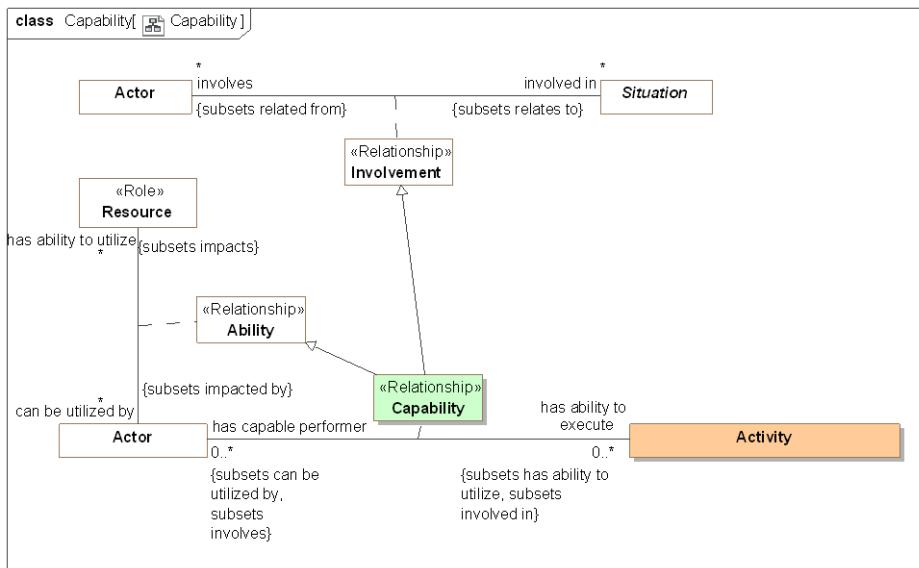


Figure 57. Capability

Direct Supertypes

[Ability](#), [Involvement](#)

Association Ends

has ability to execute : [Activity](#) [0..*] Subsets: affects:[Identifiable Entity](#)

The ability of an actor to perform a process.

has capable performer : [Actor](#) [0..*] Subsets: affects:[Identifiable Entity](#)

Actor capable of performing an process.

9.2.7 Class Facilitator <>Role>>

An actor able to provide an ability to another actor. e.g., Joe has supervisor rights to a database.

Direct Supertypes

Actor

Associations

/ <>Restriction>> : [Alter Ability](#) Subsets: performs:[Activity](#)

9.2.8 Class Lose Ability

An Event that reduces of the ability of an actor.

Direct Supertypes

[Alter Ability](#)

Associations

█ loses control : [Actor](#) [1] Subsets: affects:[Identifiable Entity](#)
through association: [Weakened Actor](#)

Control that is lost as a result of a lose control Event.

/ <>Restriction>> : [Ability](#) [1] Redefines: negates:[Situation](#)
/ withdraws : [Control](#) [1]

The control relationship that is withdrawn by a lose control activity.

9.2.9 Class Obtain Ability

An Event that increases the resources available to an actor.

Direct Supertypes

[Alter Ability](#)

Associations

/ affords : [Control](#) [1]

An act that provides control of an entity.

█ obtains control : [Actor](#) [1] Subsets: affects:[Identifiable Entity](#)
through association: [Strengthened Actor](#)

Control obtained by a obtain control action.

/ <>Restriction>> : [Ability](#) [1] Redefines: causes:[Situation](#)

9.2.10 Association Class Strengthened Actor <>Relationship>>

The act of obtaining control of an entity.

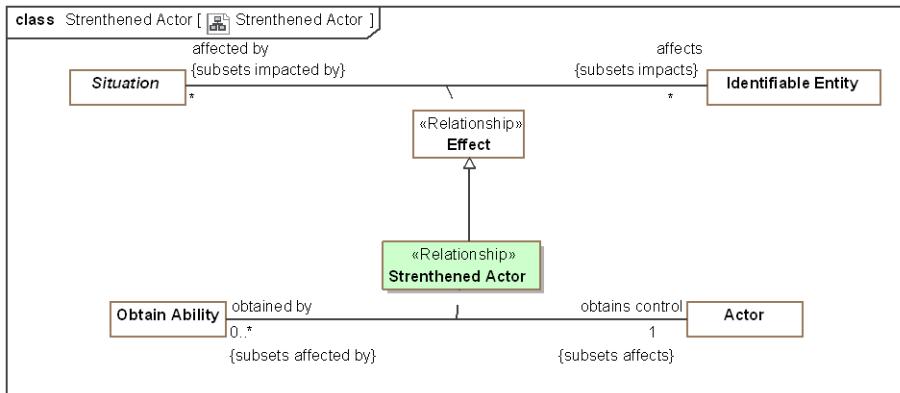


Figure 58. Strenthened Actor

Direct Supertypes

[Effect](#)

Association Ends

obtains control : [Actor](#) [1] Redefines: causes: [Situation](#)

Control obtained by a obtain control action.

obtained by : [Obtain Ability](#) [0..*] Redefines: causes: [Situation](#)

Method by which control is obtained.

9.2.11 Class Transfer Ability

The purposeful or accidental transfer of ability or control from one actor to another. Such transfer of ability or control may be by agreement or force.

Direct Supertypes

[Event](#), [Lose Ability](#), [Obtain Ability](#)

9.2.12 Association Class Weakened Actor <>Relationship>>

Relationship describing how an actor reduces the resources available to an actor.

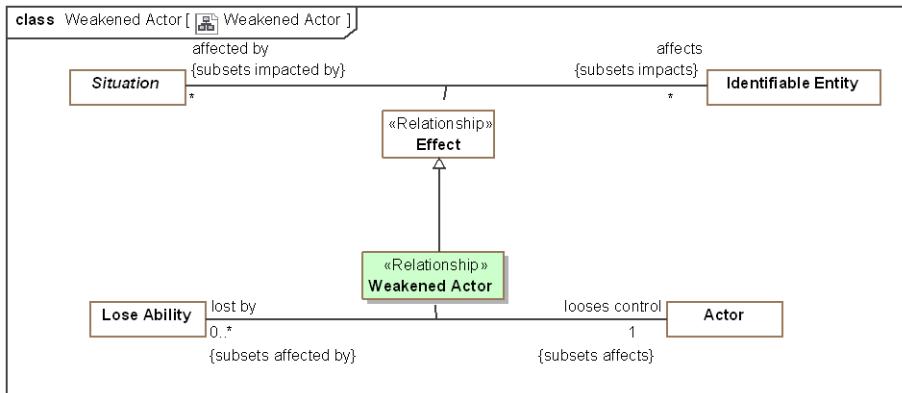


Figure 59. Weakened Actor

Direct Supertypes

[Effect](#)

Association Ends

█ loses control : [Actor](#) [1] *Redefines:* causes: [Situation](#)

Control that is lost as a result of a lose control Event.

█ lost by : [Lose Ability](#) [0..*] *Redefines:* causes: [Situation](#)

Action that causes a loss of control.

9.3 Threat-risk-conceptual-model::Generic Concept Library::Assessments

Concepts relating to the structured evaluation of an entity or entities.

9.3.1 Diagram: Assessment

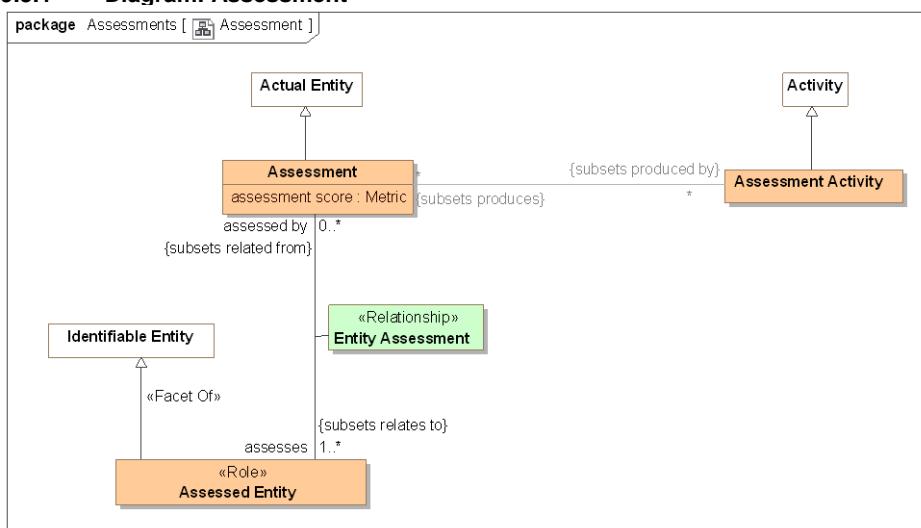


Figure 60. Assessment

The evaluation or estimation of the nature, quality, or ability of someone or something.
 [BMM] Assessment: judgment that an influencer affects the employment of means and/or the achievement of ends

9.3.2 Class Assessed Entity <<Role>>

Role of an entity that is assessed.

Direct Supertypes

[Identifiable Entity](#)

Associations

assessed by : [Assessment](#) [0..*] Subsets: related from:[Identifiable Entity](#)

through association: [Entity Assessment](#)

Entity performing an assessment.

9.3.3 Class Assessment

An evaluation, appraisal, or assessment of something or someone.

[NIEM] AssessmentType: The act of evaluating or estimating the nature, ability, or quality of something. {Note: In NIEM the assessment and activity are combined}

Direct Supertypes

[Actual Entity](#)

Attributes

◎ assessment score : [Metric](#)

An evaluation score of an assessment.[NIEM]

Associations

█ assesses : [Assessed Entity](#) [1..*] Subsets: relates to:[Identifiable Entity](#)
through association: [Entity Assessment](#)

Entity assessed by an assessment activity

↙ <<Restriction>> : [Assessment Activity](#) [*] Subsets: produced by:[Event](#)

9.3.4 Class Assessment Activity

An activity that results in an assessment - An evaluation, appraisal, or assessment of something or someone. An assessment frequently as an artifact, a report of the assessment.

[NIEM] AssessmentType: The act of evaluating or estimating the nature, ability, or quality of something.

Direct Supertypes

[Activity](#)

Associations

↙ <<Restriction>> : [Assessment](#) [*] Subsets: produces:[Identifiable Entity](#)

9.3.5 Association Class Entity Assessment <<Relationship>>

Entities assessed is a relationship between an assessment activity and an entity being assessed that is the topic of an assessment report.

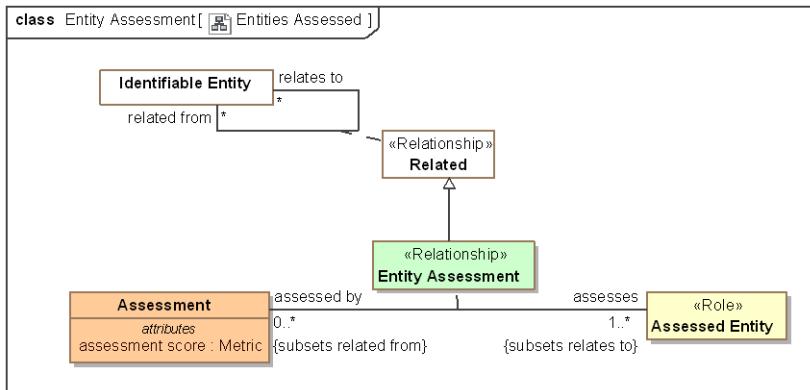


Figure 61. Entities Assessed

Direct Supertypes

[Related](#)

Association Ends

[assesses](#) : [Assessed Entity](#) [1..*] Subsets: produces: [Identifiable Entity](#)

Entity assessed by an assessment activity

[assessed by](#) : [Assessment](#) [0..*] Subsets: produces: [Identifiable Entity](#)

Entity performing an assessment.

9.4 Threat-risk-conceptual-model::Generic Concept Library::Contact Information

The definition of various ways to contact an entity. Subtypes of contact information supply specific formats.

9.4.1 Diagram: Contact Information

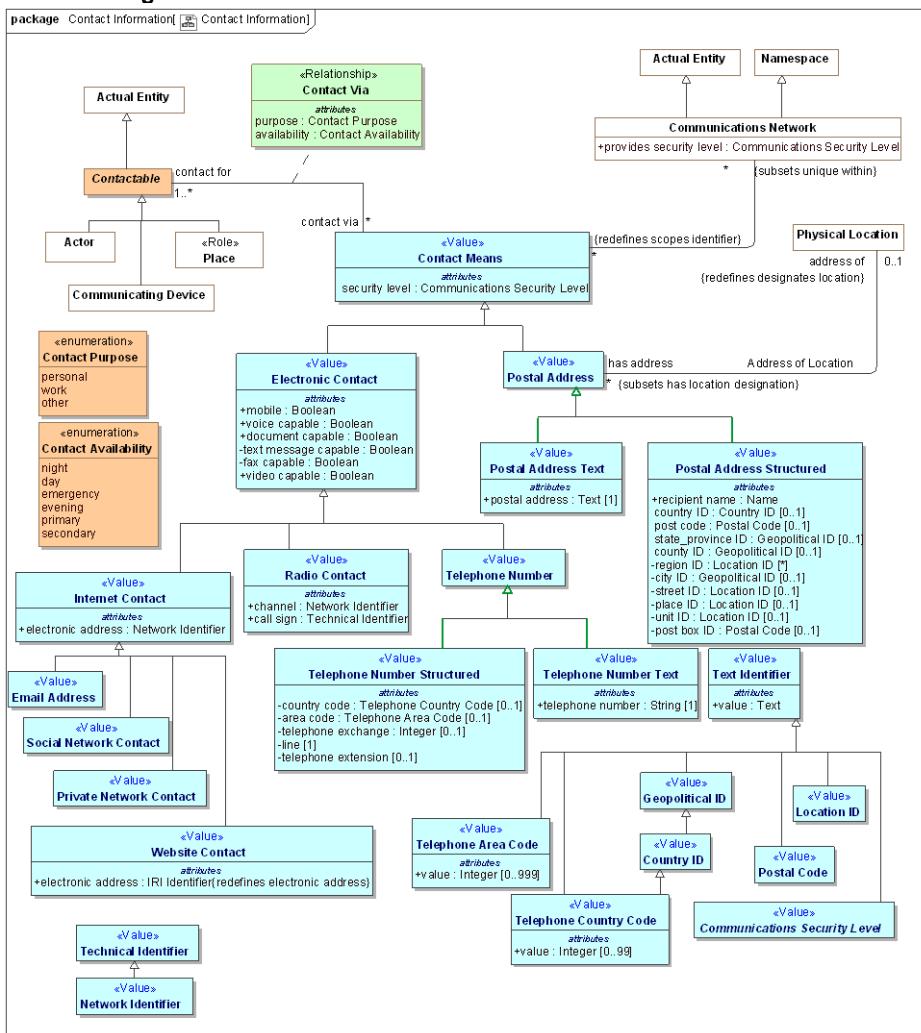


Figure 62. Contact Information

9.4.2 Class Communications Security Level <>Value>>

An abstract type for levels of security in communications.

Direct Supertypes

[Text Identifier](#)

9.4.3 Class Contact Means <>Value>>

Anything that may be used to communicate with an individual.

[FIBO] AddressingScheme

[NIEM] ContactMeans & ContactInformationType

Direct Supertypes

[Unique Identifier](#)

Attributes

◊ security level : [Communications Security Level](#)

The level of security asserted as provided by the subject contact means. May default to the security level of the communications network.

Associations

▀ contact for : [Contactable](#) [1..*]

through association: [Contact Via](#)

An actor or place for which the contact information may be used to contact that entity.

/ : [Communications Network](#) [*] Subsets: unique within:[Namespace](#)

9.4.4 Association Class Contact Via <>Relationship>>

Information relative to communicating with an entity.

[NIEM] ContactInformationAssociationType

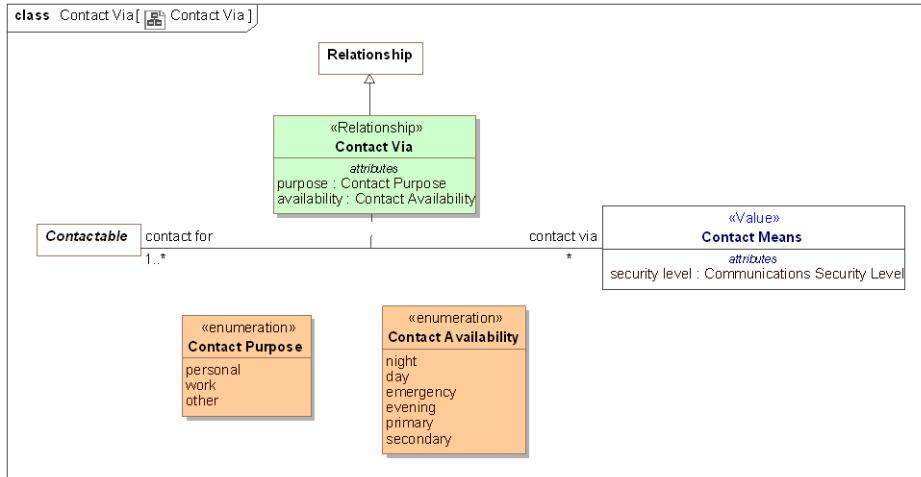


Figure 63. Contact Via

Direct Supertypes

[Relationship](#)

Association Ends

contact via : [Contact Means](#) [*] Subsets: unique within:[Namespace](#)

A way to contact an actor or place.

[FIBO] hasAddress (More specific concept - restricted to Postal Address)

contact for : [Contactable](#) [1..*] Subsets: unique within:[Namespace](#)

An actor or place for which the contact information may be used to contact that entity.

Attributes

purpose : [Contact Purpose](#)

Purposes for contacting an entity, primarily work and personal.
[NIEM] ContactPurpose

availability : [Contact Availability](#)

An enumeration of the times contact information may be used.
[NIEM] ContactInformationAvailability

9.4.5 Class Contactable

Anything that can be send or receive information or be the proxy for things that can send or receive information, e.g., people, organizations and places.

Direct Supertypes

[Actual Entity](#)

Associations

✉ contact via : [Contact Means](#) [*]

through association: [Contact Via](#)

A way to contact an actor or place.

[FIBO] hasAddress (More specific concept - restricted to Postal Address)

9.4.6 Class Electronic Contact <>Value>>

Contact information that enables communications with or via an actor or telecommunications device by electronic means.
[FIBO] VirtualAddress: an address identifying a virtual, i.e. non-physical location

Direct Supertypes

[Contact Means](#)

Attributes

◊ mobile : [Boolean](#)

Indicator that a contact method is mobile - not fixed to a location.

◊ voice capable : [Boolean](#)

An indication that a contact method is voice capable.

◊ document capable : [Boolean](#)

An indication that a contact method is capable of receiving documents, e.g., email.

◊ text message capable : [Boolean](#)

An indication that a contact method is capable of receiving text messages of limited length.

◊ fax capable : [Boolean](#)

Contact method for a communications device that is fax capable.

◊ video capable : [Boolean](#)

An indication that a contact method is video capable.

9.4.7 Class Email Address <>Value>>

Contact information for the delivery of mail via an electronic network.
[NIEM] ContactEmailId (of <electronic contact>)

Direct Supertypes

[Internet Contact](#)

9.4.8 Class Internet Contact <>Value>>

[NIEM] A means of contact that provides for the digital electronic transmission of information via the Internet or a private network.

Direct Supertypes

[Electronic Contact](#)

Attributes

◆ electronic address : [Network Identifier](#)

Electronic address by which to contact an entity via the Internet.

9.4.9 Class Network Identifier <>Value>>

A value used to identify a node in an electronic network.

[NIEM] ElectronicAddressType

Direct Supertypes

[Technical Identifier](#)

9.4.10 Class Postal Address <>Value>>

An address able to be used to deliver physical mail which may or may not represent a static physical location.

[FIBO] PPPostalAddress: a physical address where postal communications can be addressed, for any kind of organization or person.

[NIEM] AddressType

Direct Supertypes

[Contact Means](#), [Location Identifier](#)

Associations

/ address of : [Physical Location](#) [0..1] *Redefines:* designates location:[Physical Location](#)
through association: [Address of Location](#)

Location identified by an address.

9.4.11 Class Postal Address Structured <>Value>>

A structured representation of a postal address.

Direct Supertypes

[Postal Address](#)

Attributes

- recipient name : [Name](#) =

Name of the recipient in a postal address which defaults to the name of the entity having the address. Should default to the contact for "has name".

[NIEM] AddressRecipientName

- country ID : [Country ID](#) [0..1]

Postal country identifier.

- post code : [Postal Code](#) [0..1]

[OGC] An address component which represents the identification of a subdivision of addresses and postal delivery points in a country, region, or city for postal purposes.

[NIEM] LocationPostalCode

- state_province ID : [Geopolitical ID](#) [0..1]

Postal state identifier for a geopolitical regions.

[NIEM] LocationState

- county ID : [Geopolitical ID](#) [0..1]

Postal county identifier.

[NIEM] LocationCounty

- region ID : [Location ID](#) [*]

Postal region identifier.

[NIEM] AddressUrbanizationName

- city ID : [Geopolitical ID](#) [0..1]

Postal city identifier.

[NIEM] LocationCityName

- street ID : [Location ID](#) [0..1]

Postal street identifier.

[NIEM] AddressDeliveryPoint

- place ID : [Location ID](#) [0..1]

Postal identifier for a specific place: House, building, facility, etc.

- unit ID : [Location ID](#) [0..1]

Postal province identifier.

[NIEM] AddressSecondaryUnitText

- post box ID : [Postal Code](#) [0..1]

A code defined for the purposes of delivering physical mail to a specific addresses.

[NIEM] AddressPrivateMailboxText

9.4.12 Class Postal Address Text <>Value>>

A textual representation of a postal address.

Direct Supertypes

[Postal Address](#)

Attributes

- ◊ postal address : [Text](#) [1]

Textual postal address for the delivery of mail.
[NIEM] AddressFullText

9.4.13 Class Postal Code <>Value>>

A code defined for the purposes of delivering physical mail to a set of addresses. "Zip code" in the U.S.
[OGC] An address component which represents the identification of a subdivision of addresses and postal delivery points in a country, region or city for postal purposes.
[FIBO] PostalCodeArea

Direct Supertypes

[Text Identifier](#)

9.4.14 Class Private Network Contact <>Value>>

Contact identifiers valid within a private network.

Direct Supertypes

[Internet Contact](#)

9.4.15 Class Radio Contact <>Value>>

Identifier for contact via radio.
[NIEM] ContactRadioType

Direct Supertypes

[Electronic Contact](#)

Attributes

- ◊ channel : [Network Identifier](#)

Radio channel used for communications.
[NIEM] ContactRadioChannelText

- ◊ call sign : [Technical Identifier](#)

Radio or user call sign used for radio communications.
[NIEM] ContactRadioCallSignID

9.4.16 Class Social Network Contact <>Value>>

Contact information to be used via a social network.

[NIEM] InstantMessageType

--InstanceMessengerServiceName = <has name>
--InstanceMessengerScreenId = "electronic address"

Direct Supertypes

[Internet Contact](#)

9.4.17 Class Telephone Area Code <>Value>>

A three-digit number that identifies one of the telephone service regions into which the US, Canada, and certain other countries are divided and that is dialed when calling from one area to another.

Direct Supertypes

[Text Identifier](#)

Attributes

◊ value : [Integer](#) [0..999]

3 digit area code.

9.4.18 Class Telephone Country Code <>Value>>

2 digit Telephone codes for contacting people and organizations within countries.

Direct Supertypes

[Country ID](#), [Text Identifier](#)

Attributes

◊ value : [Integer](#) [0..99]

Country code digits.

9.4.19 Class Telephone Number <>Value>>

A way to contact an actor via a telephone.

[NIEM] TelephoneNumberType

Direct Supertypes

[Electronic Contact](#)

9.4.20 Class Telephone Number Structured <>Value>>

Structured representation of a telephone number.

[NIEM] NANPPhoneNumberType & InternationalPhoneNumberType

Direct Supertypes

[Telephone Number](#)

Attributes

- ◊ country code : [Telephone Country Code](#) [0..1]

Telephone country code.

[NIEM] TelephoneCountryCodeID

- ◊ area code : [Telephone Area Code](#) [0..1]

Telephone area code.

[NIEM] TelephoneAreaCodeID

- ◊ telephone exchange : [Integer](#) [0..1]

Number identifying a telephone exchange.

[NIEM] TelephoneExchangeID

- ◊ line [1]

Telephone line number.

[NIEM] TelephoneLineID

- ◊ telephone extension [0..1]

Telephone extension number.

9.4.21 Class Telephone Number Text <>Value>>

Unstructured (text) representation of a telephone number.

[NIEM] FullPhoneNumberType

Direct Supertypes

[Telephone Number](#)

Attributes

- ◊ telephone number : [String](#) [1]

Textual telephone number.

[NIEM] TelephoneNumberFullID

9.4.22 Class Website Contact <>Value>>

A website that can be used to contact an individual.

Direct Supertypes

[Internet Contact](#)

Attributes

- electronic address : [IRI Identifier](#)

Electronic address by which to contact an entity via a website.
[NIEM] ContactWebsiteURI

9.4.221 Enumeration Contact Availability

A data type for a period of time or a situation in which an entity is available to be contacted with the given contact information.[NIEM]

```
package Threat-risk-conceptual-model::Generic Concept Library::Contact Information
public enum Contact Availability
{night, day, emergency, evening, primary, secondary}
```

Literals

- night

Late night contact.

- day

Daytime contact.

- emergency

Emergency contact.

- evening

Late day or early night contact.

- primary

Primary contact.

- secondary

Secondary or alternate contact.

9.4.222 Enumeration Contact Purpose

Possible purposes for contact information.[NIEM]

```
package Threat-risk-conceptual-model::Generic Concept Library::Contact Information
public enum Contact Purpose
{personal, work, other}
```

Literals

 personal

Personal communications.

 work

Work communications.

 other

Communications other than work or personal.

9.5 Threat-risk-conceptual-model::Generic Concept Library::Containment

9.5.1 Diagram: Containment

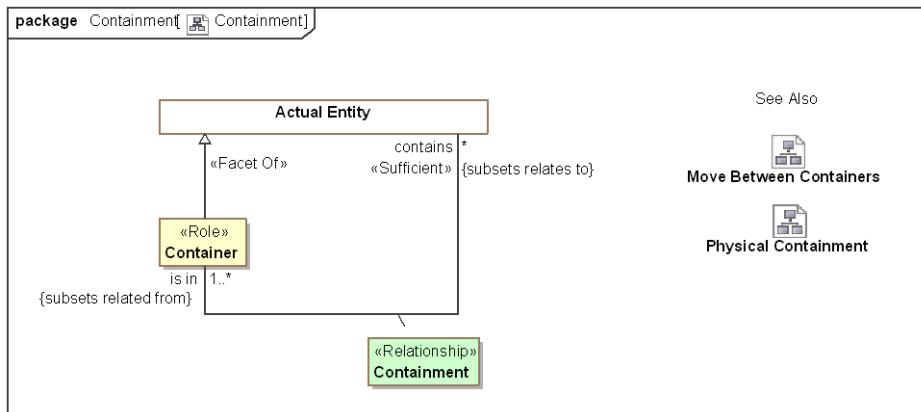


Figure 64. Containment

9.5.2 Diagram: Move Between Containers

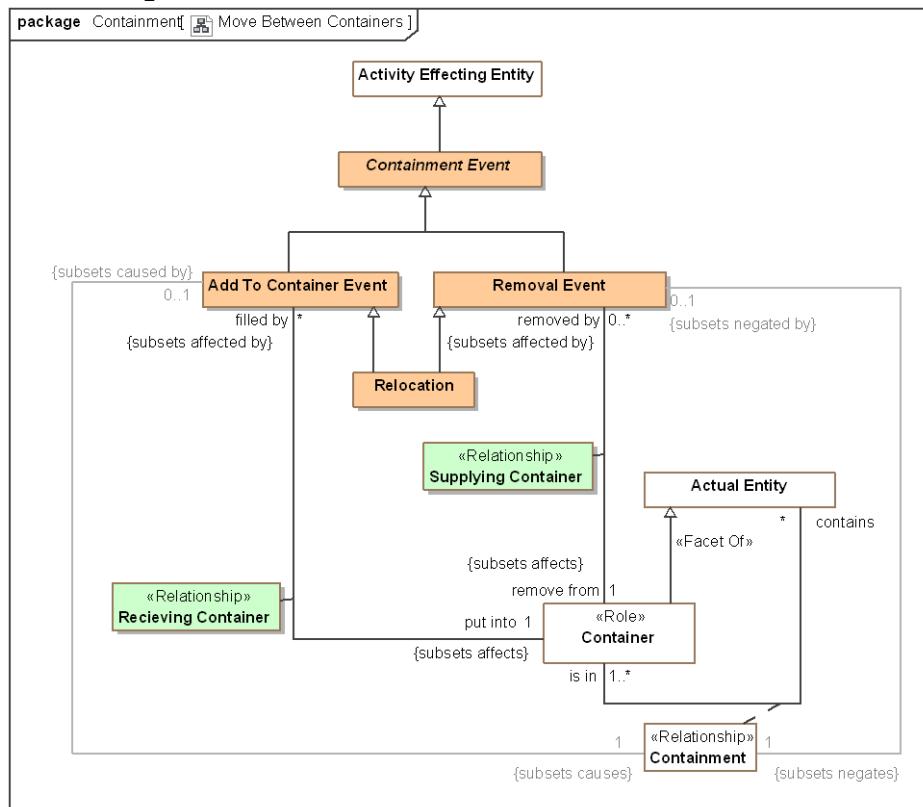


Figure 65. Move Between Containers

9.5.3 Diagram: Physical Containment

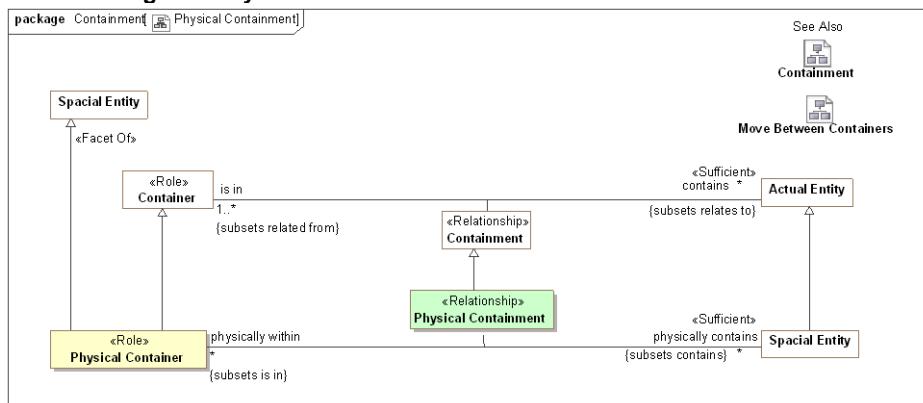


Figure 66. Physical Containment

9.5.4 Class Add To Container Event

An event that puts things into containers or locations. This results in a new containment relationship.

Direct Supertypes

[Containment Event](#)

Associations

put into : [Container](#) [1] Subsets: affects: [Identifiable Entity](#)
through association: [Receiving Container](#)

Container that receives something by a fill action.

/ <>Restriction>> : [Containment](#) [1] Subsets: causes: [Situation](#)

9.5.5 Class Container <>Role>>

Role of something as a container for other things. Containers & Containment may be physical or virtual.

Direct Supertypes

[Actual Entity](#)

Associations

contains : [Actual Entity](#) [*] Subsets: relates to: [Identifiable Entity](#)
through association: [Containment](#)

A thing contained within a container.

█ filled by : [Add To Container Event](#) [*] Subsets: affected by:[Situation](#)
through association: [Receiving Container](#)

Action that puts or moves something into a container or location.

█ removed by : [Removal Event](#) [0..*] Subsets: affected by:[Situation](#)
through association: [Supplying Container](#)

Action that removes something from a container or location.

9.5.6 Association Class Containment <>Relationship>>

Relationship between a container and a contained thing.

Containment may or may not correspond to a part-of relationship. In some cases both the container (a jar) and what it contains (jelly beans) may be considered parts of a whole (a jar of jelly beans).

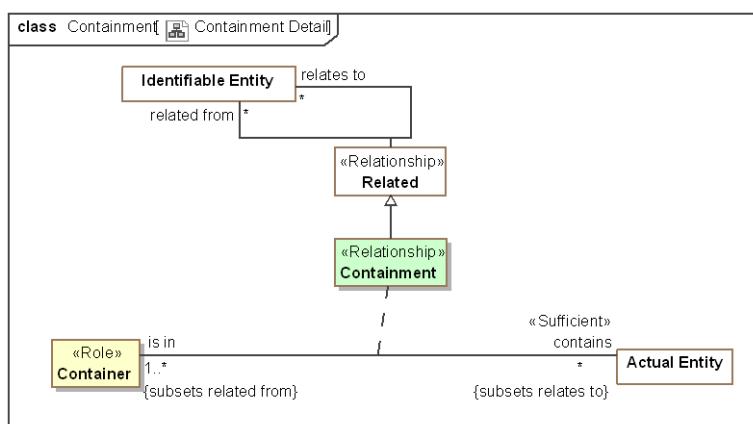


Figure 67. Containment Detail

Direct Supertypes

[Related](#)

Association Ends

█ contains : [Actual Entity](#) [*] Subsets: affected by:[Situation](#)

A thing contained within a container.

█ is in : [Container](#) [1..*] Subsets: affected by:[Situation](#)

A container which holds one or more contained things.

[FIBO] isLocatedAt: a property linking something to a location or place, which might be physical or virtual

Associations

- / <>Restriction>> : [Add To Container Event](#) [0..1] Subsets: caused by:[Situation](#)
- / <>Restriction>> : [Removal Event](#) [0..1] Subsets: negated by:[Situation](#)

9.5.7 Class Containment Event

An event impacting containment of the <contained thing>. Subtypes include "Put Into Event", "Removal Event" and "Relocation".

Direct Supertypes

[Activity Effecting Entity](#)

9.5.8 Class Physical Container <>Role>>

A physical thing or location that contains other physical things or locations.
[DOLCE] Spacial Location

Direct Supertypes

[Container, Spacial Entity](#)

Associations

- █ physically contains : [Spacial Entity](#) [*] Subsets: contains:[Actual Entity](#)
through association: [Physical Containment](#)

A physical entity contained by another physical entity.{Transitive}

9.5.9 Association Class Physical Containment <>Relationship>>

Location of something physically within a container, including locations.

Direct Supertypes

[Containment](#)

Association Ends

- █ physically contains : [Spacial Entity](#) [*] Subsets: contains:[Actual Entity](#)

A physical entity contained by another physical entity.{Transitive}

- █ physically within : [Physical Container](#) [*] Subsets: contains:[Actual Entity](#)

Physical container in which the subject physical entity is contained.{transitive}
al

9.5.10 Association Class Recieving Container <>Relationship>>

Relationship between a fill action and the container that is filled with something.

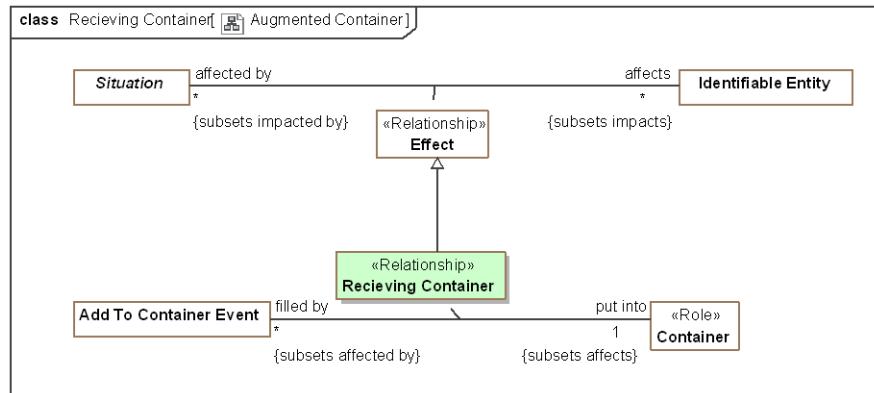


Figure 68. Augmented Container

Direct Supertypes

[Effect](#)

Association Ends

put into : [Container](#) [1] Subsets: contains:[Actual Entity](#)

Container that receives something by a fill action.

filled by : [Add To Container Event](#) [*] Subsets: contains:[Actual Entity](#)

Action that puts or moves something into a container or location.

9.5.11 Class Relocation

The transfer (send/receive) of something between containers or locations. As an Event, the move may be initiated by an actor different from the sender/receiver or may not be caused by an actor.

Examples include movement of a vehicle from one location to another or movement of supplies between warehouses.

Direct Supertypes

[Add To Container Event](#), [Removal Event](#)

9.5.12 Class Removal Event

An event that removes things from containers or locations. This results in the termination of a containment relationship.

Direct Supertypes

Containment Event

Associations

- █ remove from : [Container](#) [1] Subsets: affects:[Identifiable Entity](#)
through association: [Supplying Container](#)

Container (or location) that contained something that is removed.

- ↙ <>Restriction>> : [Containment](#) [1] Subsets: negates:[Situation](#)

9.5.13 Association Class Supplying Container <>Relationship>>

Relationship between a removal action and the container it removes something from.

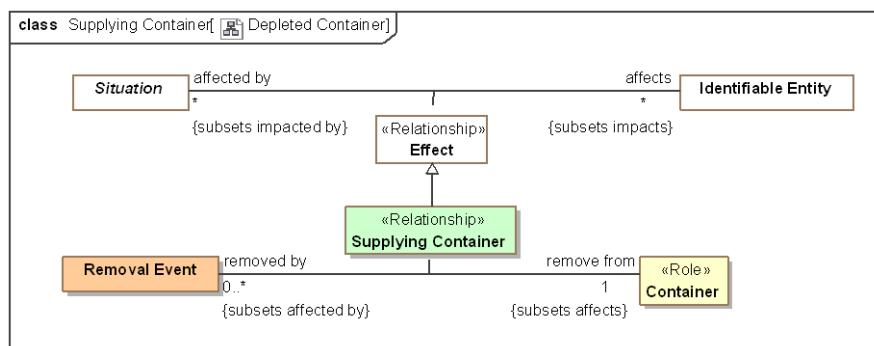


Figure 69. Depleted Container

Direct Supertypes

- Effect

Association Ends

- █ remove from : [Container](#) [1] Subsets: negates:[Situation](#)

Container (or location) that contained something that is removed.

- █ removed by : [Removal Event](#) [0..*] Subsets: negates:[Situation](#)

Action that removes something from a container or location.

9.6 Threat-risk-conceptual-model::Generic Concept Library::Control

Concepts relating to actor's control over resources.

9.6.1 Diagram: Control

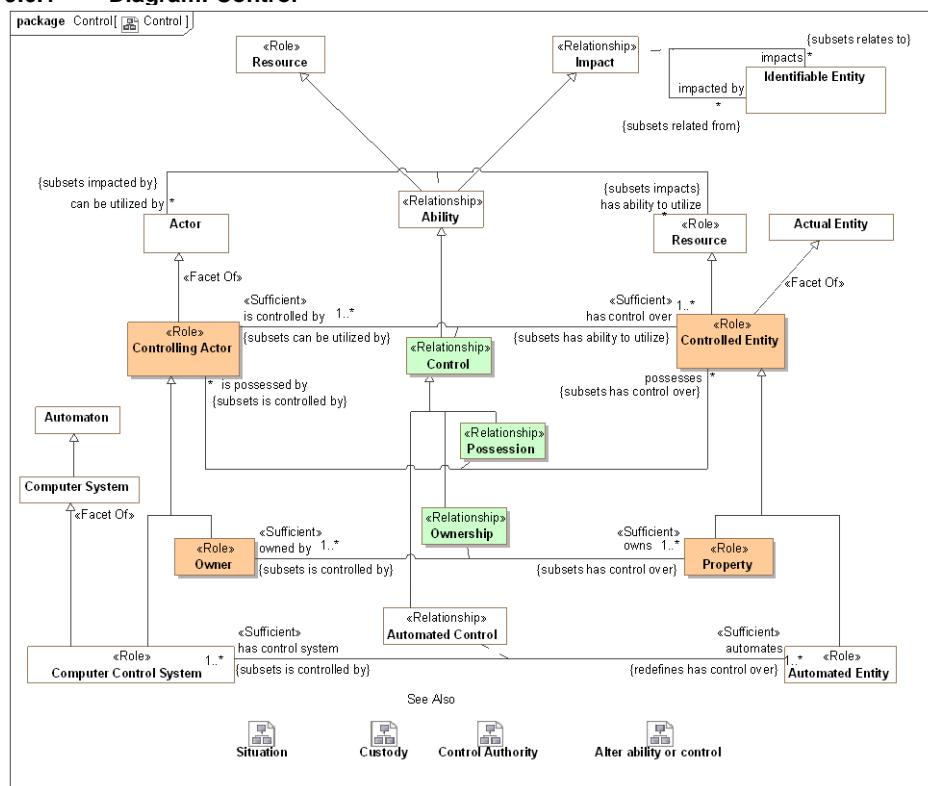


Figure 70. Control

This diagram shows that control is a kind of ability and that possession, ownership and automated control are kinds of control. For each kind of control there are specific kinds of roles involved.

9.6.2 Diagram: Control Authority

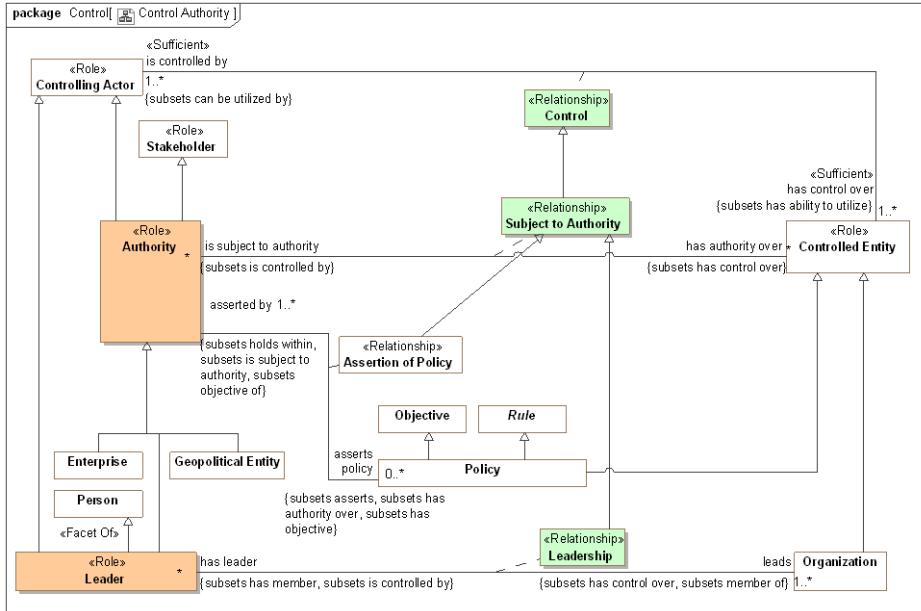


Figure 71. Control Authority

9.6.3 Diagram: Custody

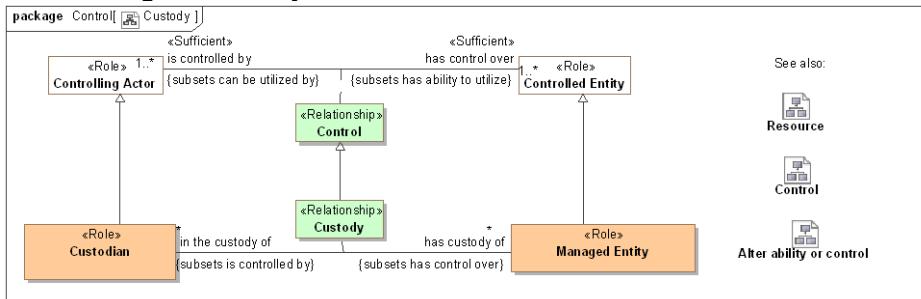


Figure 72. Custody

Custody provides a general framework for tracking the control, provenance and life cycle of items and information such that the history, trust and provenance may be ascertained. Custody provides for secure supply chains in that the life-cycle or items, information and their parts may be traced.

Custody is the relation between a Custodian and a Managed Entity (Something for which the provenance is interesting). Trust in a managed entity may also be influenced by the actors that have a capability to impact the resource.

9.6.4 Class Authority <<Role>>

An actor with authority over resources such that it can assert policy or behavior.

[ISO 15779:2011] organization, office, or individual responsible for approving equipment, installations or procedures

Direct Supertypes

[Controlling Actor](#), [Stakeholder](#)

Associations

█ asserts policy : [Policy](#) [0..*] Subsets: has objective:[Objective](#) has authority over:[Controlled Entity](#)
 asserts:[Proposition](#)
through association: [Assertion of Policy](#)

A policy asserted by an authority whom states with authority that it must be followed.

█ has authority over : [Controlled Entity](#) [*] Subsets: has control over:[Controlled Entity](#)
through association: [Subject to Authority](#)

Resource an authority has authority over - may influence in some by setting policy or defining requirements.
 [FIBO] governs

9.6.5 Association Class Control <<Relationship>>

The use or influence of an actor over an entity. This includes subtypes of control representing possession, ownership, leadership, and custody.

[FIBO] Control: the possession by a party, direct or indirect, of the power to direct or cause the direction of the management and policies of a thing, whether through the ownership of voting shares, by contract, or otherwise.

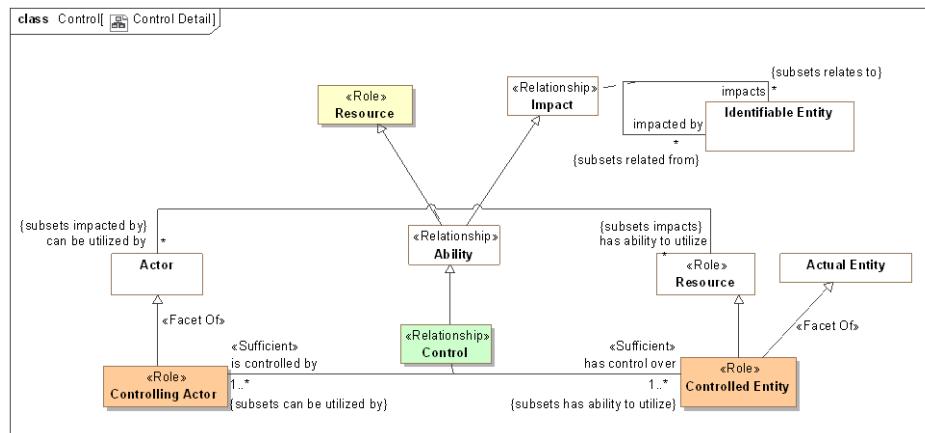


Figure 73. Control Detail

Direct Supertypes

[Ability](#)

Association Ends

 has control over : [Controlled Entity](#) [1..*] Subsets: has control over:[Controlled Entity](#)

Entity which an actor controls in some way - by authority or by possession, by force, etc.
[FIBO] controls

 is controlled by : [Controlling Actor](#) [1..*] Subsets: has control over:[Controlled Entity](#)

Actor which controls a controlled entity in some way. The nature of control may be refined in subtypes.
[FIBO] isControlledBy

Associations

 lost via : [Lose Ability](#) [0..1]

Action that causes a transfer of control.

 obtained via : [Obtain Ability](#) [1]

An action providing an actor control of an entity.

9.6.6 Class Controlled Entity <>Role>>

Role of an entity that is controlled by a controlling actor.

[FIBO] ControlledThing: thing over which some party exercises some form of control in some context

Direct Supertypes

[Actual Entity](#), [Resource](#)

Associations

 <>Sufficient>> is controlled by : [Controlling Actor](#) [1..*] Subsets: can be utilized by:[Actor](#)
through association: [Control](#)

Actor which controls a controlled entity in some way. The nature of control may be refined in subtypes.
[FIBO] isControlledBy

 is subject to authority : [Authority](#) [*] Subsets: is controlled by:[Controlling Actor](#)
through association: [Subject to Authority](#)

The authority that has some control over a resource.
[FIBO] isGovernedBy

 is possessed by : [Controlling Actor](#) [*] Subsets: is controlled by:[Controlling Actor](#)
through association: [Possession](#)

The actor that possesses the subject controlled entity.
[NIEM] ItemPossessor

9.6.7 Class Controlling Actor <>Role>>

Role of an actor that asserts control over any entity.
[FIBO] ControllingParty: Party which exercises some form of control in some context.

Direct Supertypes

[Actor](#)

Associations

 <>Sufficient>> has control over : [Controlled Entity](#) [1..*] Subsets: has ability to utilize:[Resource](#)
through association: [Control](#)

Entity which an actor controls in some way - by authority or by possession, by force, etc.
[FIBO] controls

 possesses : [Controlled Entity](#) [*] Subsets: has control over:[Controlled Entity](#)
through association: [Possession](#)

A controlled entity in the physical possession of a controlling actor.

9.6.8 Class Custodian <>Role>>

An actor who has responsibility for or looks after some managed entity. A Custodian <has custody of> a managed entity via the Custody relation.

Direct Supertypes

[Controlling Actor](#)

Associations

 has custody of : [Managed Entity](#) [*] Subsets: has control over:[Controlled Entity](#)
through association: [Custody](#)

The entity a custodian has custody of.

9.6.9 Association Class Custody <>Relationship>>

The act of a custodian protecting or taking care of a managed entity.

Direct Supertypes

[Control](#)

Association Ends

 has custody of : [Managed Entity](#) [*] Subsets: has control over:[Controlled Entity](#)

The entity a custodian has custody of.

 in the custody of : [Custodian](#) [*] Subsets: has control over:[Controlled Entity](#)

The custodian of a managed entity.

9.6.10 Class Leader <<Role>>

A person who leads or commands a group, organization, or country.

Direct Supertypes

[Authority](#), [Controlling Actor](#), [Person](#)

Associations

 leads : [Organization](#) [1..*] Subsets: has control over:[Controlled Entity](#) member of:[Organization](#)
through association: [Leadership](#)

An organization a person leads.

9.6.11 Association Class Leadership <<Relationship>>

An person leading or governing an organization.

Direct Supertypes

[Control](#), [Membership](#), [Subject to Authority](#)

Association Ends

 leads : [Organization](#) [1..*] Subsets: has control over:[Controlled Entity](#) member of:[Organization](#)
 has leader : [Leader](#) [*] Subsets: has control over:[Controlled Entity](#) member of:[Organization](#)

An organization a person leads.

 has leader : [Leader](#) [*] Subsets: has control over:[Controlled Entity](#) member of:[Organization](#)

A person leading or directing an organization.

9.6.12 Class Managed Entity <<Role>>

Any entity for which the custody of or access to the entity is managed such that it can be trusted or protected. A managed entity is in the custody of a custodian via the Custody relation.

Direct Supertypes

[Controlled Entity](#)

Associations

 in the custody of : [Custodian](#) [*] Subsets: is controlled by:[Controlling Actor](#)
through association: [Custody](#)

The custodian of a managed entity.

9.6.13 Class Owner <>Role>>

Role of an actor that owns property.

[FIBO] Owner: A party in the ownership role; one that owns something. The thing owned is an Asset to that Party.

Direct Supertypes

[Controlling Actor](#)

Associations

 <>Sufficient>> owns : [Property](#) [1..*] Subsets: has control over:[Controlled Entity](#)
through association: [Ownership](#)

Property owned by an owner.

[FIBO] owns: to have (something) as one's own, possess

9.6.14 Association Class Ownership <>Relationship>>

Relationship defining the ownership of property by an owner.

[FIBO] Ownership: Ownership is the context in which some Party is said to own some Independent Thing. The Party is defined as such due to its being the owning party to that Thing.

Direct Supertypes

[Control](#)

Association Ends

 owns : [Property](#) [1..*] Subsets: has control over:[Controlled Entity](#)

Property owned by an owner.

[FIBO] owns: to have (something) as one's own, possess

 owned by : [Owner](#) [1..*] Subsets: has control over:[Controlled Entity](#)

Owner of an entity as property.

[FIBO] isOwnedBy: identifies the party that owns the asset.

[NIEM] ItemOwner

9.6.15 Association Class Possession <>Relationship>>

A relationship defining the physical possession of an item.

Direct Supertypes

Control

Association Ends

 possesses : [Controlled Entity](#) [*] Subsets: has control over:[Controlled Entity](#)

A controlled entity in the physical possession of a controlling actor.

 is possessed by : [Controlling Actor](#) [*] Subsets: has control over:[Controlled Entity](#)

The actor that possesses the subject controlled entity.

[NIEM] ItemPossessor

9.6.16 Class Property <>Role>>

Role of an entity which has an owner.

[FIBO] Asset: A thing held by some party and having some value.

Direct Supertypes

[Controlled Entity](#)

Associations

 <>Sufficient>> owned by : [Owner](#) [1..*] Subsets: is controlled by:[Controlling Actor](#)
through association: [Ownership](#)

Owner of an entity as property.

[FIBO] isOwnedBy: identifies the party that owns the asset.

[NIEM] ItemOwner

9.6.17 Association Class Subject to Authority <>Relationship>>

The relationship between an authority and what it has authority over.

Direct Supertypes

[Control](#)

Association Ends

 has authority over : [Controlled Entity](#) [*] Subsets: is controlled by:[Controlling Actor](#)

Resource an authority has authority over - may influence in some by setting policy or defining requirements.

[FIBO] governs

 is subject to authority : [Authority](#) [*] Subsets: is controlled by:[Controlling Actor](#)

The authority that has some control over a resource.

[FIBO] isGovernedBy

9.7 Threat-risk-conceptual-model::Generic Concept Library::Credentials

Concepts relating to identity and credential management.

9.7.1 Diagram: Credentials and Managed Identifiers

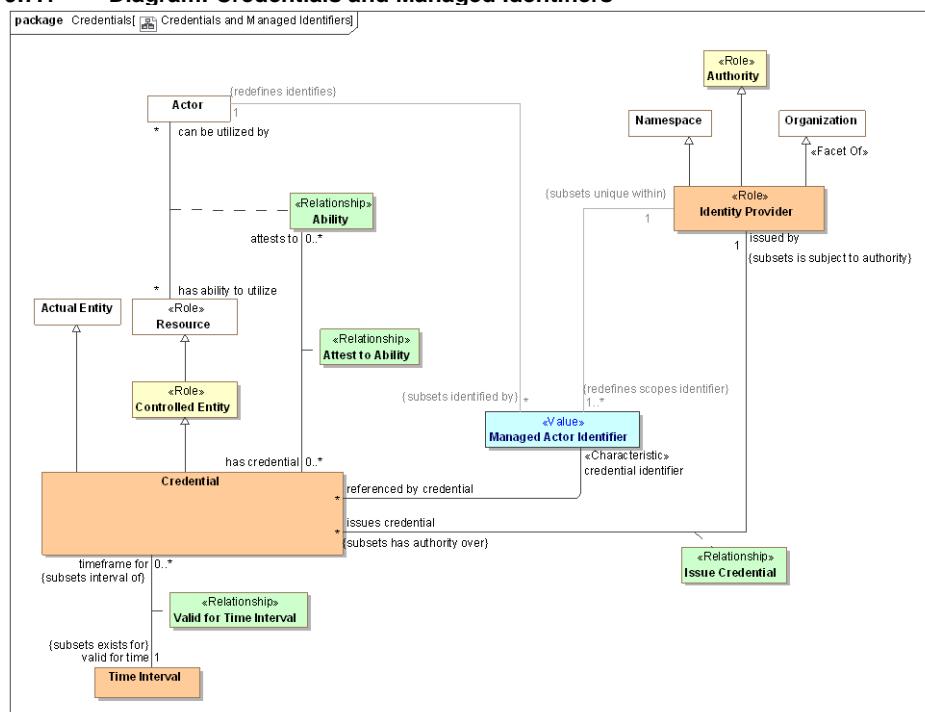


Figure 74. Credentials and Managed Identifiers

9.7.2 Association Actor Identifier of Credential

Association Ends

- / credential identifier : [Managed Actor Identifier](#) Subsets: is controlled by:[Controlling Actor](#)

Managed identifier used by a credential to identify the credential and/or actor.

 referenced by credential : [Credential](#) [*] Subsets: is controlled by:[Controlling Actor](#).

A credential that uses the subject managed identifier to identify the credential or actor.

9.7.3 Association Class Attest to Ability <>Relationship>>

Relationship between a credential and the abilities it attests to. Note that ability is a relationship between an actor and a resource, so the credentialled individual is the actor in this relationship, the actor is identified by an identifier referenced by the credential.

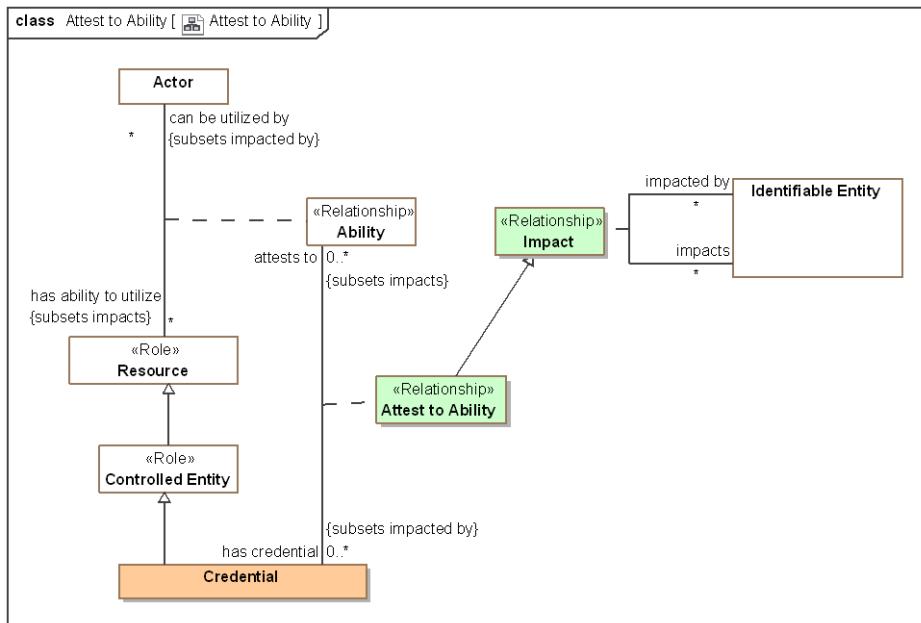


Figure 75. Attest to Ability

Direct Supertypes

[Impact](#), [Relationship](#)

Association Ends

 attests to : [Ability](#) [0..*] Subsets: is controlled by:[Controlling Actor](#)

A statement of a credentialled capability - that an actor has the stated ability to utilize a resource.

 has credential : [Credential](#) [0..*] Subsets: is controlled by:[Controlling Actor](#)

A physical or logical record of an assertion that a particular actor has a particular ability.

9.7.4 Class Credential

A credential is an attestation of qualification, competence, or authority issued to an individual by a third party with a relevant or de-facto authority or assumed competence to do so. Credentials can be physical (a house key), documents (a certificate) or virtual (a PKI key) and may be valid for a specific time frame and in specific context.

Direct Supertypes

[Actual Entity](#), [Controlled Entity](#)

Associations

/ credential identifier : [Managed Actor Identifier](#)

through association: [Actor Identifier of Credential](#)

Managed identifier used by a credential to identify the credential and/or actor.

█ attests to : [Ability](#) [0..*] Subsets: impacts:[Identifiable Entity](#)

through association: [Attest to Ability](#)

A statement of a credentialed capability - that an actor has the stated ability to utilize a resource.

█ issued by : [Identity Provider](#) [1] Subsets: is subject to authority:[Authority](#)

through association: [Issue Credential](#)

The identity provider issuing a credential By issuing the credential the identity provider is asserting the validity of the credential.

█ valid for time : [Time Interval](#) [1] Subsets: exists for:[Time Interval](#)

through association: [Valid for Time Interval](#)

Time interval over which a credential is valid (can be used to provide evidence for an ability).

9.7.5 Class Identity Provider <>Role>>

Role of an organization that validates identity and issues curated identifiers and credentials for entities.

Direct Supertypes

[Authority](#), [Namespace](#), [Organization](#)

Associations

/ <>Restriction>> : [Managed Actor Identifier](#) [1..*] Redefines: scopes identifier:[Unique Identifier](#)

█ issues credential : [Credential](#) [*] Subsets: has authority over:[Controlled Entity](#)

through association: [Issue Credential](#)

Credential issued by an identity provider. By issuing the credential the identity provider is asserting the validity of the credential.

9.7.6 Association Class Issue Credential <>Relationship>>

Issuance of and the assertion of the validity of a credential by an identity provider.

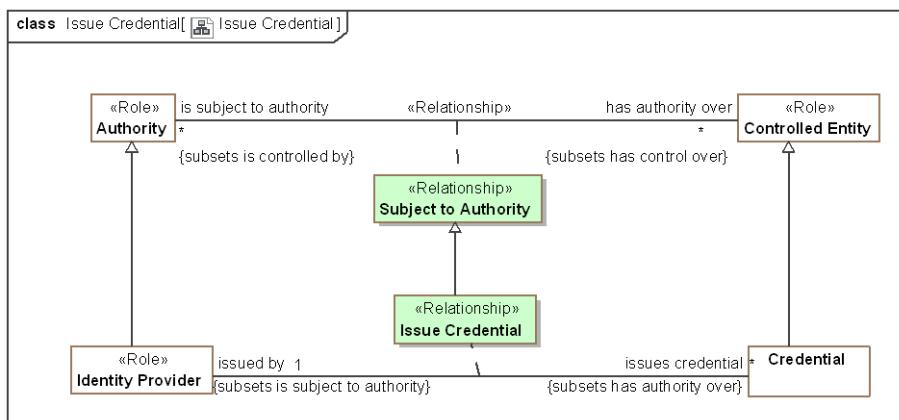


Figure 76. Issue Credential

Direct Supertypes

[Subject to Authority](#)

Association Ends

issues credential : [Credential](#) [*] Subsets: has authority over:[Controlled Entity](#)

Credential issued by an identity provider. By issuing the credential the identity provider is asserting the validity of the credential.

issued by : [Identity Provider](#) [1] Subsets: has authority over:[Controlled Entity](#)

The identity provider issuing a credential. By issuing the credential the identity provider is asserting the validity of the credential.

9.7.7 Class Managed Actor Identifier <>Value>>

An identifier managed by an identity provider who asserts the validity of the identifier. This includes technical/cyber identities as well as traditional identifiers such as passport numbers and corporate IDs. Identities can also be provided for systems, such as a SSL certificate.

Direct Supertypes

Unique Identifier

Associations

- / <>Restriction>> : [Identity Provider](#) [1] Subsets: unique within:[Namespace](#)
- / <>Restriction>> : [Actor](#) [1] Redefines: identifies:[Identifiable Entity](#)
- / referenced by credential : [Credential](#) [*]
 - through association: [Actor Identifier of Credential](#)

A credential that uses the subject managed identifier to identify the credential or actor.

9.7.8 Association Class Valid for Time Interval <>Relationship>>

Relationship describing the time interval for which a credential is valid.

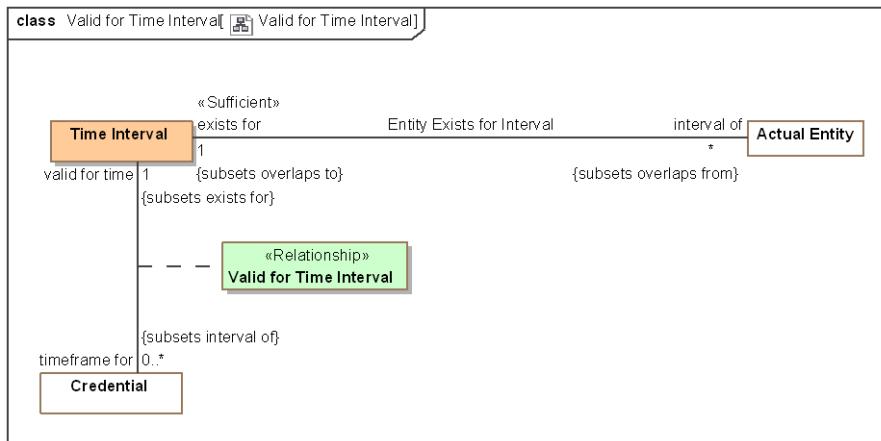


Figure 77. Valid for Time Interval

Direct Supertypes

[Entity Exists for Interval](#)

Association Ends

- / valid for time : [Time Interval](#) [1]

Time interval over which a credential is valid (can be used to provide evidence for an ability).

- / timeframe for : [Credential](#) [0..*]

Credential that is validated within the <valid for time> interval.

9.8 Threat-risk-conceptual-model::Generic Concept Library::Cyber

The Cyber package defines instances and subtypes of generic concepts specific to Cyber - computers, software and networks.

9.8.1 Diagram: Cyber

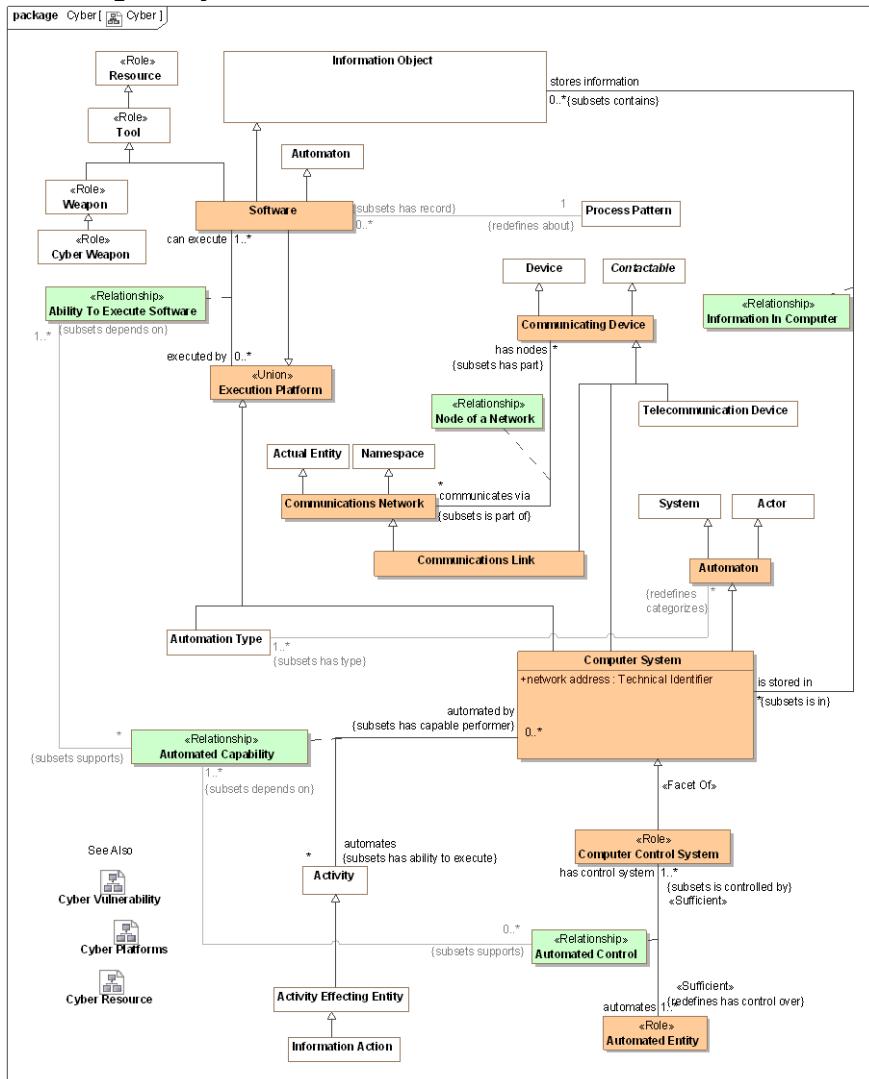


Figure 78. Cyber

9.8.2 Diagram: Cyber Platforms

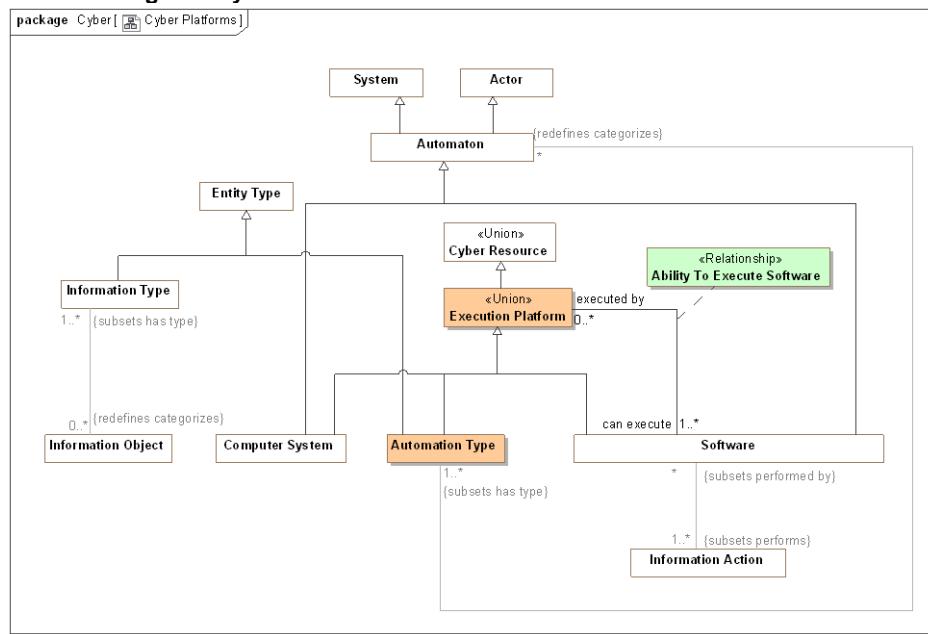


Figure 79. Cyber Platforms

9.8.3 Diagram: Cyber Resource

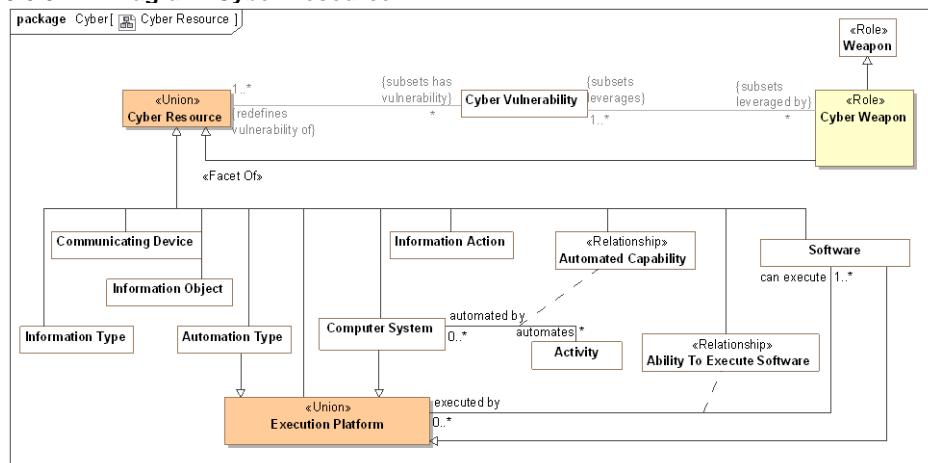


Figure 80. Cyber Resource

9.8.4 Association Class Ability To Execute Software <<Relationship>>

Relationship between software and platforms that can execute that software. Platforms include specific computers , types of computers and software.

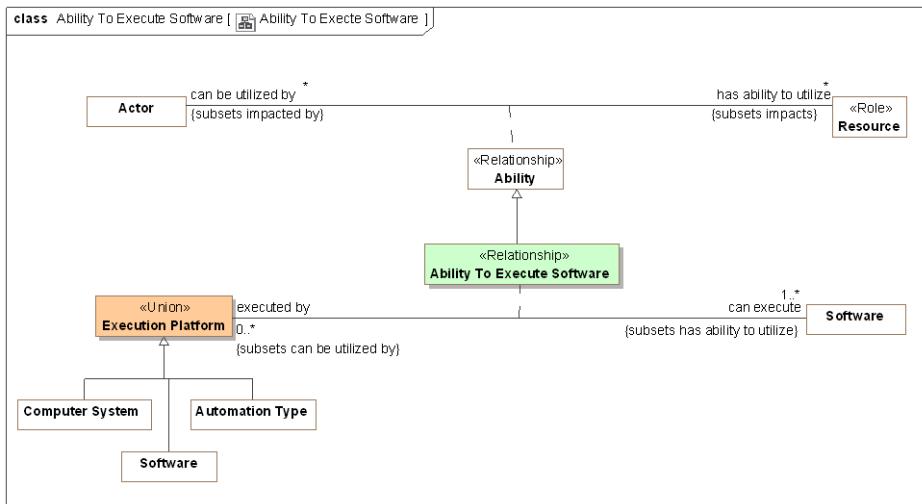


Figure 81. Ability To Execute Software

Direct Supertypes

Ability, Cyber Resource

Association Ends

 executed by : [Execution Platform](#) [0..*]

A computer platform (software, computer type or specific computer) able to execute specific software.

 can execute : [Software](#) [1..*]

Software a computer system, other software or computer type is able to execute.

Associations

/ <<Restriction>> : Automated Capability [*] Subsets: supports:Resource

9.8.5 Association Class Automated Capability <>Relationship>>

Capability of a specific computer system to automate activities.

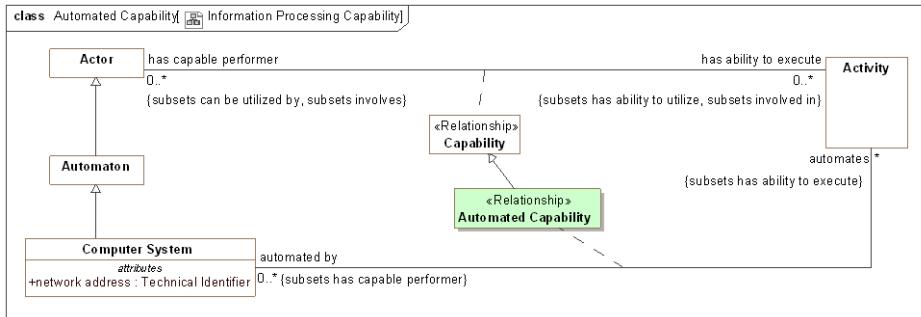


Figure 82. Information Processing Capability

Direct Supertypes

[Capability](#), [Cyber Resource](#)

Association Ends

automates : [Activity](#) [*] Subsets: supports:[Resource](#)

Activities a computer may automate.

automated by : [Computer System](#) [0..*] Subsets: supports:[Resource](#)

Computer system capable of automating an activity.

Associations

<>Restriction>> : [Automated Control](#) [0..*] Subsets: supports:[Resource](#)

<>Restriction>> : [Ability To Execute Software](#) [1..*] Subsets: depends on:[Resource](#)

9.8.6 Association Class Automated Control <>Relationship>>

Control of an entity by an automated control system - a computer and related software.

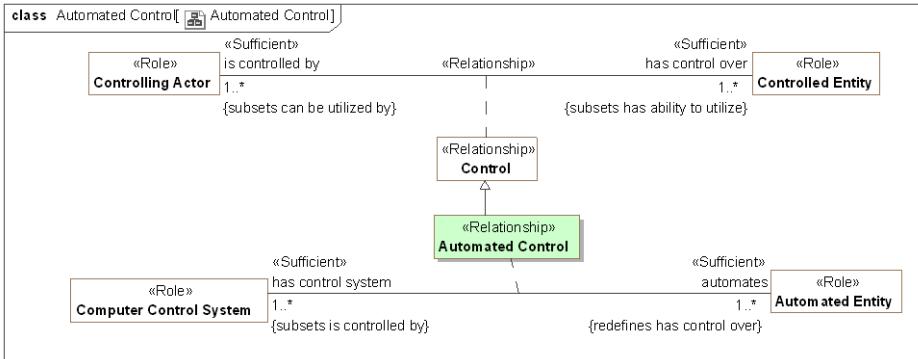


Figure 83. Automated Control

Direct Supertypes

Control

Associations Ends

automates : [Automated Entity](#) [1..*] Subsets: depends on: [Resource](#)

Entity that is controlled by a computer system.

has control system : [Computer Control System](#) [1..*] Subsets: depends on: [Resource](#)

Control system for an automated entity. e.g., an automated machine or facility.

Associations

/ <>Restriction>> : [Automated Capability](#) [1..*] Subsets: depends on: [Resource](#)

9.8.7 Class Automated Entity <>Role>>

Any actual entity all or partially controlled by automation.

Direct Supertypes

Controlled Entity

Associations

«Sufficient» has control system : [Computer Control System](#) [1..*] Subsets: is controlled by: [Controlling Actor](#)
through association: [Automated Control](#)

Control system for an automated entity. e.g., an automated machine or facility.

9.8.8 Class Automation Type

A categorization of computers and software across any dimension - chip type, operating system, language, manufacturer, virtual machine, etc. The automation type may be used to establish software compatibilities and vulnerabilities. Note that any automation may be categorized by multiple automation types.

Direct Supertypes

[Cyber Resource](#), [Entity Type](#), [Execution Platform](#)

Associations

/ <>Restriction>> : [Automaton](#) [*] Redefines: categorizes:[Thing](#)

9.8.9 Class Automaton

A machine or group of machines (most often a computer system, robot, or computerized swarm combined with software), or software that can perform actions in accordance with a process without another actor directing each step of the process. Distinguished from simple tools which facilitate an actor performing a process but have no innate ability to follow such a process.

Automation is distinguished from "legal entity" and "stakeholder", roles of some actors which indicates the ability to enter into legally binding agreements or have objectives (at this time no Automatons are legal entities or stakeholders but the model does not preclude the possibility).

Direct Supertypes

[Actor](#), [System](#)

Associations

/ <>Restriction>> : [Automation Type](#) [1..*] Subsets: has type:[Type](#)

9.8.10 Class Communicating Device

A device able to communicate or facilitate communications across a network.

Direct Supertypes

[Contactable](#), [Cyber Resource](#), [Device](#)

Associations

/ <>Restriction>> : [Communications Vulnerability](#) Subsets: has vulnerability:[Vulnerability](#)

█ communicates via : [Communications Network](#) [*] Subsets: is part of:[Identifiable Entity](#)

through association: [Node of a Network](#)

The network used by a communications device to send and receive information.

9.8.11 Class Communications Link

A physical or virtual link between communications devices allowing them to communicate.

Direct Supertypes

[Communicating Device](#), [Communications Network](#)

9.8.12 Class Communications Network

A physical or electronic system intended to facilitate communications between entities. Includes communications channels, computer networks, physical mail and RF networks.

Direct Supertypes

[Actual Entity](#), [Namespace](#)

Attributes

- ⦿ provides security level : [Communications Security Level](#)

The level of security asserted for the subject communications network.

Associations

█ has nodes : [Communicating Device](#) [*] Subsets: has part:[Identifiable Entity](#)
through association: [Node of a Network](#)

The communicating nodes of a communications network. Nodes are able to communicate with each other across the network.

↙ : [Contact Means](#) [*] Redefines: scopes identifier:[Unique Identifier](#)

9.8.13 Class Computer Control System <>Role>>

A computer control system is a device, or set of devices, that manages, commands, directs or regulates the behavior of other devices or systems. Industrial control systems are used in industrial production for controlling equipment or machines.

Direct Supertypes

[Computer System](#), [Controlling Actor](#)

Associations

█ <>Sufficient>> automates : [Automated Entity](#) [1..*] Redefines: has control over:[Controlled Entity](#)
through association: [Automated Control](#)

Entity that is controlled by a computer system.

9.8.14 Class Computer System

An identifiable and physical computer system that acts as an automaton agent performing processes.
[ISO/IEC 10514-1:1996] The combination of hardware and, optionally, firmware and software (e.g. operating system) that enables the execution of software.

Direct Supertypes

[Automaton](#), [Communicating Device](#), [Container](#), [Cyber Resource](#), [Execution Platform](#)

Attributes

- network address : [Technical Identifier](#)

Electronic address which allows communication with a computer system as a node on a network.

Associations

- / <>Restriction>> : [Information System Vulnerability](#) Subsets: has vulnerability:[Vulnerability](#)
- █ automates : [Activity](#) [*] Subsets: has ability to execute:[Activity](#)
through association: [Automated Capability](#)

Activities a computer may automate.

- █ stores information : [Information Object](#) [0..*] Subsets: contains:[Actual Entity](#)
through association: [Information In Computer](#)

Information stored in a computer.

9.8.15 Class Cyber Resource <>Union>>

Resources that, together, make up information systems capabilities and may be vulnerable to attack or used in an attack.

Associations

- / <>Restriction>> : [Cyber Vulnerability](#) [*] Subsets: has vulnerability:[Vulnerability](#)

9.8.16 Class Cyber Weapon <>Role>>

A software weapon able to exploit the vulnerabilities of a cyber system.

Direct Supertypes

[Cyber Resource](#), [Weapon](#)

Associations

- / <>Restriction>> : [Cyber Vulnerability](#) [1..*] Subsets: leverages:[Vulnerability](#)

9.8.17 Class Execution Platform <>Union>>

Computer hardware or software that provides the capability of executing software. This includes processors, operating systems and virtual machines.

Direct Supertypes

[Cyber Resource](#)

Associations

can execute : [Software](#) [1..*] Subsets: has ability to utilize:[Resource](#)
through association: [Ability To Execute Software](#)

Software a computer system, other software or computer type is able to execute.

9.8.18 Association Class Information In Computer <<Relationship>>

Relationship defining information stored in a computer system.

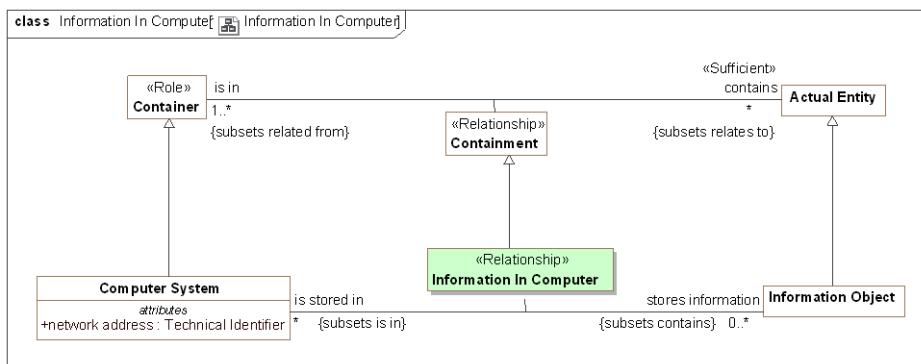


Figure 84. Information In Computer

Direct Supertypes

[Containment](#)

Association Ends

stores information : [Information Object](#) [0..*] Subsets: has ability to utilize:[Resource](#)

Information stored in a computer.

is stored in : [Computer System](#) [*] Subsets: has ability to utilize:[Resource](#)

System storing an information object.

9.8.19 Association Class Node of a Network <<Relationship>>

Relationship between a network and nodes that may communicate on that network.

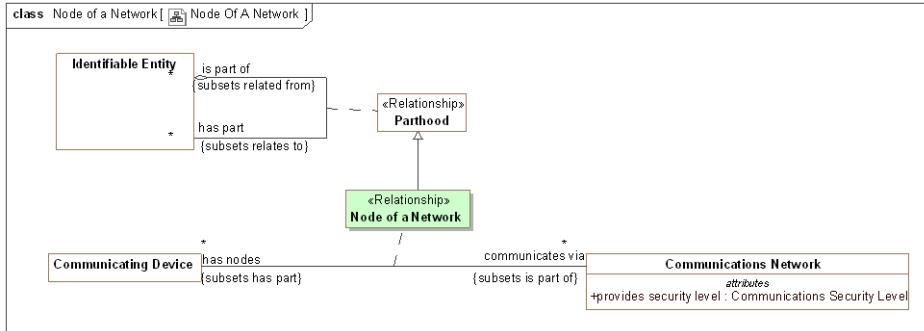


Figure 85. Node Of A Network

Direct Supertypes

[Parthood](#)

Association Ends

communicates via : [Communications Network](#) [*] Subsets: has ability to utilize:[Resource](#)

The network used by a communications device to send and receive information.

has nodes : [Communicating Device](#) [*] Subsets: has ability to utilize:[Resource](#)

The communicating nodes of a communications network. Nodes are able to communicate with each other across the network.

9.8.20 Class Software

Programs and other operating information used by a computer to control its function through the definition of a process.

Direct Supertypes

[Automaton](#), [Cyber Resource](#), [Execution Platform](#), [Information Object](#), [Tool](#)

Associations

- / <<Restriction>> : [Information Action](#) [1..*] Subsets: performs:[Activity](#)
- / <<Restriction>> : [Software Vulnerability](#) Redefines: has vulnerability:[Vulnerability](#)
- █ executed by : [Execution Platform](#) [0..*] Subsets: can be utilized by:[Actor](#)
through association: [Ability To Execute Software](#)

A computer platform (software, computer type or specific computer) able to execute specific software.

/ <<Restriction>> : [Process Pattern](#) [1] Redefines: about:[Identifiable Entity](#)

9.9 Threat-risk-conceptual-model::Generic Concept Library::Enterprises

In a generic sense, an enterprise is any organization or collection of organizations that has a common set of goals and/or a single bottom line. An enterprise, by that definition, can encompass a Military Department, DoD as a whole, a division within an organization, an organization in a single location, or a chain of geographically distant organizations linked by a common management or purpose. An enterprise today is often thought of as an extended enterprise where partners, suppliers, customers, along with their activities and supporting systems, are included in the Architectural Description. [DoDAF 2.0] section 51, Defining the Enterprise

The concept of enterprise builds on the concept of a system.

9.9.1 Diagram: Enterprise

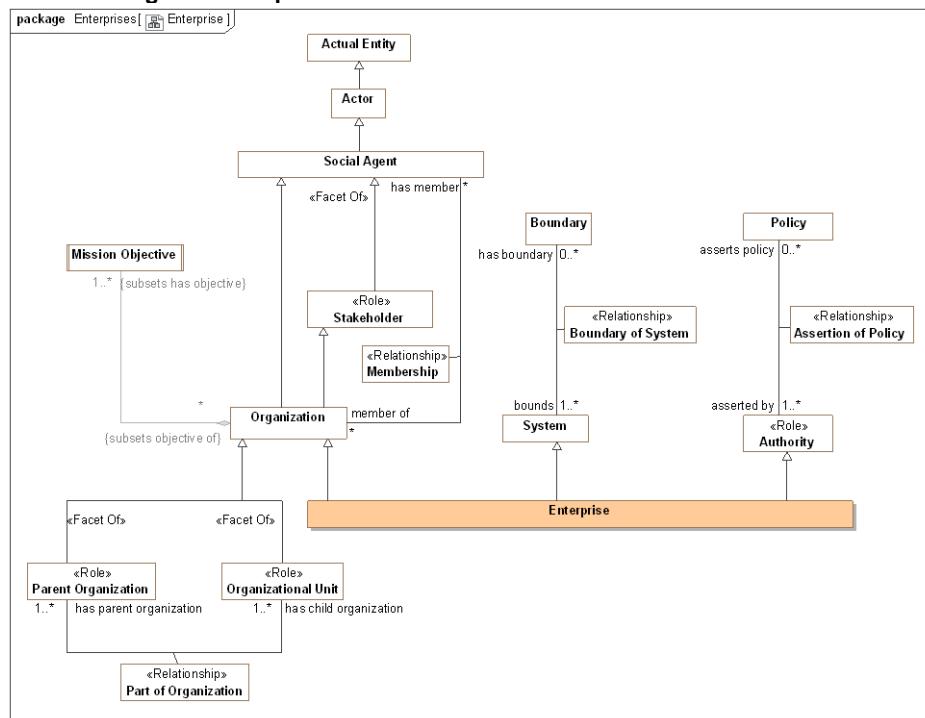


Figure 86. Enterprise

9.9.2 Class Enterprise

An enterprise is a stakeholder organization, organized as a system, with a mission, members, and authority over resources to accomplish its mission(s). An enterprise provides context for operations and analysis. An enterprise may have parts - its divisions or departments.

[BMM] Organizational Unit:

Direct Supertypes

[Authority](#), [Organization](#), [Risk Owner](#), [System](#)

9.10 Threat-risk-conceptual-model::Generic Concept Library::Entities

The foundation library provides fundamental concepts that apply to most domains or areas of concern. These fundamental concepts are specialized, combined and related for more specific concerns, such as risk management. These fundamental concepts provide for links between domains, systems, organizations, cultures and stakeholders. Unless stated otherwise, these concepts are intended to be mixed together to fully describe something in the "real world". The foundation builds on the [conceptual model](#)[conceptual reference model](#) defined in [SIMF] (Semantic Information Modeling for Federation), which is included by reference. By using SIMF we avoid redundant definitions of concepts and also allow for easy extension of threat/risk by using the SIMF modeling capabilities.

Note that something may be classified by any number of types (e.g., a transfer of custody that is an actual situation that happened in the past).

9.10.1 Diagram: Identifiable Entity

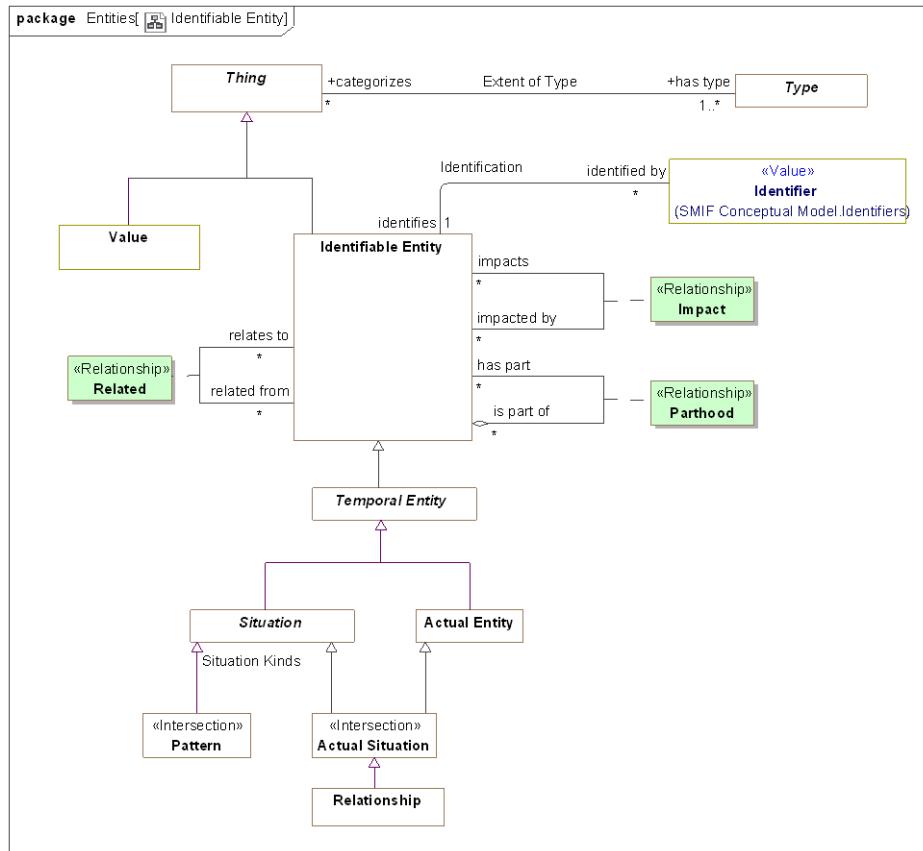


Figure 87. Identifiable Entity

The above is a summary diagram intended to show significant classes used in the concept library.

9.10.2 Diagram: Identifiable Entity Relationships

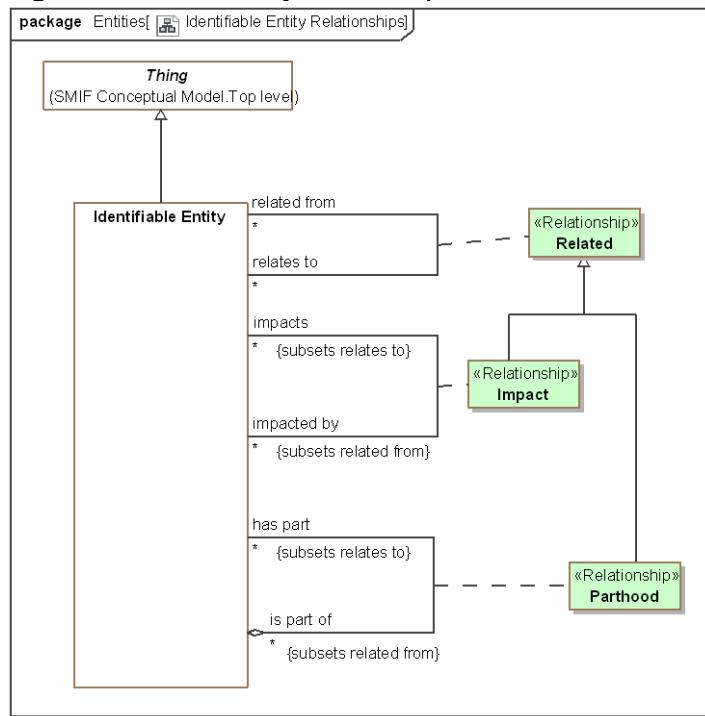


Figure 88. Identifiable Entity Relationships

9.10.3 Association Class Impact <<Relationship>>

Relationship between some entity and another on which it has some kind of impact or effect.

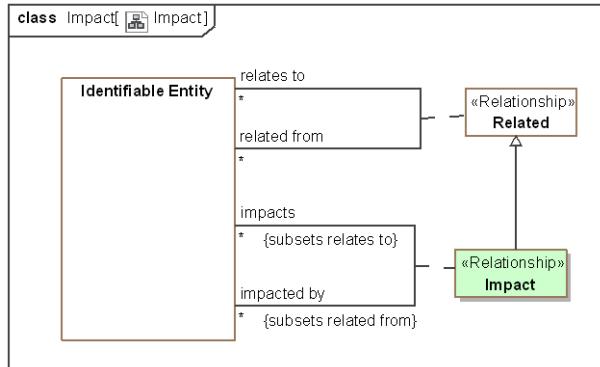


Figure 89. Impact

Direct Supertypes

[Related](#)

Association Ends

█ impacts : [Identifiable Entity](#) [*] Redefines: about: [Identifiable Entity](#)

Entity that the subject entity impacts in any way.

█ impacted by : [Identifiable Entity](#) [*] Redefines: about: [Identifiable Entity](#)

Entity that is impacted by another in any way..

9.10.4 Association Class Parthood <<Relationship>>

Relationship defining one thing as a part of another. More specific concepts of parthood and mereology (the study of parts and their relations) may subtype Parthood.

[IDEAS] wholePart: The whole-part pattern establishes a relationship between individual elements, asserting that one Object element is composed of the other element.

[IDEAS] A couple that asserts one (part) Individual is part of another (whole) Individual.

[ISO 1087] partitive relation: part-whole relation relation between two concepts (3.2.1) where one of the concepts constitutes the whole and the other concept a part of that whole

[DOLCE] Parthood

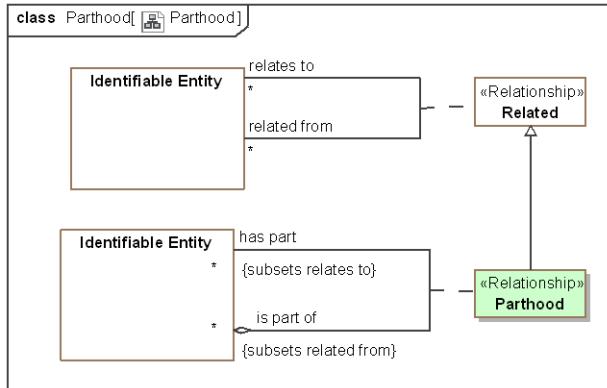


Figure 90. Parthood

Direct Supertypes

[Related](#)

Association Ends

has part : [Identifiable Entity](#) [*] *Redefines*: about: [Identifiable Entity](#)

Entity that is a part of the subject entity (the whole) such that the part is essential to the whole.
This is a general concept of part and does not assume exclusivity of partness or total part inclusion.

[FIBO] hasPart

[ISO 1087] partitive concept: concept (3.2.1) in a partitive relation (3.2.22) viewed as one of the parts making up the whole

is part of : [Identifiable Entity](#) [*] *Redefines*: about: [Identifiable Entity](#)

Composite entity (whole) of which this entity is a part.

[FIBO] isPartOf

[ISO 1087] comprehensive concept: concept (3.2.1) in a partitive relation (3.2.22) viewed as the whole

9.10.5 Association Class Related <<Relationship>>

Related defines relationships as first-class entities that are "situations" that may have conditions, context or a time frame. "Related" is the implicit supertype of all entity relationships such that any relationship can be traced between entities. Note that the generalization to Related may not be shown on diagrams.

Note that in UML relationships that are "definitional" and not expected to be time or contextually dependent are shown as regular UML associations where as potentially contextual or time-bound relationships are shown as association classes. This is a notational convention and does not have semantic intent to avoid early commitment to such considerations.

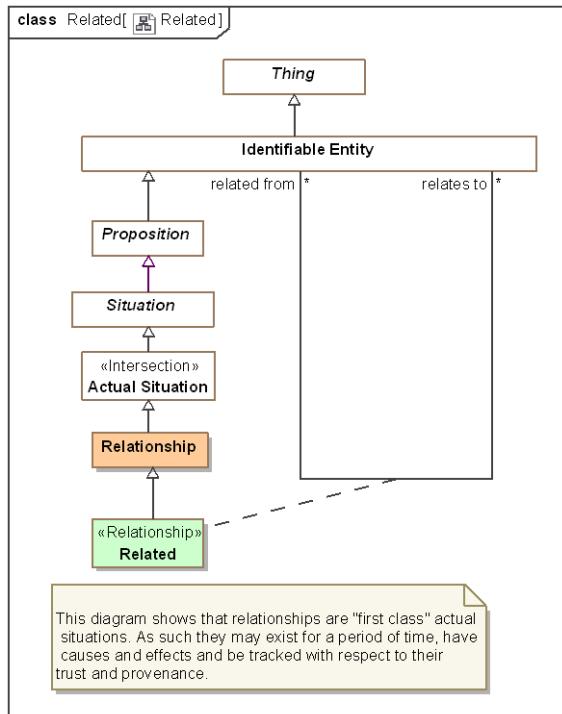


Figure 91. Related

Direct Supertypes

[Relationship](#)

Association Ends

 relates to : [Identifiable Entity](#) [*] Redefines: about: [Identifiable Entity](#)

A generic relationship to capture arbitrary relationships that do not have more specific meaning. <relates> is the implicit supertype of all relationships between entities (not including metadata). Note that to remove diagram clutter, subsets of "relates" may not show the subset on all diagrams.

 related from : [Identifiable Entity](#) [*] Redefines: about: [Identifiable Entity](#)

9.11 Threat-risk-conceptual-model::Generic Concept Library::Events and Activities

Events are things that occur in time, impacting the things involved in those events. Events include actual events as well as patterns of events that describe a process.

9.11.1 Diagram: Events and Activities

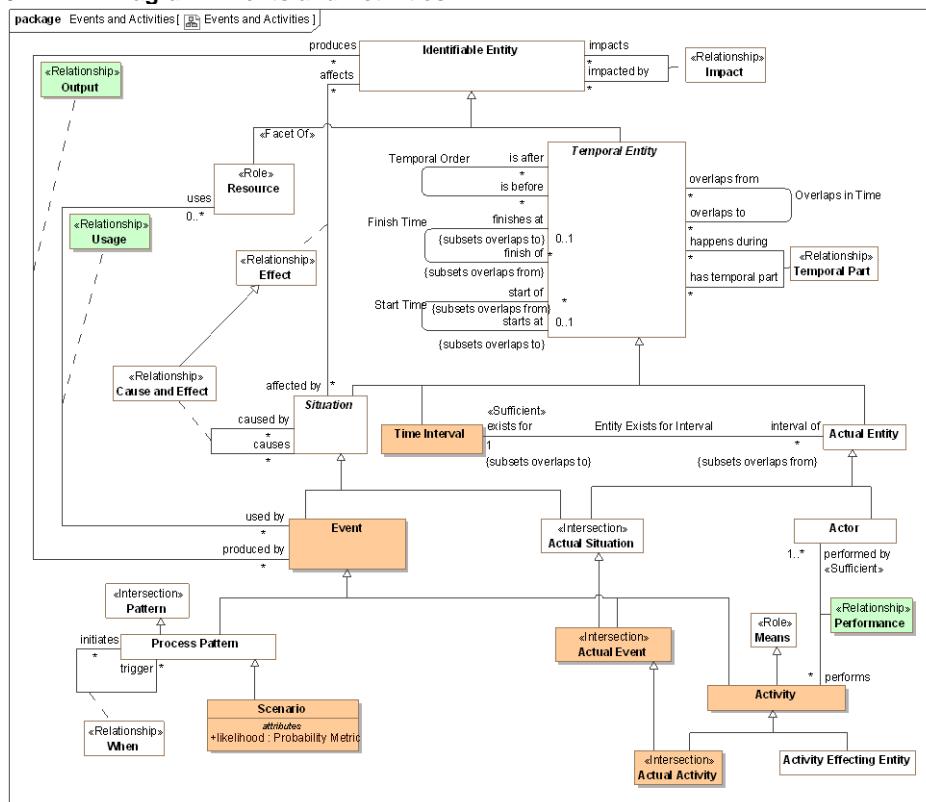


Figure 92. Events and Activities

9.11.2 Class Activity

An Event performed by one or more actors intended to meet a need.
[UAF] Work, not specific to a single organization, weapon system or individual that transforms inputs (Resources) into outputs (Resources) or changes their state.

Direct Supertypes

[Event](#), [Means](#)

Associations

 has capable performer : [Actor](#) [0..*] Subsets: involves:[Actor](#) can be utilized by:[Actor](#)
through association: [Capability](#)

Actor capable of performing an process.

 may be performed by : [Actor](#) [*] Redefines: can be utilized by:[Actor](#) performed by:[Actor](#)
through association: [Permission](#)

Actors that have permission to perform the subject activity.

 automated by : [Computer System](#) [0..*] Subsets: has capable performer:[Actor](#)
through association: [Automated Capability](#)

Computer system capable of automating an activity.

 <>Sufficient>> performed by : [Actor](#) [1..*] Subsets: involves:[Actor](#) impacted by:[Identifiable Entity](#)
through association: [Performance](#)

The actor which is the performer of an activity.

9.11.3 Class Actor

An entity capable of behavior - performing an activity or process.

[IDEAS] Agent: Something capable of action.

[FIBO] AutonomousAgent: An agent is an autonomous individual that can adapt to and interact with its environment.

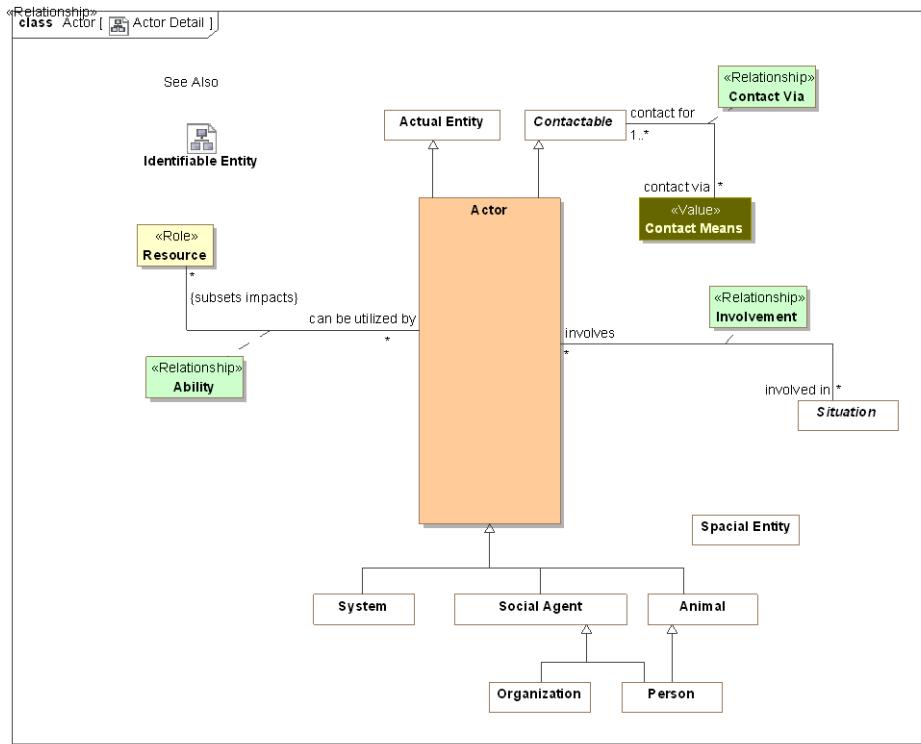


Figure 93. Actor Detail

Direct Supertypes

[Actual Entity](#), [Contactable](#)

Associations

has ability to utilize : [Resource](#) [*] Subsets: impacts:[Identifiable Entity](#)
through association: [Ability](#)

A resource an actor can employ as part of a capability.

has ability to execute : [Activity](#) [0..*] Subsets: has ability to utilize:[Resource](#) involved in:[Situation](#)
through association: [Capability](#)

The ability of an actor to perform a process.

lost by : [Lose Ability](#) [0..*] Subsets: affected by:[Situation](#)
through association: [Weakened Actor](#)

Action that causes a loss of control.

- ─ obtained by : [Obtain Ability](#) [0..*] Subsets: affected by:[Situation](#)
through association: [Strenthened Actor](#)

Method by which control is obtained.

- ─ <>Restriction>> : [Managed Actor Identifier](#) [*] Subsets: identified by:[Identifier](#)
- ─ performs at : [Place](#) [*] Subsets: has ability to utilize:[Resource](#)
through association: [Operating Location](#)

Places where an actor perform activities.

- ─ has permission to perform : [Activity](#) [*] Subsets: has ability to execute:[Activity](#) performs:[Activity](#)
through association: [Permission](#)

Activity the actor has permission to perform.

- ─ <>Sufficient>> performs : [Activity](#) [*] Subsets: impacts:[Identifiable Entity](#) involved in:[Situation](#)
through association: [Performance](#)

An activity performed (executed or enacted) by an actor.

- ─ involved in : [Situation](#) [*] Subsets: relates to:[Identifiable Entity](#)
through association: [Involvement](#)

Situations in which an actor has any kind of involvement.

9.11.4 Class Actual Activity <>Intersection>>

A specific, actual, activity that has or may happen.

Direct Supertypes

- [Activity](#), [Actual Event](#)

9.11.5 Class Actual Event <>Intersection>>

A specific individual event that has happened, is happening or may happen.

[FIBO] Occurrence: An Occurrence is a happening of an OccurrenceKind. Each Occurrence has a DateTimeStamp, which identifies when the Occurrence happened, and a Location (possibly virtual), that identifies where the Occurrence happened.

Direct Supertypes

- [Actual Situation](#), [Event](#)

Associations

 enactment of : [Process Pattern](#) [0..1] Subsets: caused by:[Situation](#)
through association: [Invoke Process](#)

Process enacted by an Invoke Process

9.11.6 Class Event

An Event is something that happens (a.k.a. occurs). A dynamic situation (past, present or future) composed of a set of things changing over a period of time. e.g., a rock falling.

Events are not limited in their timeframe. Events can have long or short timeframes, from an instant to infinity and beyond.

An Event that is "performed by" an actor is considered an activity.

[DOLCE] Perdurant

[BFO] Event: perdurant that is related to exactly two states (its pre-state and its post-state).
An event is related to the states before and after it has happened.

[NIEM] ActivityType

Direct Supertypes

[Situation](#)

Associations

 <>Sufficient>> produces : [Identifiable Entity](#) [*] Subsets: affects:[Identifiable Entity](#)
through association: [Output](#)

Resources produced by a process or actual event

 <>Sufficient>> uses : [Resource](#) [0..*] Subsets: affects:[Identifiable Entity](#)
through association: [Usage](#)

A resources used by a process or actual event.

 : [Process Action](#) Subsets: affected by:[Situation](#)

9.11.7 Association Class Output <>Relationship>>

Outputs from a process or actual event - the things or situations it creates.

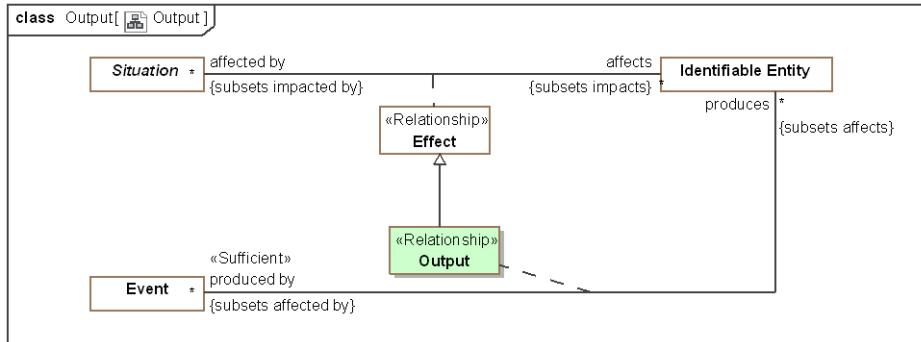


Figure 94. Output

Direct Supertypes

[Effect](#)

Association Ends

 produces : [Identifiable Entity](#) [*] Subsets: affected by:[Situation](#)

Resources produced by a process or actual event

 produced by : [Event](#) [*] Subsets: affected by:[Situation](#)

Events which produce an entity.

9.11.8 Association Class Performance <<Relationship>>

Performance is the act of an actor as the driving force in the execution of an activity. Related to "Capability" as the ability to perform.

[DOLCE] Subtype of Participation

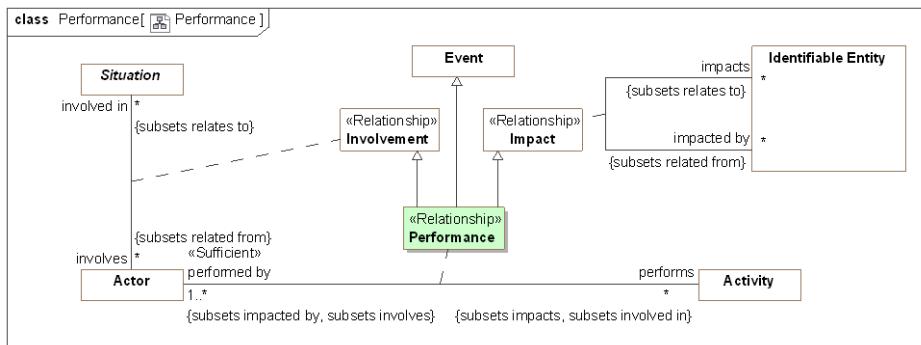


Figure 95. Performance

Direct Supertypes

[Event](#), [Impact](#), [Involvement](#)

Association Ends

performs : [Activity](#) [*] Subsets: affected by:[Situation](#)

An activity performed (executed or enacted) by an actor.

performed by : [Actor](#) [1..*] Subsets: affected by:[Situation](#)

The actor which is the performer of an activity.

9.11.9 Association Class Usage <<Relationship>>

Inputs to a process or actual event - what it uses

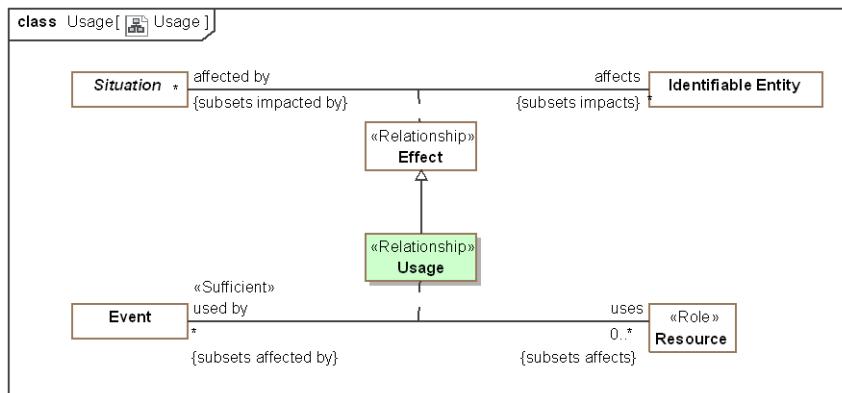


Figure 96. Usage

Direct Supertypes

[Effect](#)

Association Ends

uses : [Resource](#) [0..*] Subsets: affected by:[Situation](#)

A resources used by a process or actual event.

used by : [Event](#) [*] Subsets: affected by:[Situation](#)

A process or actual event that is used by a resource for the resource to fulfill its function.

9.12 Threat-risk-conceptual-model::Generic Concept Library::Identifiers and Coordinates

Identification connects identifiers with the entity they identify. Identifiers are values, that is they are immutable "data". An entity may be assigned different identifiers over time and may have many at any one time.

The base Identifier class (defined in SIMF) identifies a set of entities and is not assumed to be unique or to identify only one entity. For example, a name is an identifier but many people could have the same name and a person could have multiple names. Identifiers and the relation to an entity may be contextual.

Identifiers should not be confused with Identity, which is an abstraction of individuality that provide the foundation for identifiers.

The class of Unique Identifiers is more typical of I.T. systems and managed identifiers, such as driver's license numbers. A unique identifier is assumed unique within exactly one Namespace.

Subtypes of Identifier may be specific to identifying particular kinds of entities. For example, a Location Identifier (such as an address or GPS coordinate) is specific to identifying locations.

Note that as with all concepts, identifiers are independent of representation. Since names are so often textual, we also define a representation of names - "Textual Name".

The generic library of identifiers extends the SIMF identifiers with the concepts of coordinates.

9.12.1 Diagram: Identifiers

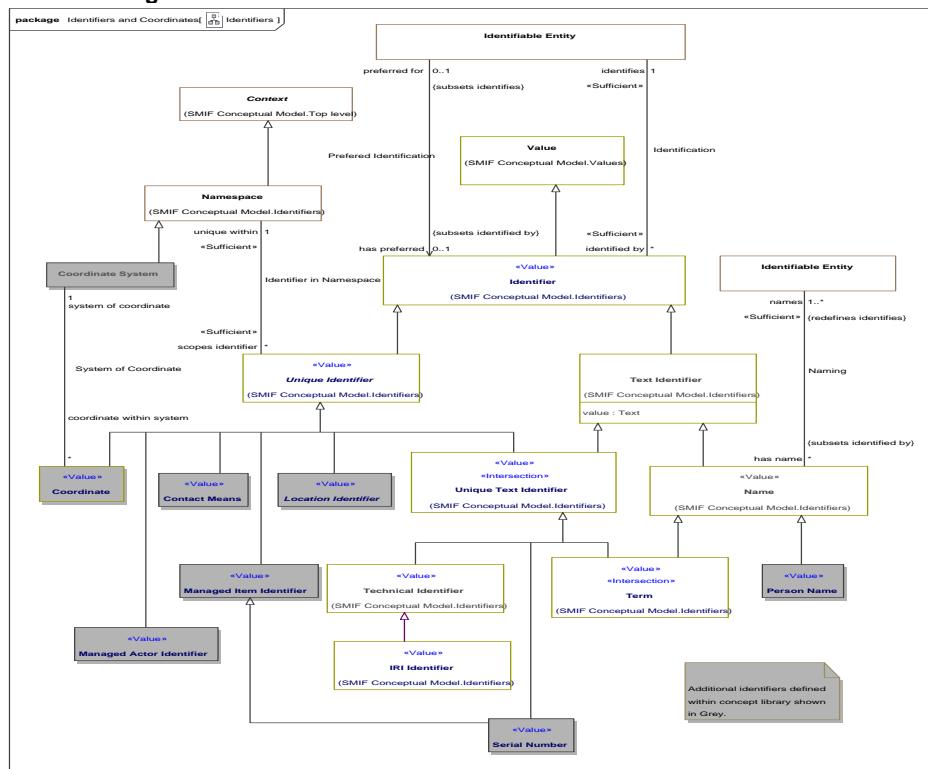


Figure 97. Identifiers

9.12.2 Class Coordinate <<Value>>

Any set of magnitudes that serve to define the position of a point, line, or the like, by reference to a coordinate system.

Direct Supertypes

Unique Identifier

Associations

/ system of coordinate : [Coordinate System](#) [1]

through association: System of Coordinate

The set of rules and reference points used for interpreting a coordinate.

9.12.3 Class Coordinate System

A reference system for a coordinate. e.g., WGS-84.

[OGC] Set of mathematical rules for specifying how coordinates are to be assigned to points.

Direct Supertypes

[Namespace](#)

Associations

/ coordinate within system : [Coordinate](#) [*]

through association: [System of Coordinate](#)

A particular coordinate identifying an entity within the scope of a coordinate system.

9.12.4 Association System of Coordinate

Relationship between a coordinate and a system of coordinates that defines how the coordinate is to be interpreted.

Association Ends

/ system of coordinate : [Coordinate System](#) [1]

The set of rules and reference points used for interpreting a coordinate.

/ coordinate within system : [Coordinate](#) [*]

A particular coordinate identifying an entity within the scope of a coordinate system.

9.13 Threat-risk-conceptual-model::Generic Concept Library::Information

Concepts relating to information (including data) about entities.

9.13.1 Diagram: Information Action

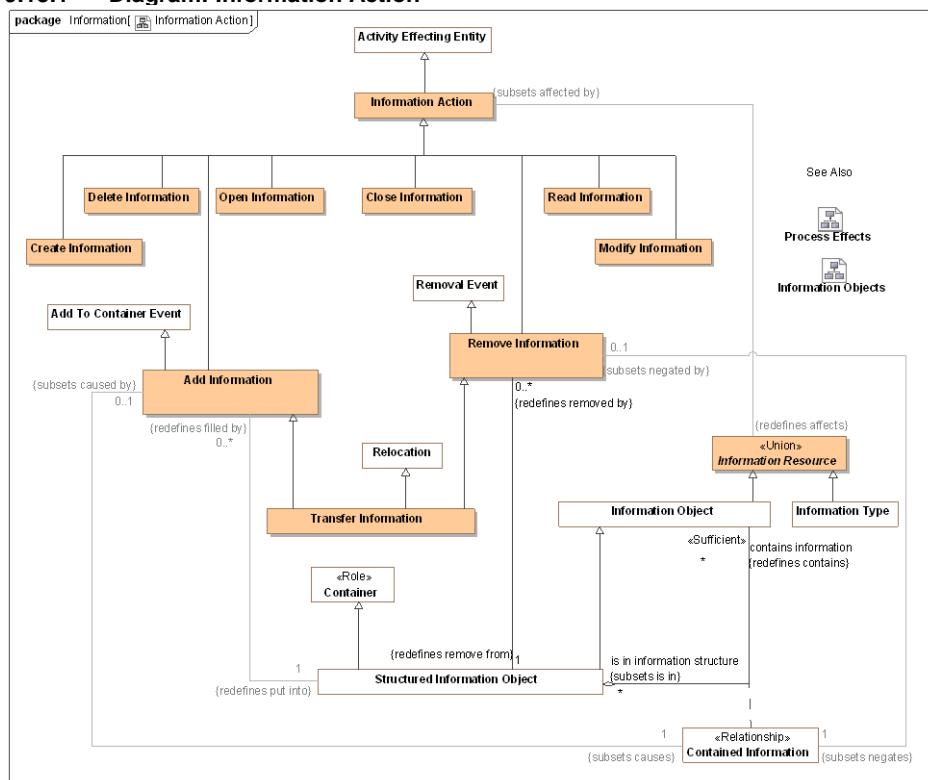


Figure 98. Information Action

9.13.2 Diagram: Information Objects

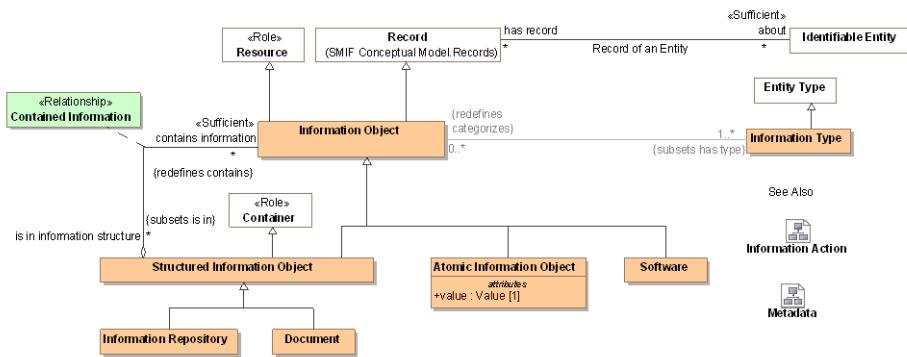


Figure 99. Information Objects

9.13.3 Diagram: Metadata

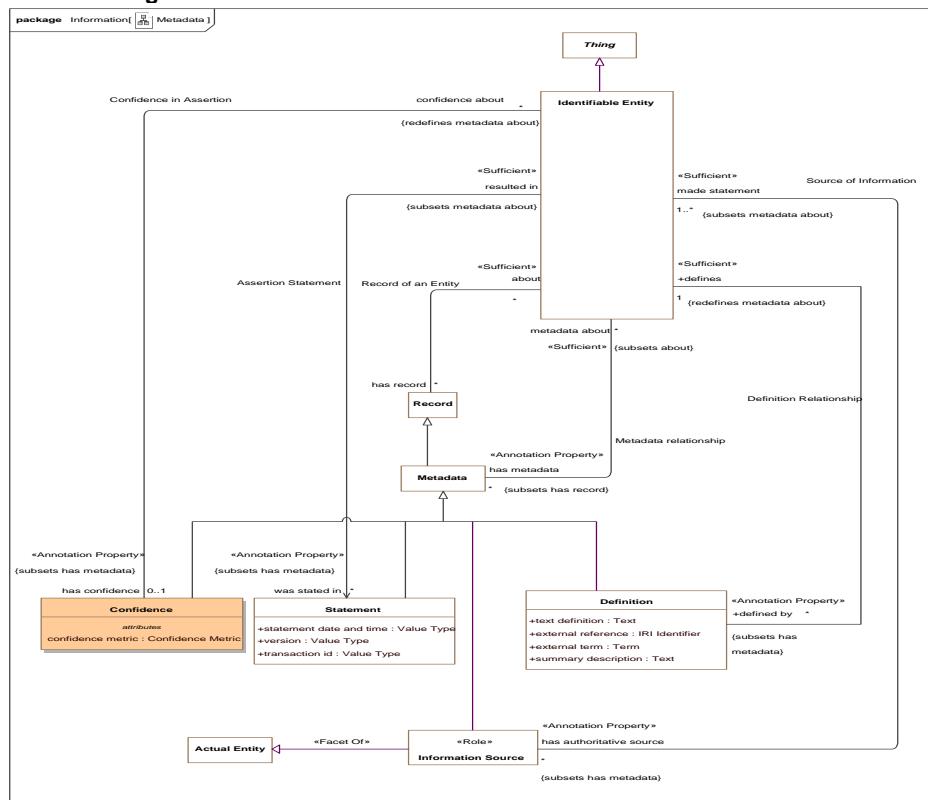


Figure 100. Metadata

9.13.4 Class Add Information

An action to add information to a repository or information structure.

Direct Supertypes

[Add To Container Event](#), [Information Action](#)

Associations

- / <<Restriction>> : [Structured Information Object](#) [1] Redefines: put into:[Container](#)
- / <<Restriction>> : [Contained Information](#) [1] Subsets: causes:[Situation](#)

9.13.5 Class Atomic Information Object

An atomic information object is a managed piece of information composed entirely of a single value. e.g. an MP3 representation of a song. Note that different viewpoints and abstractions may not agree on what is "atomic". e.g. a music editor may consider a song a series of samples.

Direct Supertypes

[Information Object](#)

Attributes

- ◊ value : [Value](#) [1]

Atomic value associated with an atomic information object.

9.13.6 Class Close Information

An action that removes information from visibility.

Direct Supertypes

[Information Action](#)

9.13.7 Class Confidence

A statement and measure of the confidence in any fact or set of facts about an entity.

Direct Supertypes

[Metadata](#)

Attributes

- ◊ confidence metric : [Confidence Metric](#)

A metric reflecting confidence in an assertion condition or effect.

Associations

/ <<Annotation Property>> confidence about : [Identifiable Entity](#) [*] Redefines: metadata about:[Identifiable Entity](#)

through association: [Confidence in Assertion](#)

Subject of confidence; the facts, situations or subject that confidence is being evaluated for.

9.13.8 Association Confidence in Assertion

A relationship relating a degree of confidence with the topic or subject of that confidence. Confidence is metadata about statements in a model; the degree of belief in those statements.

Association Ends

/ confidence about : [Identifiable Entity](#) [*] Redefines: metadata about: [Identifiable Entity](#)

Subject of confidence; the facts, situations or subject that confidence is being evaluated for.

/ has confidence : [Confidence](#) [0..1] Redefines: metadata about: [Identifiable Entity](#)

Confidence is a metric quantifying the belief that the facts asserted about the entity are true and valid.

9.13.9 Association Class Contained Information <>Relationship>>

Relationship connecting an information container with what it contains.

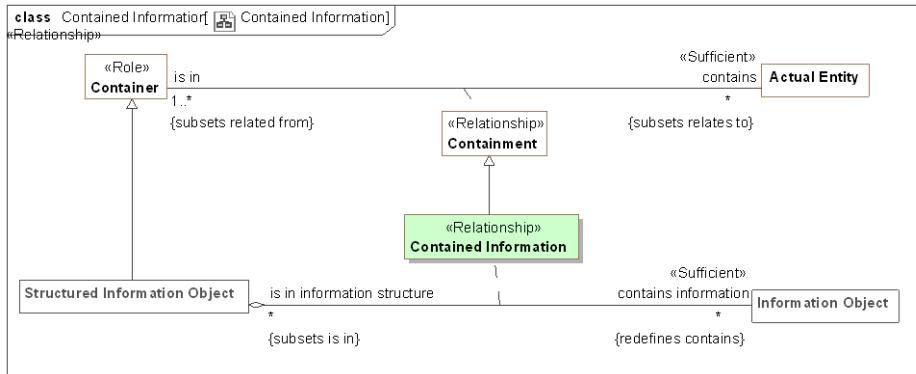


Figure 101. Contained Information

Direct Supertypes

[Containment](#)

Association Ends

/ contains information : [Information Object](#) [*] Redefines: metadata about: [Identifiable Entity](#)

An information object structurally contained in another.

/ is in information structure : [Structured Information Object](#) [*] Redefines: metadata about: [Identifiable Entity](#)

Structural containment of an information object within an information object.

Associations

/ <>Restriction>> : [Add Information](#) [0..1] Subsets: caused by:[Situation](#)

/ <>Restriction>> : [Remove Information](#) [0..1] Subsets: negated by:[Situation](#)

9.13.10 Class Create Information

An action that creates information.

Direct Supertypes

[Create, Information Action](#)

9.13.11 Class Delete Information

An action to delete information, erase it or render it inaccessible.

Direct Supertypes

[Destroy, Information Action](#)

9.13.12 Class Document

A collection of information about a topic, frequently containing some analysis or summary, intended for use by a stakeholder.

Direct Supertypes

[Structured Information Object](#)

9.13.13 Class Information Action

An action that impacts information objects.

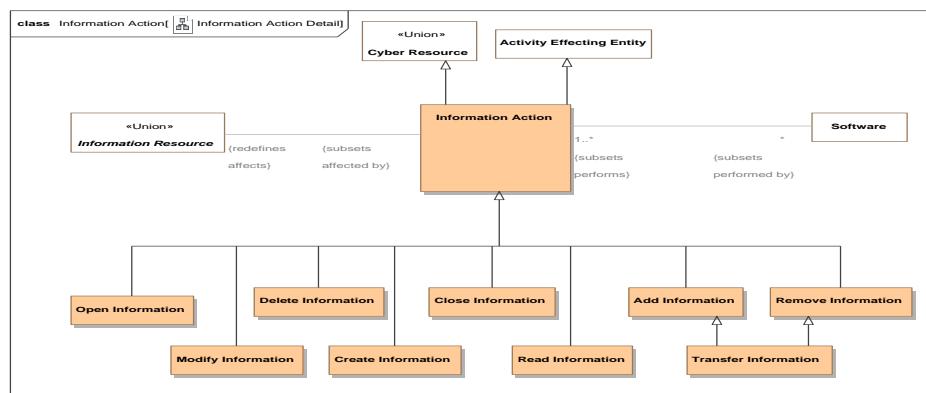


Figure 102. Information Action Detail

Direct Supertypes

[Activity Effecting Entity, Cyber Resource](#)

Associations

- / <>Restriction>> : [Software](#) [*] Subsets: performed by:[Actor](#)
- / <>Restriction>> : [Information Resource](#) Redefines: affects:[Identifiable Entity](#)

9.13.14 Class Information Object

A representation of information, data, facts, assertions or statements about something.

As information may be copied while retaining its identity, the same information copied onto new physical media may be considered the same object. Where the individual representation of information is of concern another object should be used to represent the individual physical thing than holds the information.

As information is a resource it may depend on other resources.

[FIBO] Document

[NIEM] DocumentType

Direct Supertypes

- [Actual Entity](#), [Cyber Resource](#), [Information Resource](#), [Record](#), [Resource](#)

Associations

- / <>Restriction>> : [Information Type](#) [1..*] Subsets: has type:[Type](#)
- / <>Restriction>> : [Information Vulnerability](#) Subsets: has vulnerability:[Vulnerability](#)
- █ is stored in : [Computer System](#) [*] Subsets: is in:[Container](#)
through association: [Information In Computer](#)

System storing an information object.

- █ is in information structure : [Structured Information Object](#) [*] Subsets: is in:[Container](#)
through association: [Contained Information](#)

Structural containment of an information object within an information object.

9.13.15 Class Information Repository

A resource in which information is stored and can then be retrieved.

Direct Supertypes

- [Structured Information Object](#)

9.13.16 Class Information Resource <>Union>>

Information objects or types that can be manipulated by an information action.

Associations

- / <>Restriction>> : [Information Action](#) Subsets: affected by:[Situation](#)

9.13.17 Class Information Type

A categorization of information across any dimension - content, format, source, sensitivity, etc. e.g. a schema. The information type may be used to establish software capabilities and vulnerabilities.

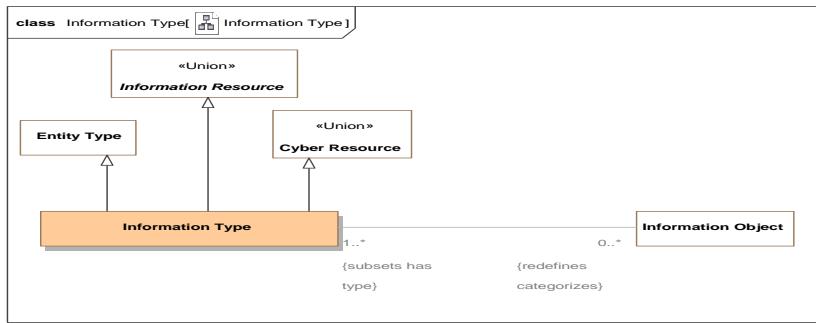


Figure 103. Information Type

Direct Supertypes

[Cyber Resource](#), [Entity Type](#), [Information Resource](#)

Associations

/ <>Restriction>> : [Information Object](#) [0..*] Redefines: categorizes:[Thing](#)

9.13.18 Class Modify Information

Action to change information (for good or bad reasons).

Direct Supertypes

[Information Action](#)

9.13.19 Class Open Information

Action to gain visibility to some information, e.g., Open a file or an envelope.

Direct Supertypes

[Information Action](#)

9.13.20 Class Read Information

An action to read, access, or understand some information.

Direct Supertypes

[Information Action](#)

9.13.21 Class Remove Information

An action to remove information from some repository or composite information structure.

Direct Supertypes

[Information Action](#), [Removal Event](#)

Associations

- / : [Structured Information Object](#) [1] *Redefines*: remove from:[Container](#)
- / <>Restriction>> : [Contained Information](#) [1] *Subsets*: negates:[Situation](#)

9.13.22 Class Structured Information Object

An information object that contains sub-elements. e.g., a "record".

Direct Supertypes

[Container](#), [Information Object](#)

Associations

- █ contains information : [Information Object](#) [*] *Redefines*: contains:[Actual Entity](#)
through association: [Contained Information](#)

An information object structurally contained in another.

- / <>Restriction>> : [Add Information](#) [0..*] *Redefines*: filled by:[Add To Container Event](#)
- / : [Remove Information](#) [0..*] *Redefines*: removed by:[Removal Event](#)

9.13.23 Class Transfer Information

The transfer of information from one information store to another.

Direct Supertypes

[Add Information](#), [Relocation](#), [Remove Information](#)

9.14 Threat-risk-conceptual-model::Generic Concept Library::Locations

Concepts related to locations and places.

9.14.1 Diagram: Location

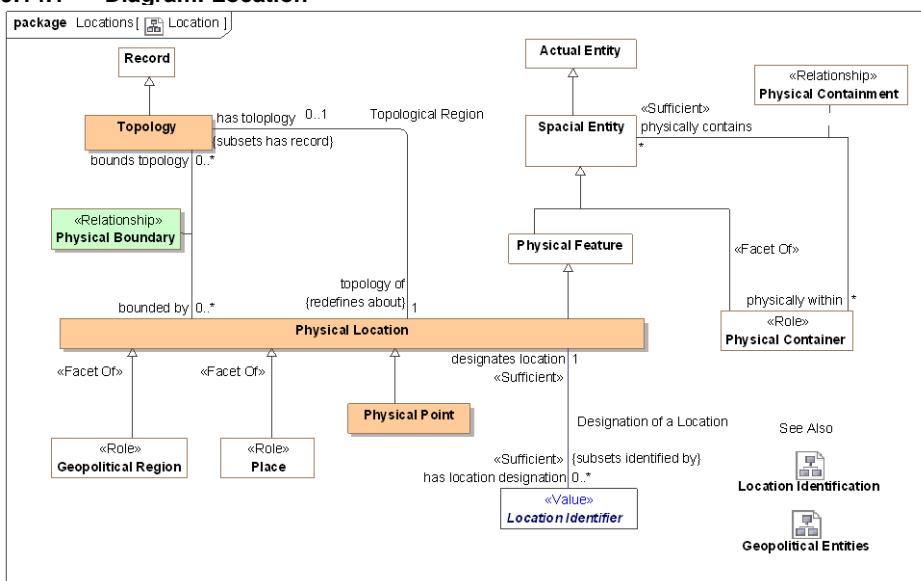


Figure 104. Location

9.14.2 Diagram: Location Identification

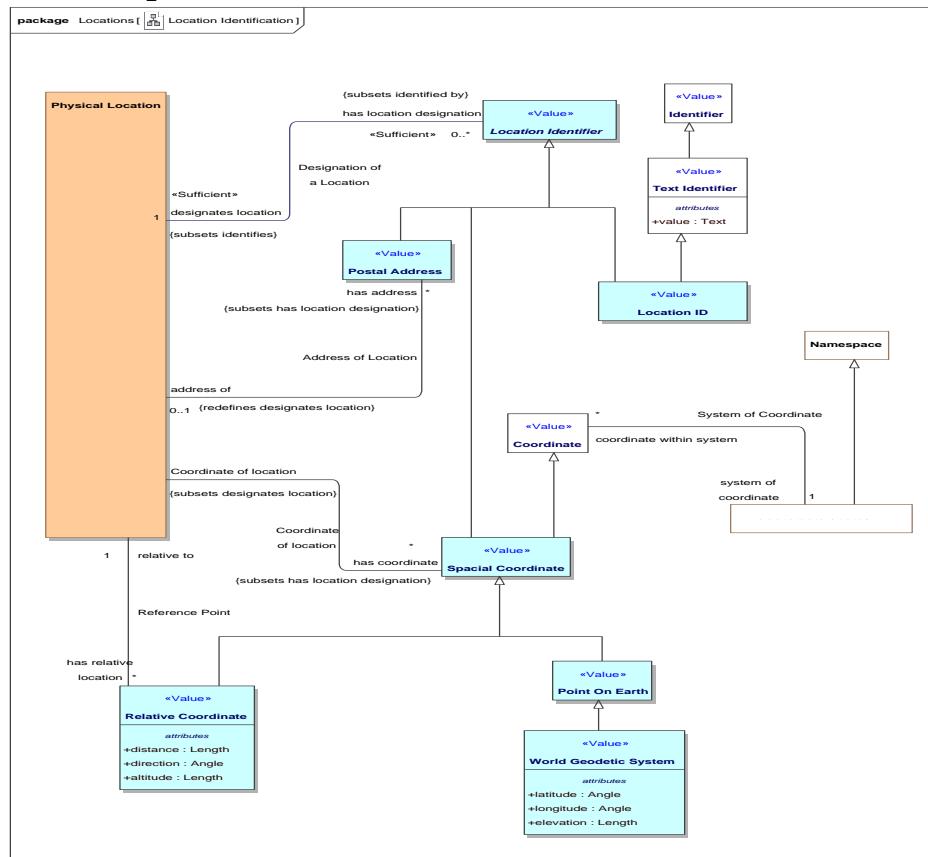


Figure 105. Location Identification

9.14.3 Association Address of Location

identification of a location by an address. Note that there are postal addresses that do not identify a location, so this relation is optional. However, most postal addresses do identify a location thus this relation is possible.

Association Ends

/ has address : **Postal Address** [*] Redefines: removed by: [Removal Event](#)

A postal address of a physical location.

/ address of : [Physical Location](#) [0..1] *Redefines*: removed by: [Removal Event](#)

Location identified by an address.

9.14.4 Association Coordinate of location

Relationship between a physical location and the coordinate that defines its position.

Association Ends

/ has coordinate : [Spacial Coordinate](#) [*] *Redefines*: removed by: [Removal Event](#)

A coordinate that identifies a location.

/ Coordinate of location : [Physical Location](#) *Redefines*: removed by: [Removal Event](#)

Coordinate of location based on coordinate system.

9.14.5 Association Designation of a Location

Relationship defining the location identified by a location identifier.

Association Ends

/ designates location : [Physical Location](#) [1] *Redefines*: removed by: [Removal Event](#)

The physical location identified or described by a location identifier..

/ has location designation : [Location Identifier](#) [0..*] *Redefines*: removed by: [Removal Event](#)

A description or identifier that designates a particular location.

9.14.6 Class Location ID <>Value>>

A code, ID or name for a physical location.

Direct Supertypes

[Location Identifier](#), [Text Identifier](#)

9.14.7 Class Location Identifier <>Value>>

Any identifier able to uniquely identify a physical location

Syn. spatial reference - description of position in the real world [OGC]

Direct Supertypes

[Unique Identifier](#)

Associations

/ <<Sufficient>> designates location : [Physical Location](#) [1] Subsets: identifies:[Identifiable Entity](#)
through association: [Designation of a Location](#)

The physical location identified or described by a location identifier..

9.14.8 Association Class Physical Boundary <<Relationship>>

Boundary describing the topology of a location.

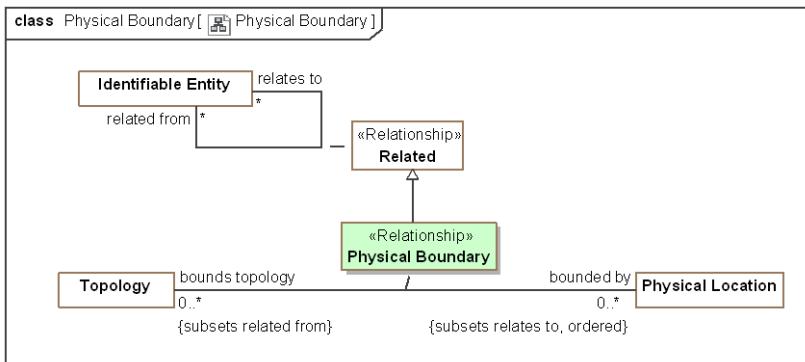


Figure 106. Physical Boundary

Direct Supertypes

[Related](#)

Association Ends

Physical Location [0..*] Subsets: identifies:[Identifiable Entity](#)

The edge points of a topology where each successive pair of features (as well as the first and last points), connected by lines, describes a boundary.

Topology [0..*] Subsets: identifies:[Identifiable Entity](#)

A location identified by geographic boundaries.

9.14.9 Class Physical Location

A point or extent in physical space.

[NIEM] A geospatial location.

[FIBO] PhysicalLocation: A location in physical space

Direct Supertypes

Physical Feature

Associations

- / <>Sufficient>> has location designation : [Location Identifier](#) [0..*] Subsets: identified by:[Identifier](#)
through association: [Designation of a Location](#)

A description or identifier that designates a particular location.

- / has address : [Postal Address](#) [*] Subsets: has location designation:[Location Identifier](#)
through association: [Address of Location](#)

A postal address of a physical location.

- / has coordinate : [Spacial Coordinate](#) [*] Subsets: has location designation:[Location Identifier](#)
through association: [Coordinate of location](#)

A coordinate that identifies a location.

- / has relative location : [Relative Coordinate](#) [*]
through association: [Reference Point](#)
- / has topology : [Topology](#) [0..1] Subsets: has record:[Record](#)
through association: [Topological Region](#)

Topology that describes a physical location in terms of physical boundaries.

- / bounds topology : [Topology](#) [0..*] Subsets: related from:[Identifiable Entity](#)
through association: [Physical Boundary](#)

A location identified by geographic boundaries.

- / located person : [Person](#) [*] Subsets: physically contains:[Spacial Entity](#)
through association: [Person at location](#)

A person who is at a location.

9.14.10 Class Physical Point

A dimensionless physical point in space or on the surface of the earth such as a corner or center point.

Direct Supertypes

[Physical Location](#)

9.14.11 Class Point On Earth <>Value>>

A point that defines a location on earth where the point is within the bounds of <designates location>.

Direct Supertypes

[Spacial Coordinate](#)

9.14.12 Association Reference Point

Reference point for a relative location

Association Ends

- / relative to : [Physical Location](#) [1] Subsets: physically contains:[Spacial Entity](#)

Where the position of something is relative to a location, the reference location.

- / has relative location : [Relative Coordinate](#) [*] Subsets: physically contains:[Spacial Entity](#)

9.14.13 Class Relative Coordinate <>Value>>

A coordinate described relative to another. e.g., 5 miles west of the empire state building.

Direct Supertypes

[Spacial Coordinate](#)

Attributes

- ◊ distance : [Length](#)

Distance as part of a relative coordinate that, when combined with angle, identifies a point <relative to> another point.

- ◊ direction : [Angle](#)

An angle as part of a coordinate.

- ◊ altitude : [Length](#)

Measure of how much something is above <relative to> something else, usually the earth.

Associations

- / relative to : [Physical Location](#) [1]
through association: [Reference Point](#)

Where the position of something is relative to a location, the reference location.

9.14.14 Class Spacial Coordinate <>Value>>

Any point that uniquely identifies a spacial location relative to a coordinate system.

One of a sequence of n numbers designating the position of a point in n-dimensional space [OGC]

Direct Supertypes

[Coordinate, Location Identifier](#)

Associations

- / Coordinate of location : [Physical Location](#) Subsets: designates location:[Physical Location](#)
through association: [Coordinate of location](#)

Coordinate of location based on coordinate system.

9.14.15 Association Topological Region

Physical location described by a topology.

Association Ends

- / topology of : [Physical Location](#) [1] Subsets: designates location:[Physical Location](#)
- / has topology : [Topology](#) [0..1] Subsets: designates location:[Physical Location](#)

Topology that describes a physical location in terms of physical boundaries.

9.14.16 Class Topology

A record of a contiguous 1, 2 or 3 dimensioned area defined by geographic features and points.
[NIEM] AreaType

Direct Supertypes

- [Record](#)

Associations

- / topology of : [Physical Location](#) [1] Redefines: about:[Identifiable Entity](#)
through association: [Topological Region](#)

Location described by a topology.

-  bounded by : [Physical Location](#) [0..*] Subsets: relates to:[Identifiable Entity](#)
through association: [Physical Boundary](#)

The edge points of a topology where each successive pair of features (as well as the first and last points), connected by lines, describes a boundary.

9.14.17 Class World Geodetic System <>Value>>

The World Geodetic System defines a reference frame for the earth, for use in geodesy and navigation. The latest revision is WGS 84 dating from 1984. [WGS-84]
[NIEM] Location2DGeospatialCoordinateType or Location3DGeospatialCoordinateType (With elevation)

Direct Supertypes

Point On Earth

Attributes

- ◊ **latitude** : [Angle](#)

Latitude based on the prime meridian.
[FIBO] hasLatitude

- ◊ **longitude** : [Angle](#)

Longitude based on the prime meridian.
[FIBO] hasLongitude

- ◊ **elevation** : [Length](#)

Height above nominal sea level.

9.15 Threat-risk-conceptual-model::Generic Concept Library::Objectives

Objectives captures how the intents of *stakeholder's* relate to the real-world *consequences of situations* that have or may happen. A *consequence* results in a *benefit* or *harm* to these *objectives* - generally related to a specific entity of value to the stakeholder.

As any situation may have multiple consequences, both benefits and harms, the net desirability of any situation to a stakeholder is calculated in the *Stakeholder Desirability Relation* by combining all of the related consequences.

9.15.1 Diagram: Objectives

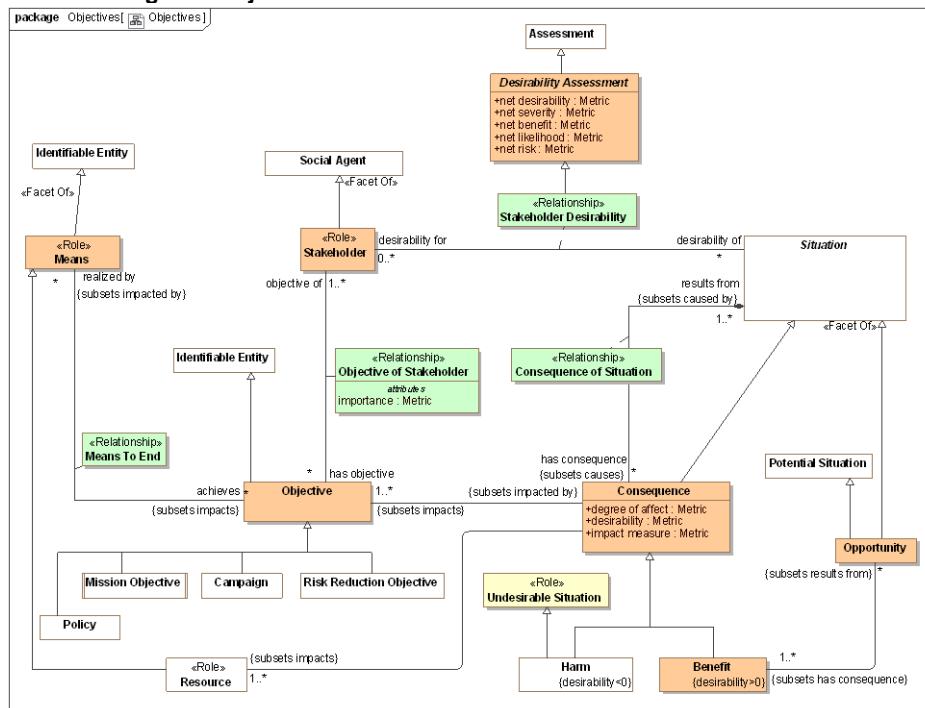


Figure 107. Objectives

9.15.2 Class Benefit

A benefit is a consequence of a situation having positive desirability.

Direct Supertypes

[Consequence](#)

Associations

 : [Opportunity](#) [*] Subsets: results from: [Situation](#)

A situation that may result in an opportunity.

9.15.3 Class Consequence

A consequence or impact of the outcome of a situation affecting objectives of a stakeholder.

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and can have positive or negative effects on objectives.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

[ISO 73-2009]

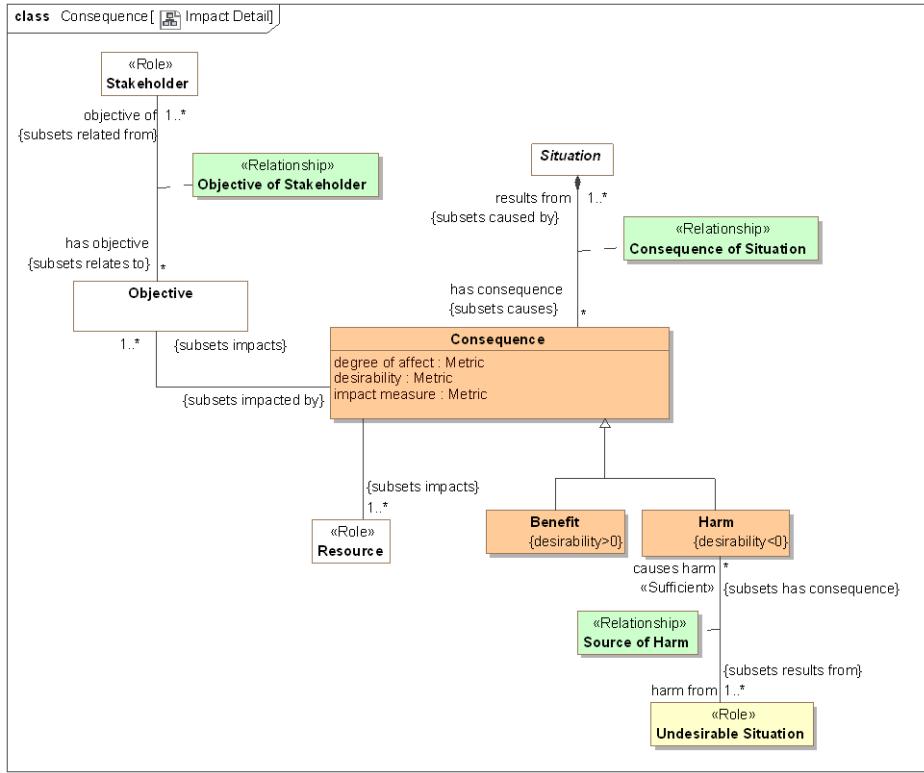


Figure 108. Impact Detail

Direct Supertypes

[Situation](#)

Attributes

◦ **degree of affect** : [Metric](#)

A metric for how much the consequence affects an objective - a measure of harm or benefit.

◦ **desirability** : [Metric](#)

A metric describing the desirability of an impact. May be positive or negative where positive is desirable and negative is undesirable.

◦ **impact measure** : [Metric](#)

A metric for impact where Impact = desirability * likelihood

Associations

 : [Objective](#) [1..*] Subsets: impacts:[Identifiable Entity](#)

 : [Resource](#) [1..*] Subsets: impacts:[Identifiable Entity](#)

Resource a consequence may affect.

 results from : [Situation](#) [1..*] Subsets: caused by:[Situation](#)

through association: [Consequence of Situation](#)

Situation causing an impact..

9.15.4 Association Class Consequence of Situation <>Relationship>>

Impact of a situation - its affect on the objectives of stakeholders.

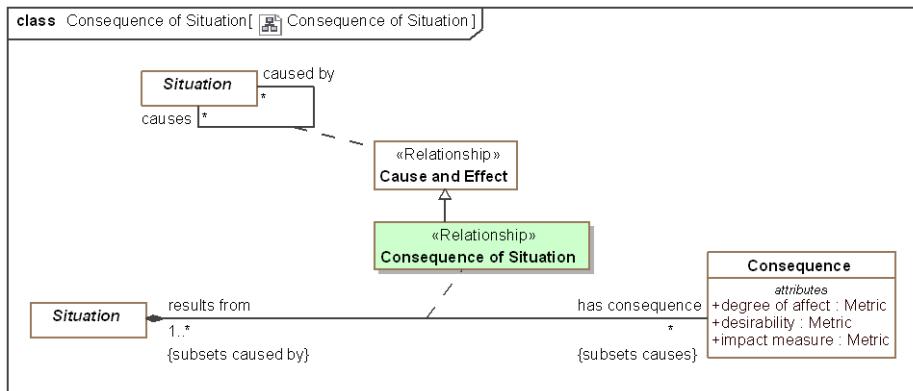


Figure 109. Consequence of Situation

Direct Supertypes

[Cause and Effect](#)

Association Ends

 has consequence : [Consequence](#) [*] Subsets: caused by:[Situation](#)

A consequence of a situation that impacts the objectives of a stakeholder.

 results from : [Situation](#) [1..*] Subsets: caused by:[Situation](#)

Situation causing an impact..

9.15.5 Class Desirability Assessment

Desirability measure of a situation. The context of the desirability can be the specific stakeholder desirability relation or a classification of a situation in a context, such as an undesirable situation.

Desirability may be computed by aggregating the impact of a situation on stakeholders but the specific calculation is not specified in the standard.

A positive desirability is an opportunity; a negative desirability is a danger.

When the stakeholder desirability of a situation to a stakeholder has net harm, that harm may be identified as a risk. S

Direct Supertypes

[Assessment](#)

Attributes

◊ [net desirability : Metric](#)

A metric representing the aggregation of the impact of all consequences of a situation for a stakeholder. (net benefit - net risk)

◊ [net severity : Metric](#)

The aggregation of the impact of all detriments (negative consequences) of a situation for a stakeholder.

◊ [net benefit : Metric](#)

A metric representing the aggregation of the impact of all benefits (positive consequences) of a situation for a stakeholder.

◊ [net likelihood : Metric](#)

The net sum of the likelihood of a situation or risk.

◊ [net risk : Metric](#)

A metric representing the aggregation of risk metrics computed as likelihood*impact.

9.15.6 Class Means <>Role>>

[BMM] A means represents any device, capability, regime, technique, restriction, agency, instrument, or method that may be called upon, activated, or enforced to achieve Ends.

Direct Supertypes

[Identifiable Entity](#)

Associations

█ achieves : [Objective](#) [*] Subsets: impacts:[Identifiable Entity](#)

through association: [Means To End](#)

Objectives supported by a means.

9.15.7 Association Class Means To End <>Relationship>>

The relation between a means and an objective such that the means supports the objective.
 [BMM] means is impacted by influencer

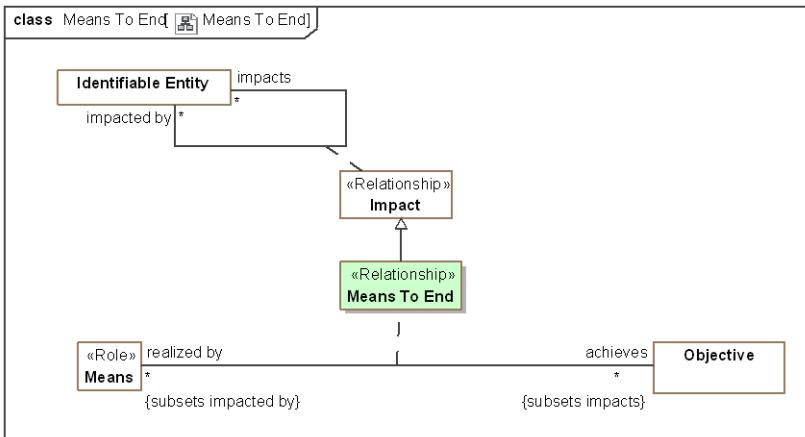


Figure 110. Means To End

Direct Supertypes

Impact

Association Ends

achieves : [Objective](#) [*] Subsets: impacts:[Identifiable Entity](#)

Objectives supported by a means.

realized by : [Means](#) [*] Subsets: impacts:[Identifiable Entity](#)

Means that serves to meet an objective.

9.15.8 Class Objective

An aim or goal that a stakeholder intends to attain or accomplish; purpose; goal; target.

[BMM] End: something that is to be accomplished.

[BMM] Objective: An Objective is a statement of an attainable, time-targeted, and measurable target that the enterprise seeks to meet in order to achieve its Goals.

[FIBO] Objective

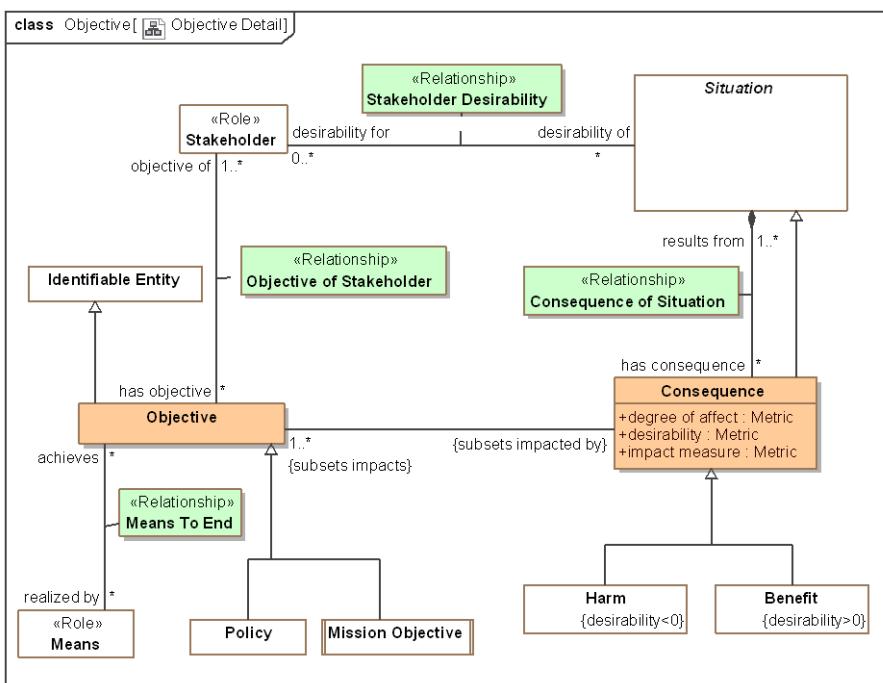


Figure 111. Objective Detail

Direct Supertypes

Identifiable Entity

Associations

- <<Restriction>> : [Disrupt Stakeholder's Objective](#) [*] Subsets: affected by:[Situation](#)
 - : [Consequence](#) Subsets: impacted by:[Identifiable Entity](#)
 - realized by : [Means](#) [*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Means To End](#)

Means that serves to meet an objective.

-  objective of : [Stakeholder](#) [1..*] Subsets: related from:[Identifiable Entity](#) through association: [Objective of Stakeholder](#)

A stakeholder having an objective they intend to attain or retain.

9.15.9 Association Class Objective of Stakeholder <>Relationship>>

Relationship between a stakeholder and their objectives.

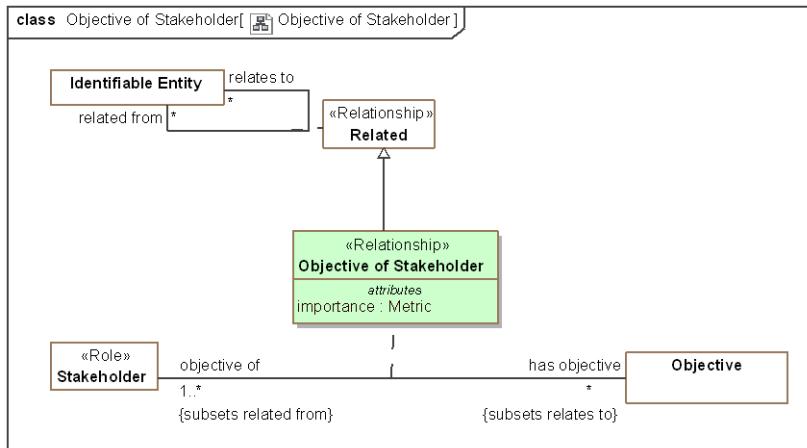


Figure 112. Objective of Stakeholder

Direct Supertypes

[Related](#)

Association Ends

has objective : [Objective](#) [*] Subsets: related from:[Identifiable Entity](#)

An objective that a stakeholder intends to retain or achieve.

objective of : [Stakeholder](#) [1..*] Subsets: related from:[Identifiable Entity](#)

A stakeholder having an objective they intend to attain or retain.

Attributes

importance : [Metric](#)

A metric of importance of an objective to a stakeholder.

9.15.10 Class Opportunity

An opportunity is any potential future situation having beneficial consequences.

[BMM] Opportunity: This category of Assessment indicates that some Influencer can have a favorable impact on the organization's employment of Means or achievement of Ends. For example, the bankruptcy of Pizza Company's major competitor in Region-Y is assessed to be an Opportunity in its Goal "To increase market share."

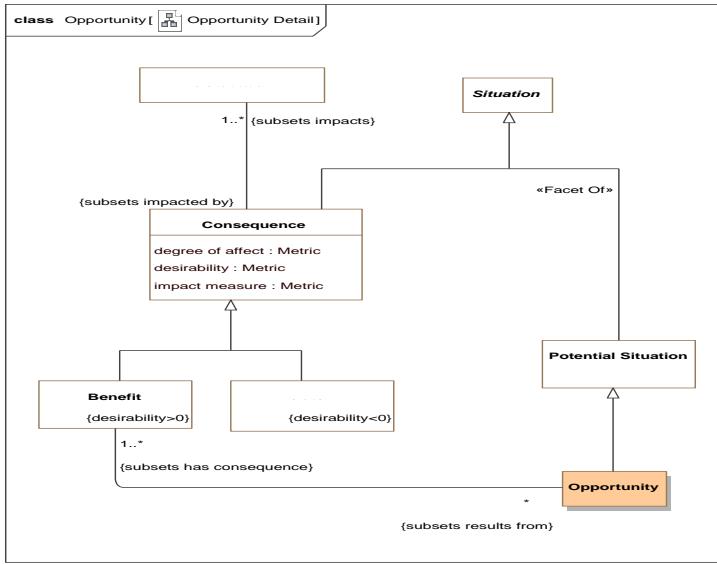


Figure 113. Opportunity Detail

Direct Supertypes

[Potential Situation](#), [Situation](#)

Associations

[Benefit](#) [1..*] *Subsets:* has consequence;[Consequence](#)

A consequence of a situation that impacts the objectives of a stakeholder in a positive way.

9.15.11 Class Stakeholder <<Role>>

A stakeholder is a responsible performer having objectives and promoting the means for achieving those objectives.

Direct Supertypes

[Social Agent](#)

Associations

desirability of : [Situation](#) [*] *Subsets:* relates to;[Identifiable Entity](#)
through association: [Stakeholder Desirability](#)

The situation evaluated in terms of its desirability for a stakeholder.

has objective : [Objective](#) [*] *Subsets:* relates to;[Identifiable Entity](#)

through association: [Objective of Stakeholder](#)

An objective that a stakeholder intends to retain or achieve.

9.15.12 Association Class Stakeholder Desirability <>Relationship>>

A relationship representing the net desirability of a situation for a stakeholder.

Note: Stakeholder desirability is expected to be computed based on aggregating the impact of a situation for a stakeholder. However, the algorithm for this aggregation is not specified in the standard.

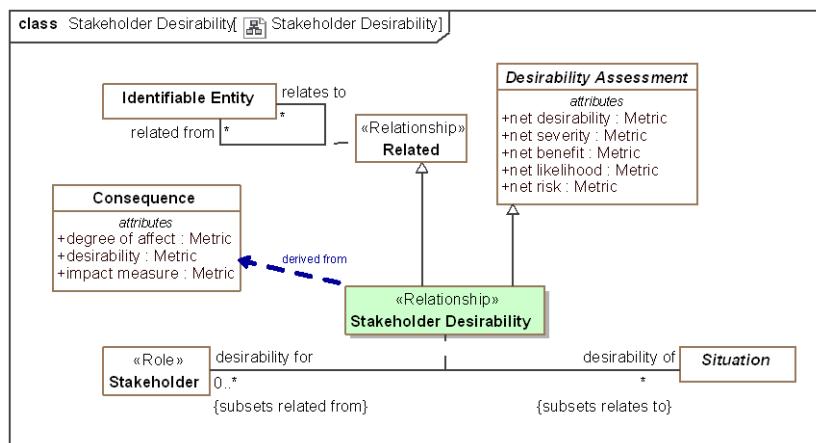


Figure 114. Stakeholder Desirability

Direct Supertypes

[Desirability Assessment](#), [Related](#)

Association Ends

desirability of : [Situation](#) [*] Subsets: relates to: [Identifiable Entity](#)

The situation evaluated in terms of its desirability for a stakeholder.

desirability for : [Stakeholder](#) [0..*] Subsets: relates to: [Identifiable Entity](#)

A stakeholder for which desirability of a situation is evaluated.

9.16 Threat-risk-conceptual-model::Generic Concept Library::Observations

Observations are acts where an observer notes some entity (including situations and individuals) that are observed in a situation.

9.16.1 Diagram: Measurement

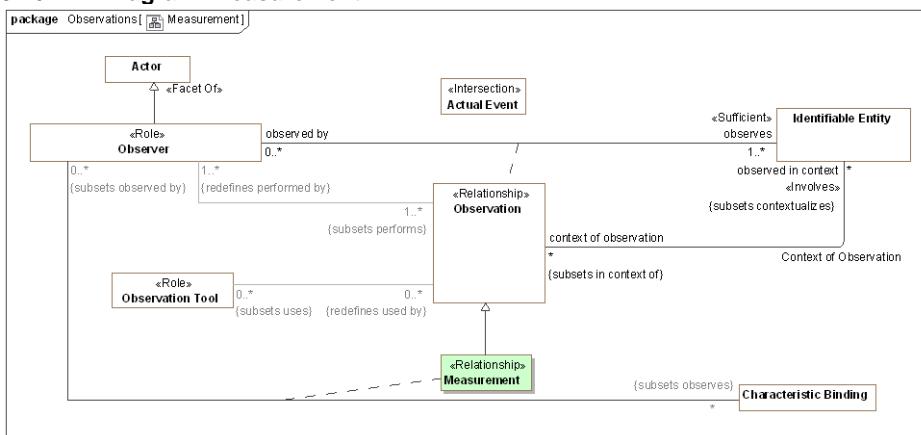


Figure 115. Measurement

9.16.2 Diagram: Observability

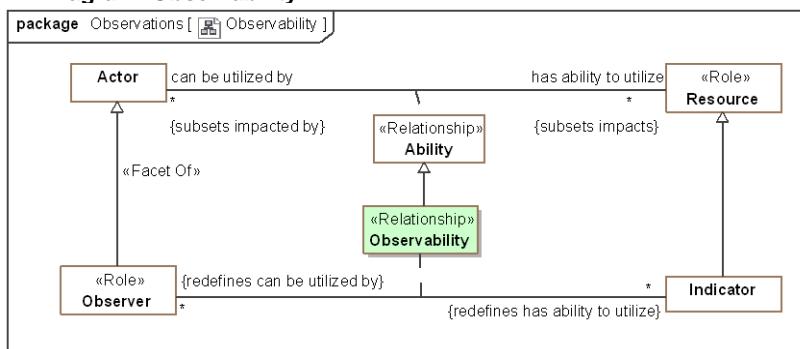


Figure 116. Observability

9.16.3 Diagram: Observations

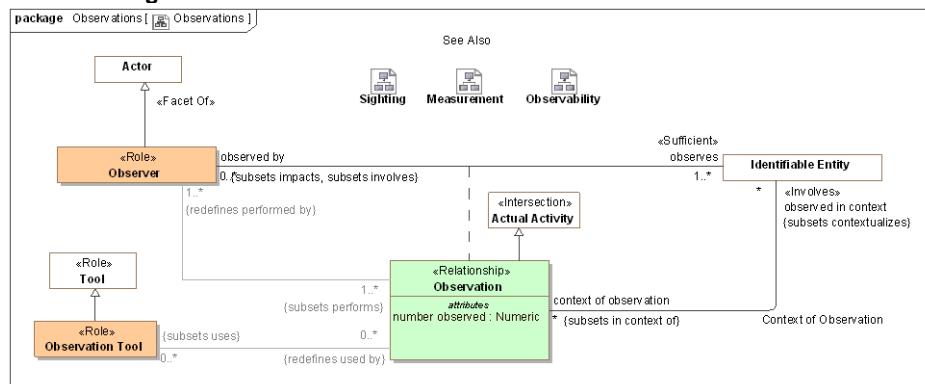


Figure 117. Observations

9.16.4 Association Context of Observation

Context of an observations - e.g. the physical place, situation or timeframe in which the observation was made.

Direct Supertypes

Extent of Context

Association Ends

/ observed in context : [Identifiable Entity](#) [*] Subsets: relates to:[Identifiable Entity](#)

The context of an observation, what environment, location, timeframe or system is being observed. e.g. A man with a gun observed in an airport. The man is <observed in context> of the airport.

/ context of observation : [Observation](#) [*] Subsets: relates to:[Identifiable Entity](#)

Observations made in the context of the subject entity. E.G. Sightings within an airport.

9.16.5 Association Class Measurement <>Relationship>>

A measurement is an observation made by <observed by> that <observes> the value of a characteristic for a particular entity, which is the Characteristic Binding the observer <observes>. The characteristic binding binds a particular value, e.g. 2 meters, with a particular characteristic, e.g. height, of a particular individual, e.g. John Smith.

As a characteristic binding is a temporal entity it has a time and context which may be different from the time and context of the measurement. e.g. The nurse "Sue" took the patients (Joe) weight measurement (Characteristic Binding - Joe <has weight> 94 KG) on 2/5/2010 at 9:31AM which was recorded as the patients current weight for 90 days.

Direct Supertypes

Observation

Association Ends

- ▀ : [Characteristic Binding](#) [*] Subsets: relates to: [Identifiable Entity](#)
- ▀ : [Observer](#) [0..*] Subsets: relates to: [Identifiable Entity](#)

9.16.6 Association Class Observability <<Relationship>>

Observability is a relationship representing the capability of an <can be utilized by> actor to observe an <has ability to utilize> indicator.

Direct Supertypes

Ability

Association Ends

- ▀ : [Indicator](#) [*] Subsets: relates to: [Identifiable Entity](#)
- ▀ : [Observer](#) [*] Subsets: relates to: [Identifiable Entity](#)

9.16.7 Association Class Observation <<Relationship>>

An observation is an actual (not possible) activity of the <observed by> observer where <observes> has been noticed or perceived as being significant. The observation is <observed in context> such as a place or condition. The observation <uses> any number of observation tools.

Example: Sam, a driver and Observer, notices <observes> a Deer <observed in context> of the road on which he is driving.

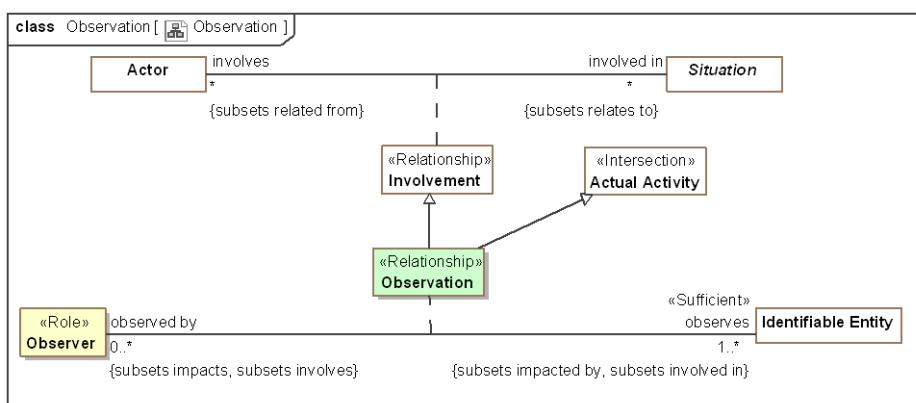


Figure 118. Observation

Direct Supertypes

Actual Activity, Impact, Involvement

Association Ends

 observes : [Identifiable Entity](#) [1..*] Subsets: relates to: [Identifiable Entity](#)

Entity observed by an observer making an observation.

 observed by : [Observer](#) [0..*] Subsets: relates to: [Identifiable Entity](#)

Observations of an entity by an observer.

Attributes

 number observed : [Numeric](#)

The number of individual observations aggregated into a single observation. The <observes> entity will likely be a type.
E.G. Sue saw 5 birds.

Associations

 <>Restriction>> : [Observer](#) [1..*] Redefines: performed by: [Actor](#)

An observer of an observation.

 <>Restriction>> : [Observation Tool](#) [0..*] Subsets: uses: [Resource](#)

Something used to facilitate an observation.

 observed in context : [Identifiable Entity](#) [*] Subsets: contextualizes: [Thing](#)

through association: [Context of Observation](#)

The context of an observation, what environment, location, timeframe or system is being observed. e.g. A man with a gun observed in an airport. The man is <observed in context> of the airport.

9.16.8 Class Observation Tool <>Role>>

A tools that assists in observations. e.g. a wireless microphone is used to observe a conversation.

Direct Supertypes

[Tool](#)

Associations

 <>Restriction>> : [Observation](#) [0..*] Redefines: used by: [Event](#)

Uses of an observation tool.

9.16.9 Class Observer <>Role>>

Role of an actor that can or has observed something

Direct Supertypes

[Actor](#)

Associations

- █ <>Restriction>> : [Identifiable Entity](#) [*] Subsets: observes:[Identifiable Entity](#)
through association: [Sighting](#)
- █ <>Restriction>> : [Characteristic Binding](#) [*] Subsets: observes:[Identifiable Entity](#)
through association: [Measurement](#)
- ↙ <>Restriction>> : [Observation](#) [1..*] Subsets: performs:[Activity](#)

Observations made by an observer.

- █ : [Indicator](#) [*] Redefines: has ability to utilize:[Resource](#)
through association: [Observability](#)
- █ observes : [Identifiable Entity](#) [1..*] Subsets: impacted by:[Identifiable Entity](#) involved in:[Situation](#)
through association: [Observation](#)

Entity observed by an observer making an observation.

9.17 Threat-risk-conceptual-model::Generic Concept Library::Organizations

An Organization is group of persons and/or other actors and resources organized for some end or work.
Subtypes of organizations include governments and corporations.

9.17.1 Diagram: Organization

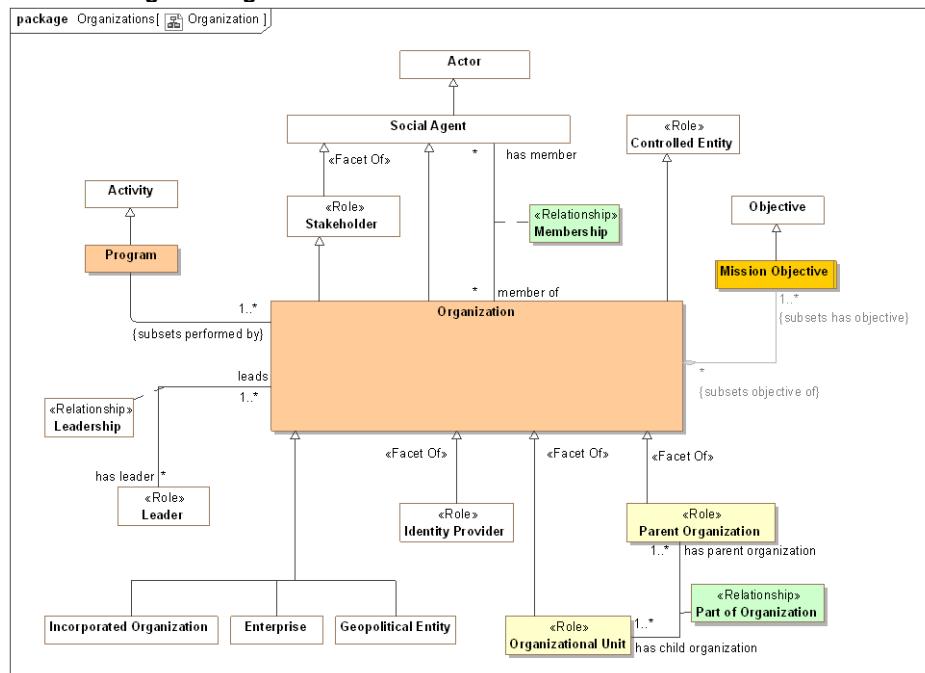


Figure 119. Organization

9.17.2 Association Class Membership <>Relationship>>

Relationship representing the participation of an actor in an organization. Subtypes of membership may provide more explicit membership kinds.

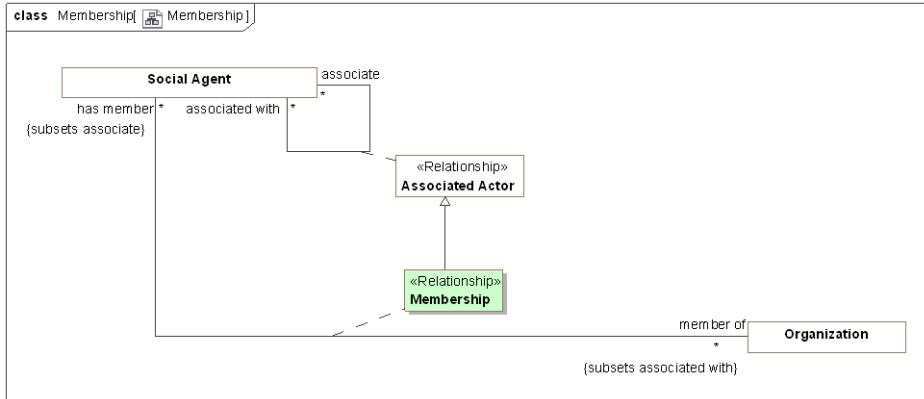


Figure 120. Membership

Direct Supertypes

[Associated Actor](#)

Association Ends

has member : [Social Agent](#) [*] Subsets: impacted by:[Identifiable Entity](#) involved in:[Situation](#)

An assertion of membership in an organization.

[FIBO] hasMember

member of : [Organization](#) [*] Subsets: impacted by:[Identifiable Entity](#) involved in:[Situation](#)

Organization a performer belongs to.

[FIBO] memberOf

9.17.3 Class Mission Objective

A core objective of an enterprise.

[BMM] A Mission indicates the ongoing operational activity of the enterprise. The Mission describes what the business is or will be doing on a day-to-day basis.

Direct Supertypes

[Objective](#)

Associations

<<Restriction>> : [Organization](#) [*] Subsets: objective of:[Stakeholder](#)

9.17.4 Class Organization

An Organization is a group of persons and/or other actors and resources organized for some end or work
[FIBO] Organization: a social unit of people, systematically structured and managed to meet a need or pursue collective goals on a continuing basis.
[NIEM] OrganizationType
[DOLCE] Society

Direct Supertypes

[Controlled Entity](#), [Social Agent](#), [Stakeholder](#)

Associations

 has member : [Social Agent](#) [*] Subsets: associate:[Social Agent](#)
through association: [Membership](#)

An assertion of membership in an organization.

[FIBO] hasMember

 : [Program](#)
 <>Restriction>> : [Mission Objective](#) [1..*] Subsets: has objective:[Objective](#)
 has leader : [Leader](#) [*] Subsets: is controlled by:[Controlling Actor](#) has member:[Social Agent](#)
through association: [Leadership](#)

A person leading or directing an organization.

9.17.5 Class Organizational Unit <>Role>>

Organizational unit is a role that encompasses subdivisions, departments, subsidiaries and other organizational parts of an organization.
[BMM] organization unit: An administrative or functional unit within an organization structure.

Direct Supertypes

[Controlled Entity](#), [Organization](#)

Associations

 has parent organization : [Parent Organization](#) [1..*] Subsets: is controlled by:[Controlling Actor](#) is part of:[Identifiable Entity](#)
through association: [Part of Organization](#)

The parent (controlling organization) of another organization.

9.17.6 Class Parent Organization <>Role>>

Organization with component parts such as divisions and departments.

Direct Supertypes

Controlling Actor, Organization

Associations

has child organization : [Organizational Unit](#) [1..*] Subsets: has part:[Identifiable Entity](#) is controlled by:[Controlling Actor](#)
through association: [Part of Organization](#)

An organization constituted as a component of another organization.

9.17.7 Association Class Part of Organization <<Relationship>>

Relationship between an organization and its organizational units - the sub-organizations such as departments and subsidiaries.

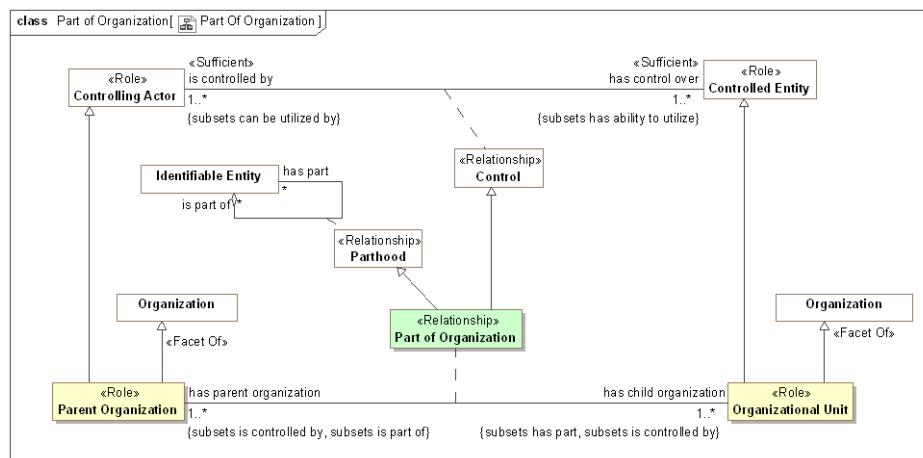


Figure 121. Part Of Organization

Direct Supertypes

[Control](#), [Parthood](#)

Association Ends

has parent organization : [Parent Organization](#) [1..*] Subsets: has part:[Identifiable Entity](#) is controlled by:[Controlling Actor](#)

The parent (controlling organization) of another organization.

has child organization : [Organizational Unit](#) [1..*] Subsets: has part:[Identifiable Entity](#) is controlled by:[Controlling Actor](#)

An organization constituted as a component of another organization.

9.17.8 Class Program

A set of projects, activities, or services of an organization that are intended to meet a need.
[NIEM] ProgramType

Direct Supertypes

[Activity](#)

Associations

 : [Organization](#) [1..*] Subsets: performed by:[Actor](#)

9.18 Threat-risk-conceptual-model::Generic Concept Library::Organizations::Corporations

9.18.1 Diagram: Corporations

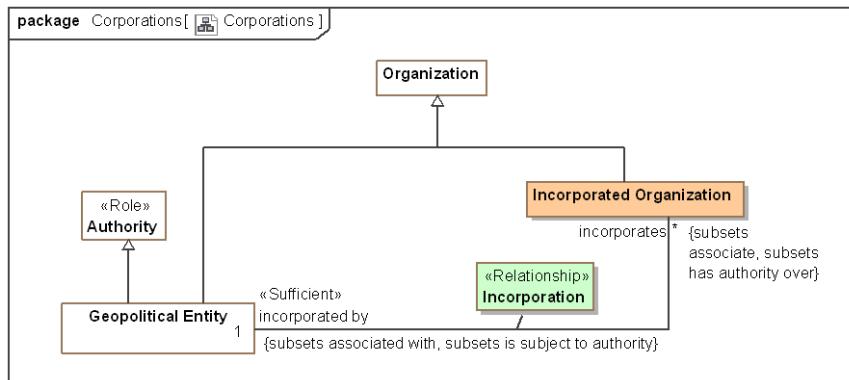


Figure 122. Corporations

9.18.2 Class Incorporated Organization

An organization recognized by and incorporated by a recognized government.
[FIBO] FormalOrganization: an organization that is recognized in some legal jurisdiction, with associated rights and responsibilities

Direct Supertypes

[Organization](#)

Associations

incorporated by : [Geopolitical Entity](#) [1] Subsets: associated with:[Social Agent](#), is subject to authority:[Authority](#)
through association: [Incorporation](#)

Geopolitical entity incorporating an organization.

9.18.3 Association Class Incorporation <<Relationship>>

Act by which individuals are voluntarily united into a new entity through the creation of an artificial, intangible, and legal person called a corporation.

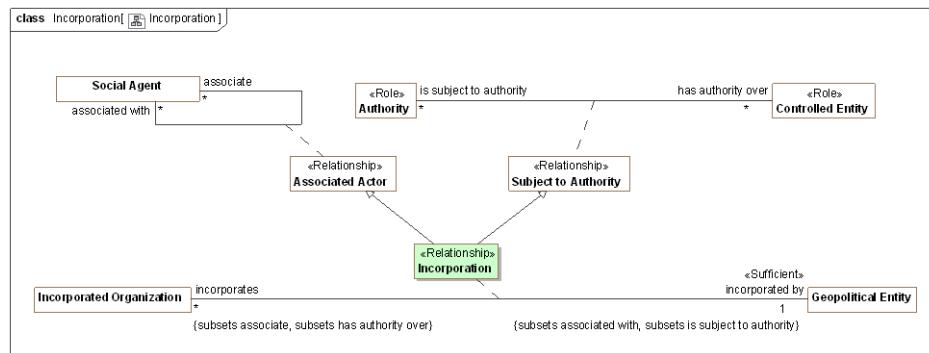


Figure 123. Incorporation

Direct Supertypes

Associated Actor, Subject to Authority

Association Ends

 incorporated by : [Geopolitical Entity](#) [1] Subsets: associated with: [Social Agent](#) is subject to authority: [Authority](#)

Geopolitical entity incorporating an organization.

 incorporates : [Incorporated Organization](#) [*] Subsets: associated with: [Social Agent](#) is subject to authority:[Authority](#)

An organization incorporated by a government.

9.19 Threat-risk-conceptual-model::Generic Concept Library::Organizations::Geopolitical Organizations

9.19.1 Diagram: Geopolitical Entities

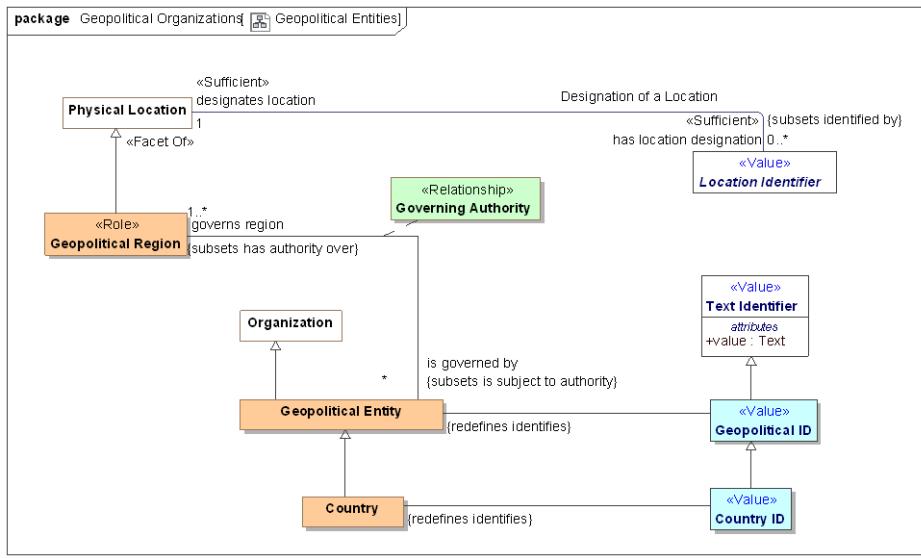


Figure 124. Geopolitical Entities

9.19.2 Class Country

A nation with its own government, occupying a particular territory (not necessarily contiguous).

[FIBO] Country: A self-governing geopolitical unit that is recognized as a country by the United Nations (more specific concept as being recognized by the U.N.)

Direct Supertypes

Geopolitical Entity

Associations

/ : Country ID

9.19.3 Class Country ID <>Value>>

A code, ID, or name for a country.

[ISO 1087] country identifier: information in a terminological entry (3.8.2) which indicates the name of a geographical region where the designation (3.4.1) is used

Direct Supertypes

[Geopolitical ID](#)

Associations

:[Country](#) Redefines: identifies:[Identifiable Entity](#)

9.19.4 Class Geopolitical Entity

An organization which is the governing body of a nation, state, tribe or community.

[FIBO] GeopoliticalEntity (In FIBO this is a subclass of Physical Location. In Threat/risk Geopolitical Region is a role of a physical location. FIBO combines Geopolitical Entity with Geopolitical Region).

Direct Supertypes

[Authority](#), [Organization](#)

Associations

:[Geopolitical ID](#)

governs region :[Geopolitical Region](#) [1..*] Subsets: has authority over:[Controlled Entity](#)
through association: [Governing Authority](#)

Region governed by a geopolitical entity.

incorporates :[Incorporated Organization](#) [*] Subsets: associate:[Social Agent](#) has authority over:[Controlled Entity](#)
through association: [Incorporation](#)

An organization incorporated by a government.

9.19.5 Class Geopolitical ID <>Value>>

A code, ID or administered name for a geopolitical entity with governmental authority e.g., city, state, county, tribe.

Direct Supertypes

[Text Identifier](#)

Associations

:[Geopolitical Entity](#) Redefines: identifies:[Identifiable Entity](#)

9.19.6 Class Geopolitical Region <<Role>>

A physical location governed by a geopolitical entity.

[FIBO] GeopoliticalEntity (In FIBO this is a subclass of Physical Location. In Threat/risk Geopolitical Region is a role of a physical location. FIBO combines Geopolitical Entity with Geopolitical Region.
[NIEM] LocaleType

Direct Supertypes

[Physical Location](#)

Associations

 is governed by : [Geopolitical Entity](#) [*] Subsets: is subject to authority:[Authority](#)
through association: [Governing Authority](#)

A governing authority for a region.

9.19.7 Association Class Governing Authority <<Relationship>>

Relationship representing authority over a region.

Direct Supertypes

[Associated Actor](#), [Subject to Authority](#)

Association Ends

 governs region : [Geopolitical Region](#) [1..*] Subsets: is subject to authority:[Authority](#)

Region governed by a geopolitical entity.

 is governed by : [Geopolitical Entity](#) [*] Subsets: is subject to authority:[Authority](#)

A governing authority for a region.

9.20 Threat-risk-conceptual-model::Generic Concept Library::Permissions

Concepts relating to the permission an actor has to perform some process.

9.20.1 Diagram: Permission

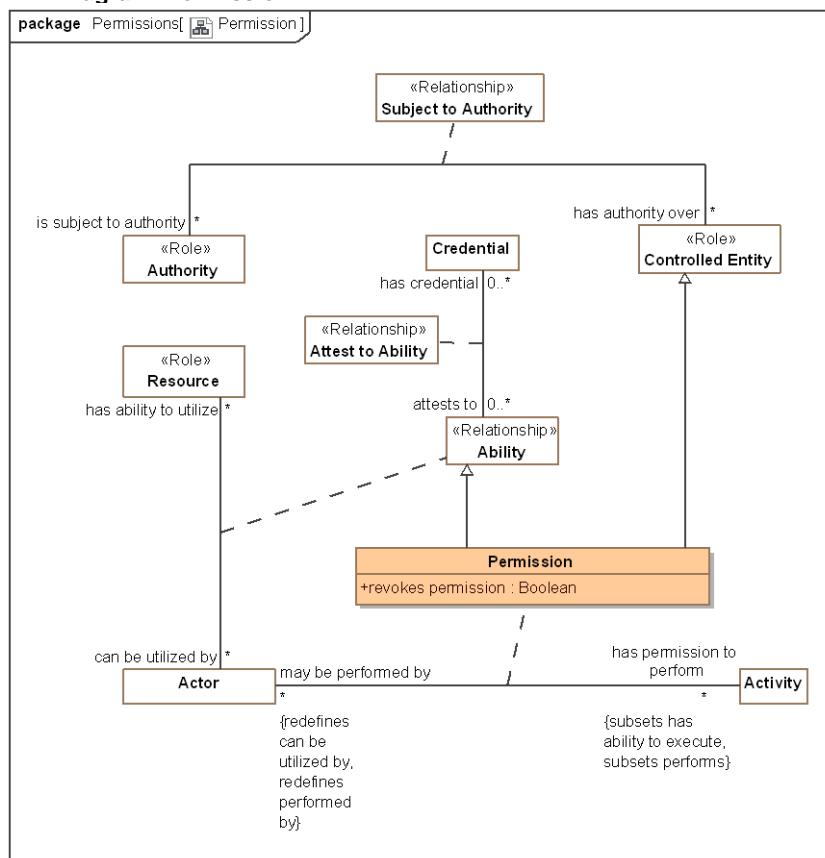


Figure 125. Permission

9.20.2 Association Class Permission

Permission is a relationship representing authorization granted by an authority to an actor to perform a kind of activity. The activity may be either an "Actual Activity" or a kind of activity - a Modus Operandi.

Direct Supertypes

[Ability](#), [Controlled Entity](#)

Association Ends

 has permission to perform : [Activity](#) [*] Subsets: is subject to authority:[Authority](#)

Activity the actor has permission to perform.

 may be performed by : [Actor](#) [*] Subsets: is subject to authority:[Authority](#)

Actors that have permission to perform the subject activity.

Attributes

 revokes permission : [Boolean](#)

Inverts or removes the permission asserted by the permission relationship.

9.21 Threat-risk-conceptual-model::Generic Concept Library::Persons

This person module defines foundation concepts of people such as their location and name. More specific person attributes may augment this specification.

9.21.1 Diagram: Person

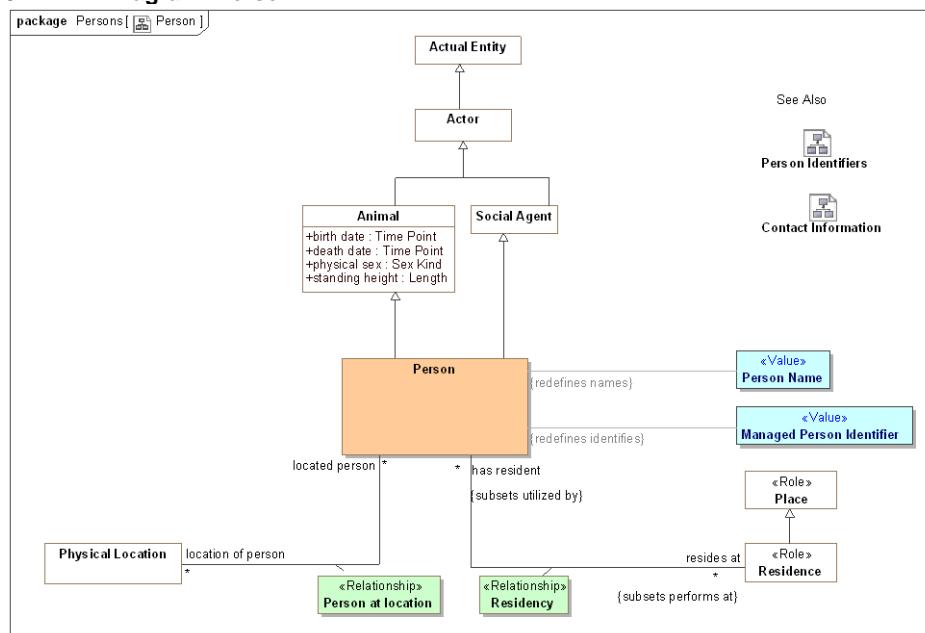


Figure 126. Person

9.21.2 Diagram: Person Identifiers

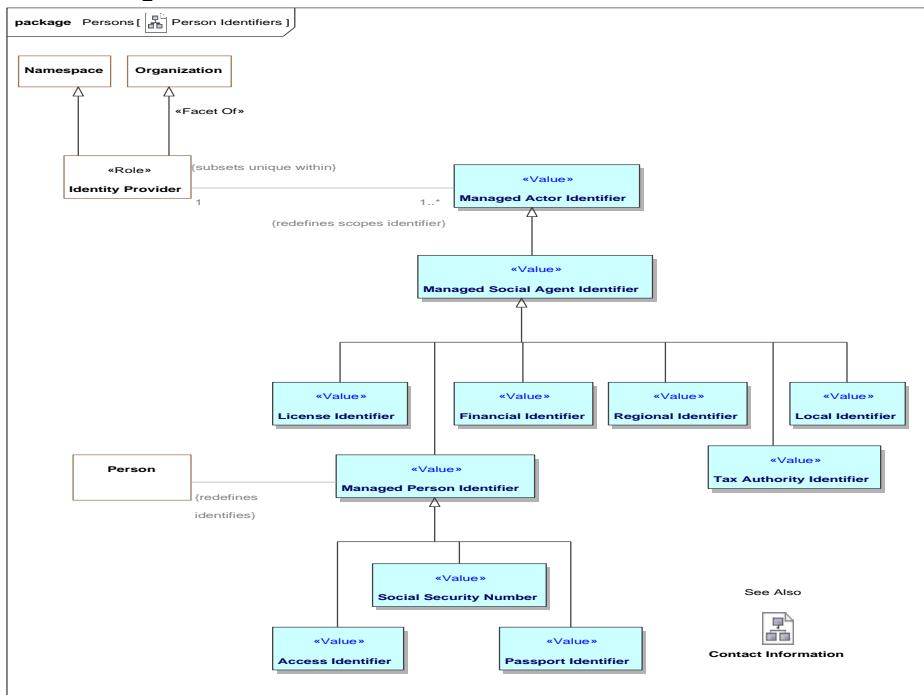


Figure 127. Person Identifiers

9.21.3 Diagram: Person Name Representations

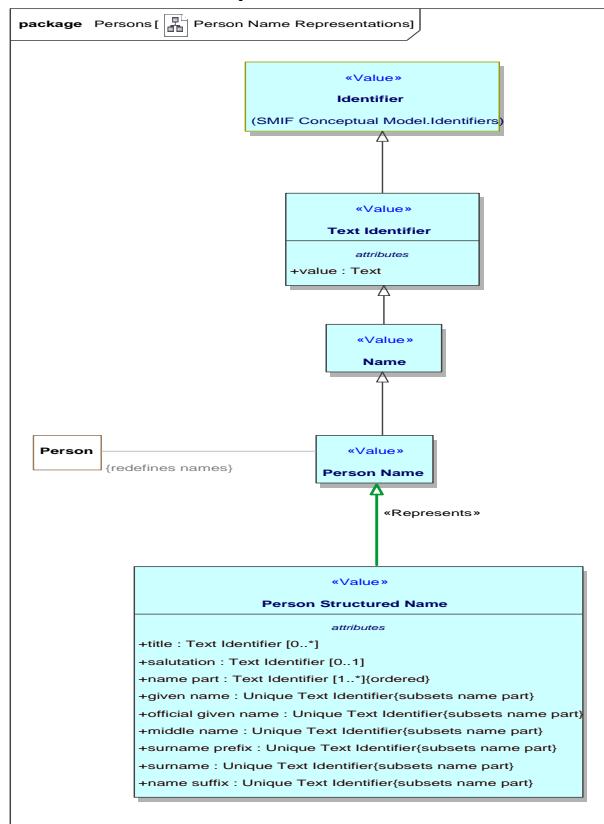


Figure 128. Person Name Representations

9.21.4 Class Access Identifier <>Value>>

An term, data value or other sign that identifies a person for access to a resource.

Direct Supertypes

[Managed Person Identifier](#)

9.21.5 Class Financial Identifier <>Value>>

An identifier for purposes of making financial transactions, such as a credit card number or bank account.

Direct Supertypes

[Managed Social Agent Identifier](#)

9.21.6 Class Managed Person Identifier <>Value>>

An identifier for a person managed by some identity provider who asserts the validity of the identifier, frequently but not always a government organization.

Direct Supertypes

[Managed Social Agent Identifier](#)

Associations

 : [Person](#) Redefines: identifies:[Identifiable Entity](#)

9.21.7 Class Passport Identifier <>Value>>

[NIEM] PersonPassportIdentification (property): An identification of a passport issued to a person.

Direct Supertypes

[Managed Person Identifier](#)

9.21.8 Class Person

An individual human being.

[FIBO] Person

[NIEM] PersonType

[DOLCE] (Subtype of) Agentive Physical Object

Direct Supertypes

[Animal](#), [Social Agent](#)

Associations

 : [Person Name](#)

 location of person : [Physical Location](#) [*] Subsets: physically within:[Physical Container](#)

through association: [Person at location](#)

Location of the subject person.

[FIBO] isSituatedAt (mode general concept)

 : [Managed Person Identifier](#)

 resides at : [Residence](#) [*] Subsets: performs at:[Place](#)

through association: [Residency](#)

A residence of a person, where they live.
 [FIBO] isDomiciledIn: identifies the permanent home or principal establishment of an individual or organization

9.21.9 Association Class Person at location <>Relationship>>

A relationship representing the location of a person at a particular time.
 [NIEM] PersonLocationAssociationType

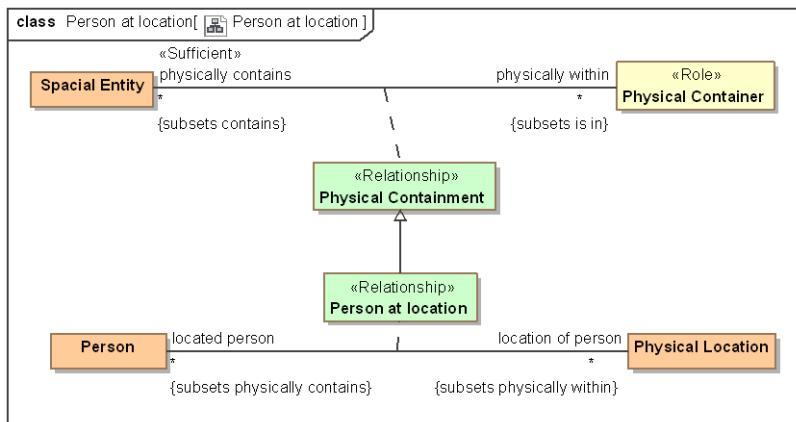


Figure 129. Person at location

Direct Supertypes

[Physical Containment](#)

Association Ends

location of person : [Physical Location](#) [*] Subsets: performs at:[Place](#)

Location of the subject person.

[FIBO] isSituatedAt (mode general concept)

located person : [Person](#) [*] Subsets: performs at:[Place](#)

A person who is at a location.

9.21.10 Class Person Name <>Value>>

Text identifying a person by a recognized name.
 [FIBO] hasFullLegalName (More specific concept)
 [NIEM] PersonNameType

Direct Supertypes

[Name](#)

Associations

 : [Person](#) Redefines: names: [Identifiable Entity](#)

9.21.11 Class Person Structured Name <>Value>>

A full name of a person in a structured form.

Note: Conversion between structured and textual names is provided by the implementation and is not defined in this specification.

Direct Supertypes

[Person Name](#)

Attributes

◊ title : [Text Identifier](#) [0..*]

[NIEM] PersonNamePrefixText: A title or honorific used by a person.

◊ salutation : [Text Identifier](#) [0..1]

[NIEM] PersonNameSalutationText: A formal sign or expression of greeting that is appropriate for a person.

◊ name part : [Text Identifier](#) [1..*]

Parts of a person's name, e.g., surname, given name.

[FIBO] hasFamilyName

◊ given name : [Unique Text Identifier](#)

[NIEM] PersonGivenName: A first name of a person.

[FIBO] hasGivenName

◊ official given name : [Unique Text Identifier](#)

[NIEM] PersonOfficialGivenName: A name, out of possibly multiple given names, that a person selects to use as his or her official given name.

◊ middle name : [Unique Text Identifier](#)

[NIEM] PersonMiddleName: A middle name of a person.

◊ surname prefix : [Unique Text Identifier](#)

[NIEM] PersonSurNamePrefix: A prefix that precedes this person's family name such as Van, Von.

◊ surname : [Unique Text Identifier](#)

[NIEM] PersonSurName: A last name or family name of a person.

[FIBO] hasSurname

◊ name suffix : [Unique Text Identifier](#)

[NIEM] PersonNameSuffixText: A term appended after the family name that qualifies the name.

9.21.12 Association Class Residency <<Relationship>>

A residence of a person - where they live.

[NIEM] PersonResidenceAssociationType

[FIBO] Residence: Note that residence is not the same as domicile, as a person or organization can have many transient residences but only one legal domicile. The domicile of a formal organization is the address (location) where the establishment is maintained or where the governing power of the organization is exercised.

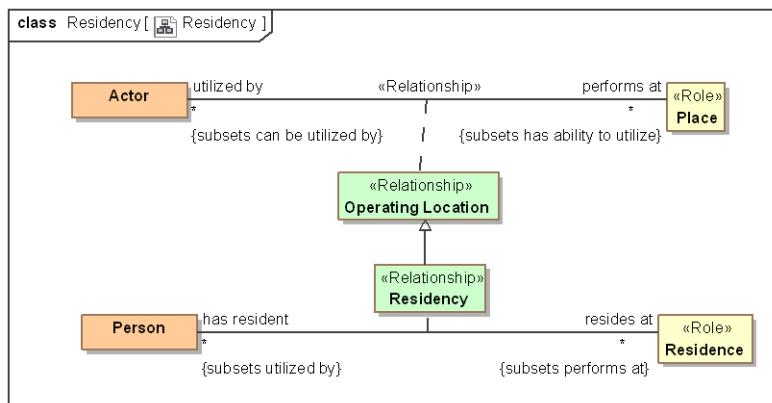


Figure 130. Residency

Direct Supertypes

[Operating Location](#)

Association Ends

resides at : [Residence](#) [*] Redefines: names: [Identifiable Entity](#)

A residence of a person, where they live.

[FIBO] isDomiciledIn: identifies the permanent home or principal establishment of an individual or organization

has resident : [Person](#) [*] Redefines: names: [Identifiable Entity](#)

A person living in a residence.

9.21.13 Class Social Security Number <<Value>>

[NIEM] PersonSSNIdentification (property): A unique identification reference to a living person; assigned by the United States Social Security Administration.

Direct Supertypes

[Managed Person Identifier](#)

9.22 Threat-risk-conceptual-model::Generic Concept Library::Physical Entities

This package defines a hierarchy of physical entities and items. Items are inanimate material object as distinct from a living sentient being.

9.22.1 Diagram: Physical Entities

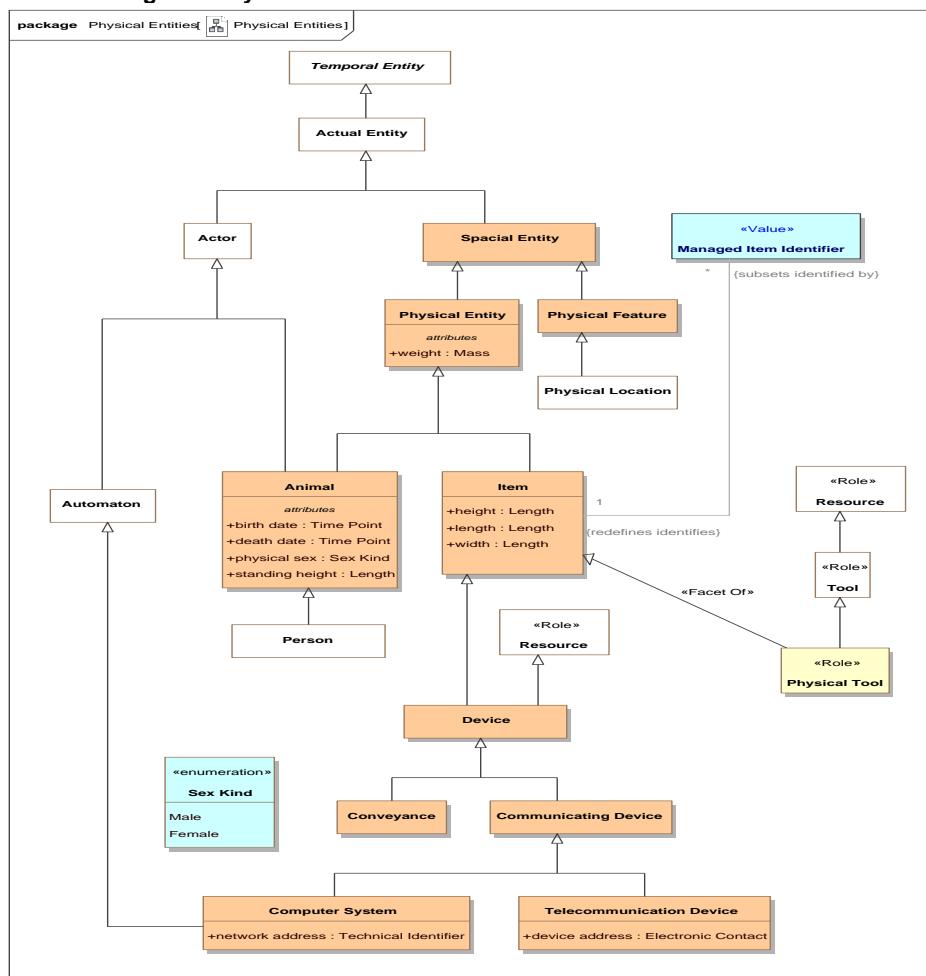


Figure 131. Physical Entities

9.22.2 Class Animal

Any member of the kingdom Animalia, comprising multicellular organisms that have a well-defined shape and usually limited growth, can move voluntarily, actively acquire food and digest it internally, and have sensory and nervous systems that allow them to respond rapidly to stimuli. A super type of "Person".

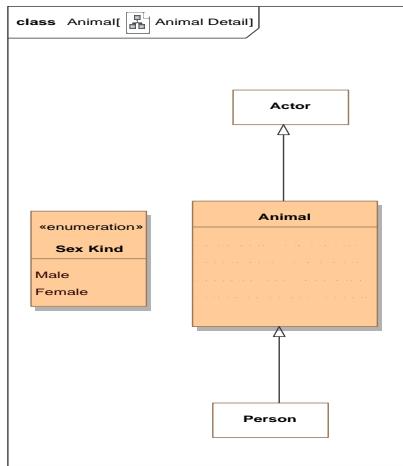


Figure 132. Animal Detail

Direct Supertypes

[Actor](#), [Physical Entity](#)

Attributes

◊ birth date : [Time Point](#)

The date an animal (including a person) was born, became an independent entity.
[FIBO] hasDateOfBirth

◊ death date : [Time Point](#)

The date an animal (including a person) died, ceased to be living.

◊ physical sex : [Sex Kind](#)

Sex of a living thing as indicated by essential physical characteristics, primarily genitalia.
[FIBO] hasGender

◊ standing height : [Length](#)

The measurement from base to top or (of a standing person) from head to foot. "Current" is relative to the time frame of the defining context.

9.22.3 Class Conveyance

A device or system providing a means of physical transport from place to place.
[NIEM] ConveyanceType

Direct Supertypes

[Device](#)

9.22.4 Class Device

A thing made for a particular purpose; an invention or contrivance, especially a mechanical or electrical one.
[NIEM] DeviceType

Direct Supertypes

[Item](#), [Resource](#)

9.22.5 Class Item

An inanimate material object as distinct from a living sentient being.
[NIEM] ItemType
[DOLCE] Non-agentive Physical Object

Direct Supertypes

[Physical Entity](#)

Attributes

◆ height : [Length](#)

[NIEM] ItemHeightMeasure: A measurement of the height of an item.
A measurement in the vertical plane. For a person, from head to toe.

◆ length : [Length](#)

[NIEM] ItemLengthMeasure: A measurement of the length of an item.
A longitudinal measurement - from end to end. Usually greater than width.

◆ width : [Length](#)

[NIEM] ItemWidthMeasure: A measurement of the width of an item.
A horizontal measurement - from side to side.

Associations

/ <>Restriction>> : [Managed Item Identifier](#) [*] Subsets: identified by:[Identifier](#)

9.22.6 Class Managed Item Identifier <>Value>>

[NIEM] An identification inscribed on or attached to a part, collection of parts, or complete unit by the manufacturer.
Syn. ItemSerialIdentification.
[FIBO] ProductIdentifier: an identifier for a product

Direct Supertypes

[Unique Identifier](#)

Associations

/ <>Restriction>> : [Item](#) [1] Redefines: identifies:[Identifiable Entity](#)

9.22.7 Class Physical Entity

A thing that exists in space and time including people, places, and things.

[DOLCE] Object

[IDEAS] Individual: A Thing that has spatio-temporal extent.

Note1 - this may be some that existed in the past, exists now, or may exist in some future possible world.

Note2 - the Individual may be scattered - i.e. it is the fusion of several disconnect parts.

Direct Supertypes

[Spacial Entity](#)

Attributes

◆ weight : [Mass](#)

The current weight (as mass) of a physical thing.

9.22.8 Class Physical Feature

Physical features are spacial entities which are generically constantly dependent on physical objects (their hosts). Typical examples of features are “parasitic entities” such as holes, boundaries, surfaces, or stains. Physical features do not have mass independent of their host.

[DOLCE] Feature

Direct Supertypes

[Spacial Entity](#)

9.22.9 Class Physical Tool <>Role>>

An physical item intended to be used to perform some function.

Direct Supertypes

[Item](#), [Tool](#)

9.22.10 Class Spacial Entity

A thing that exists in space: The union of locations and physical entities.

[DOLCE] Physical Endurant

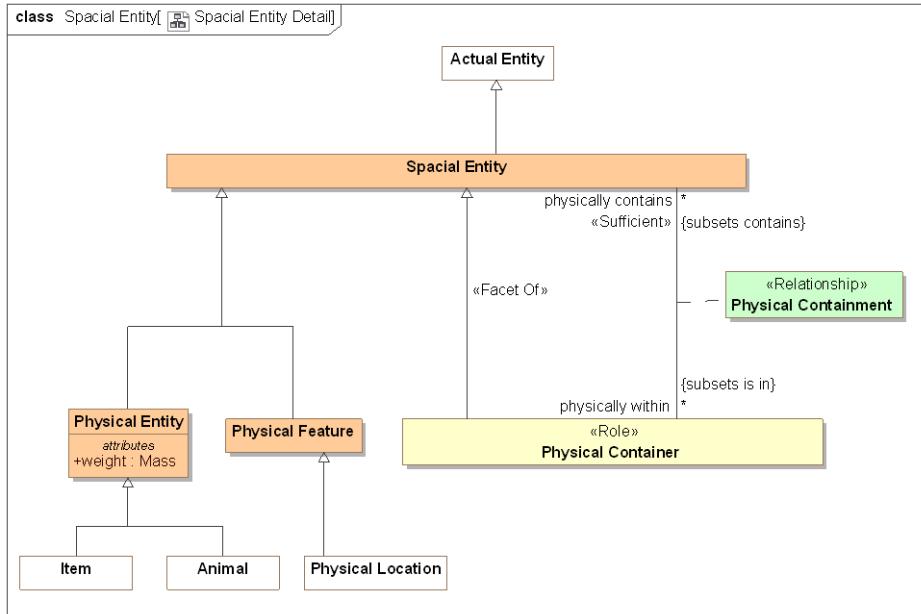


Figure 133. Spacial Entity Detail

Direct Supertypes

[Actual Entity](#)

Associations

- / <<Sufficient>> : [Physical Vulnerability](#) Subsets: has vulnerability:[Vulnerability](#)
- █ physically within : [Physical Container](#) [*] Subsets: is in:[Container](#)
through association: [Physical Containment](#)

Physical container in which the subject physical entity is contained.{transitive}
al

9.22.11 Class Telecommunication Device

A device for human to human communication over a distance by cable, telegraph, telephone, computer networks, or broadcasting.

[NIEM] TelecommunicationsDeviceType

Direct Supertypes

[Communicating Device](#)

Attributes

- device address : [Electronic Contact](#)

An code or number used to communicate with or through a telecommunications device.

9.22.111 Enumeration Sex Kind

Kinds of sex. Eg. male/female.

```
package Threat-risk-conceptual-model::Generic Concept Library::Physical Entities
public enum Sex Kind
{Male, Female}
```

Literals

- Male

A male person, plant, or animal. One able to fertilize a female with gametes.

- Female

A female person, plant, or animal. Of or denoting the sex that can bear offspring or produce eggs, distinguished biologically by the production of gametes (ova) that can be fertilized by male gametes:

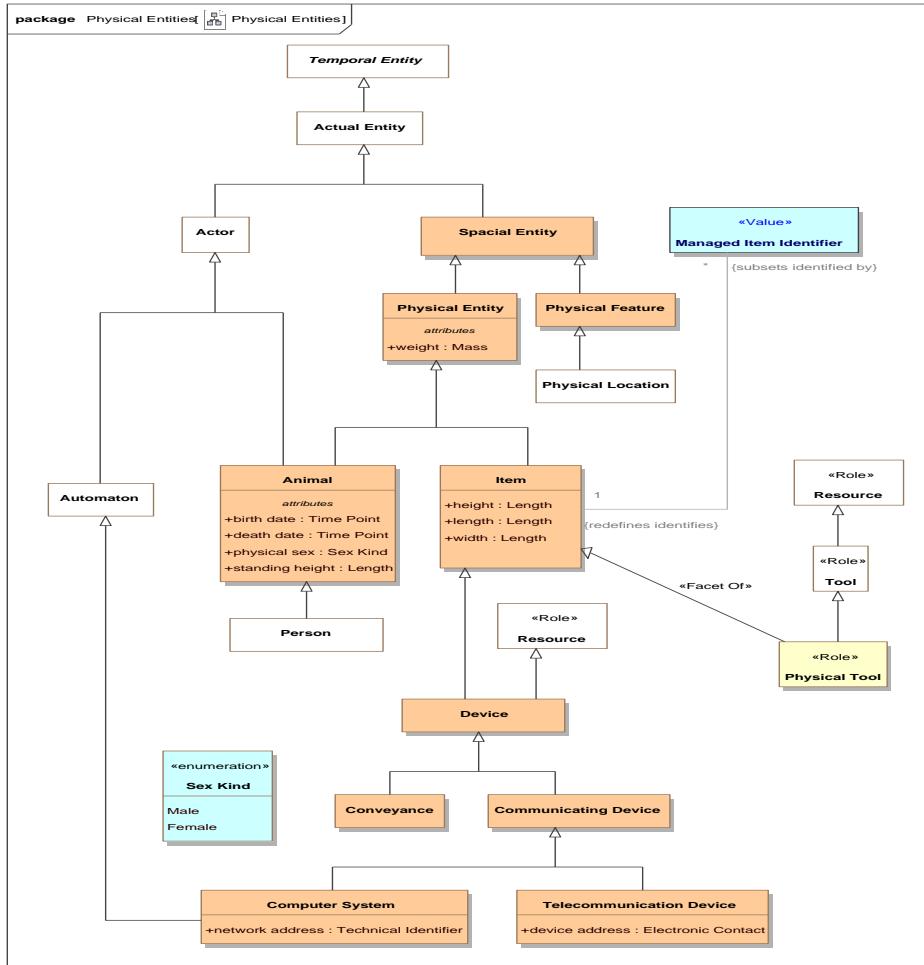


Figure 134. Physical Entities

9.23 Threat-risk-conceptual-model::Generic Concept Library::Places

This package defines concepts related to places. Places are buildings or localities used or intended for a purpose.

9.23.1 Diagram: Place

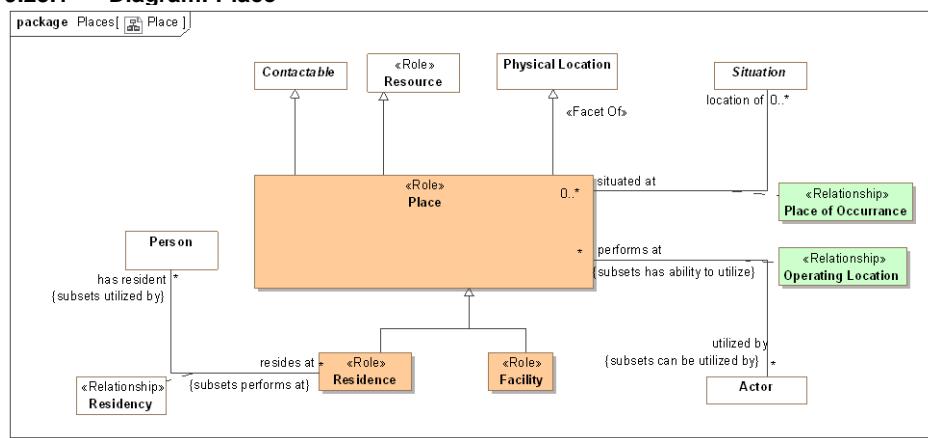


Figure 135. Place

9.23.2 Class Facility <<Role>>

[NIEM] FacilityType: A building, place, or structure that provides a particular service.

Direct Supertypes

[Place](#)

9.23.3 Association Class Operating Location <<Relationship>>

Place where an actor performs activities.

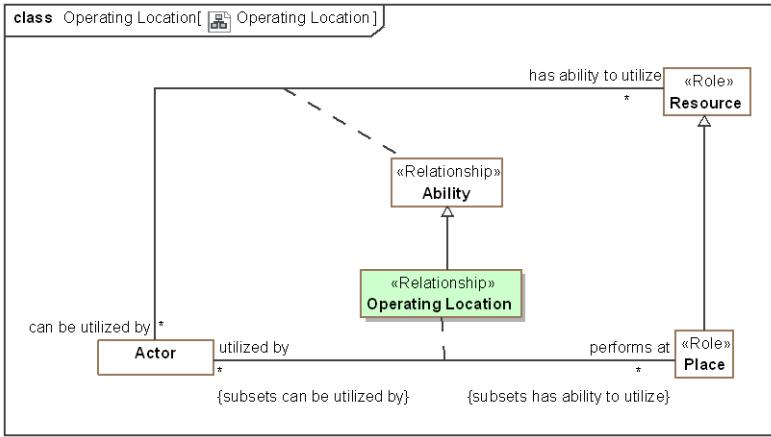


Figure 136. Operating Location

Direct Supertypes

[Ability](#)

Associations

█ performs at : [Place](#) [*] Subsets: is in:[Container](#)

Places where an actor perform activities.

█ utilized by : [Actor](#) [*] Subsets: is in:[Container](#)

Actors who utilizes a place to perform activities.

9.23.4 Class Place <<Role>>

A building or locality used or intended for a specific purpose such as a house or factory.

[FIBO] Facility: something that is built, contrived, established, or installed to serve a particular purpose, or make some course of action or operation easier, or provide some capability or service

Direct Supertypes

[Contactable](#), [Physical Location](#), [Resource](#)

Associations

█ location of : [Situation](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Place of Occurrence](#)

Situations (Events, incidents, static arrangements, etc.) that happen at the subject place.

 utilized by : [Actor](#) [*] Subsets: can be utilized by:[Actor](#)
through association: [Operating Location](#)

Actors who utilizes a place to perform activities.

9.23.5 Association Class Place of Occurrence <<Relationship>>

Relationship describing where something happens.

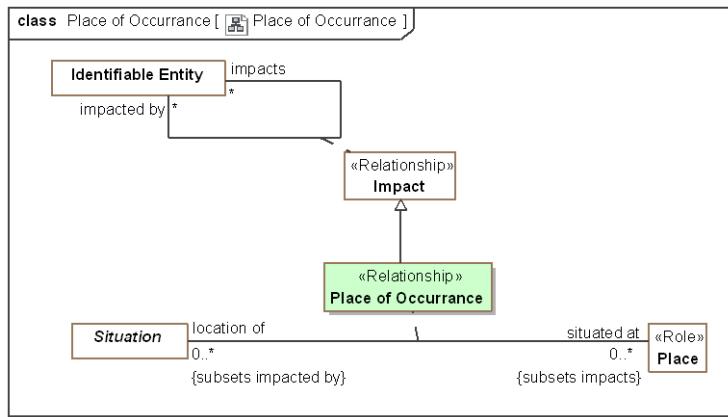


Figure 137. Place of Occurrence

Direct Supertypes

[Impact](#)

Association Ends

 situated at : [Place](#) [0..*] Subsets: can be utilized by:[Actor](#)

Place where a situation or event is located or happens.

 location of : [Situation](#) [0..*] Subsets: can be utilized by:[Actor](#)

Situations (Events, incidents, static arrangements, etc.) that happen at the subject place.

9.23.6 Class Residence <<Role>>

A place where people live/reside.

Direct Supertypes

[Place](#)

Associations

█ has resident : [Person](#) [*] Subsets: utilized by [Actor](#)
through association: [Residency](#)

A person living in a residence.

9.24 Threat-risk-conceptual-model::Generic Concept Library::Policies

This package defines concepts related to policies. Policies deal with conditions asserted on one entity by another. This includes requirements and laws.

9.24.1 Diagram: Policy

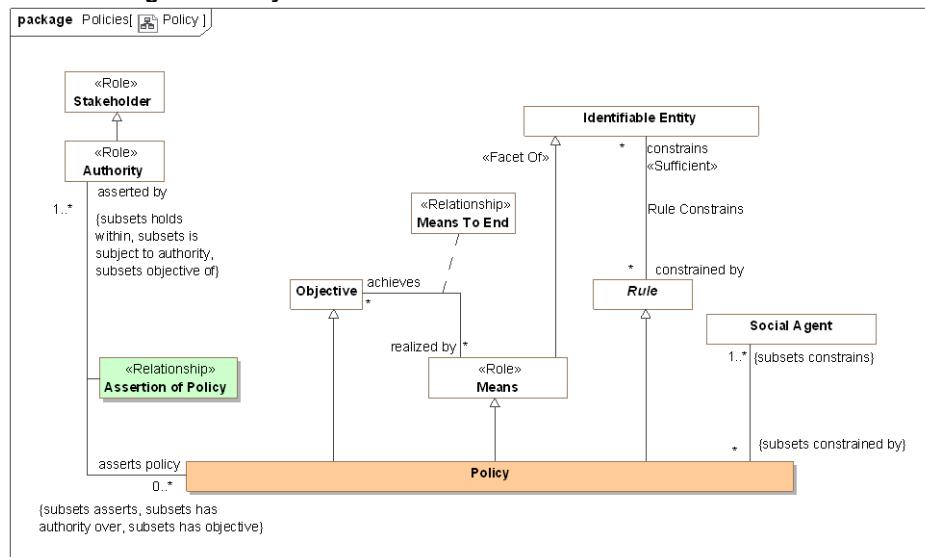


Figure 138. Policy

9.24.2 Association Class Assertion of Policy <<Relationship>>

The assertion of a policy by an authority.

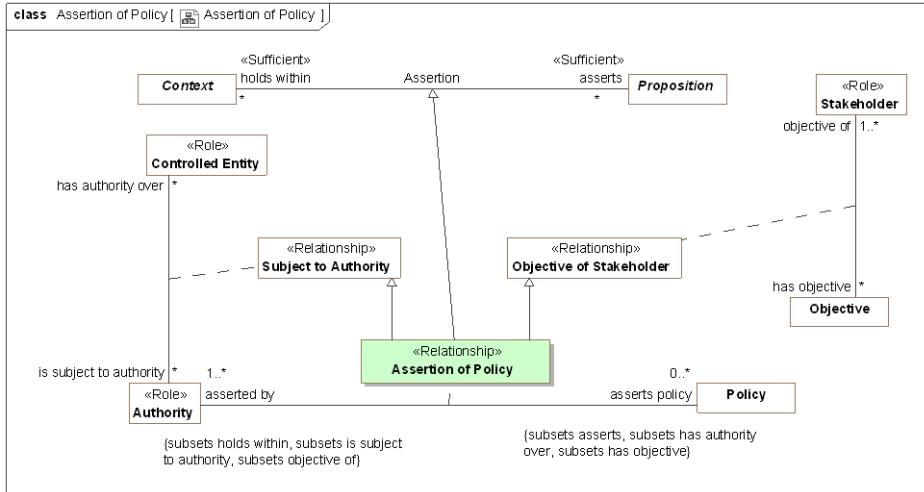


Figure 139. Assertion of Policy

Direct Supertypes

[Assertion](#), [Objective of Stakeholder](#), [Subject to Authority](#)

Association Ends

█ asserts policy : [Policy](#) [0..*] Subsets: utilized by:[Actor](#)

A policy asserted by an authority whom states with authority that it must be followed.

█ asserted by : [Authority](#) [1..*] Subsets: utilized by:[Actor](#)

The authority that asserts a policy, states with authority that it must be followed

9.24.3 Class Policy

A policy is a thing that is compulsory; a necessary condition.

A statement that identifies a necessary attribute, capability, characteristic, or quality of a system for it to have value and utility to a customer, organization, internal user, or other stakeholder. The constrained parties are identified as the <constraints> responsible performer(s).

A policy is a means in that it fulfills a broader objective. A policy is an objective in that performers seek to comply with the objective. A policy is a state in that it is a situation that exists for a finite period of time.

Policies include requirements.

[BMM] Business policy: directive that is concerned with directly controlling, influencing, or regulating the actions of an enterprise and the people in it and that is not directly enforceable

Direct Supertypes

[Controlled Entity](#), [Means](#), [Objective](#), [Rule](#)

Associations

 asserted by : [Authority](#) [1..*] Subsets: objective of:[Stakeholder](#) is subject to authority:[Authority](#) holds within:[Context](#)
through association: [Assertion of Policy](#)

The authority that asserts a policy, states with authority that it must be followed

 : [Social Agent](#) [1..*] Subsets: constrains:[Identifiable Entity](#)

9.25 Threat-risk-conceptual-model::Generic Concept Library::Predictions

Predictions are acts where an actor predicts that some possible situation will occur.

9.25.1 Diagram: Prediction

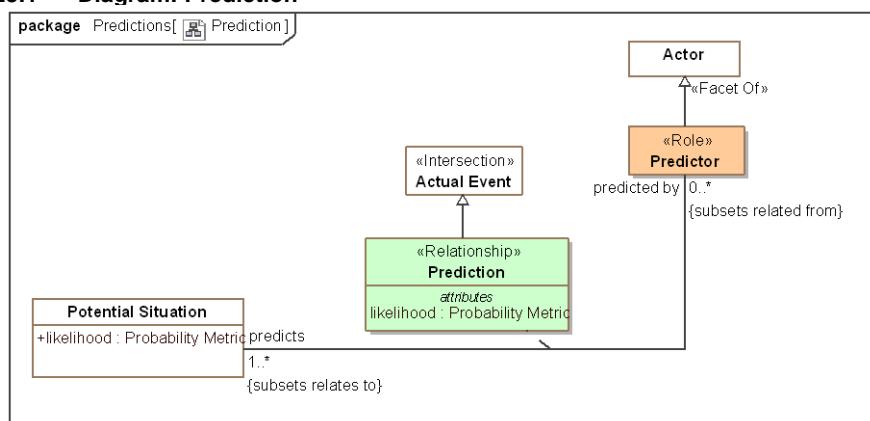


Figure 140. Prediction

9.25.2 Association Class Prediction <<Relationship>>

A prediction is a forecast that potential situations will happen.

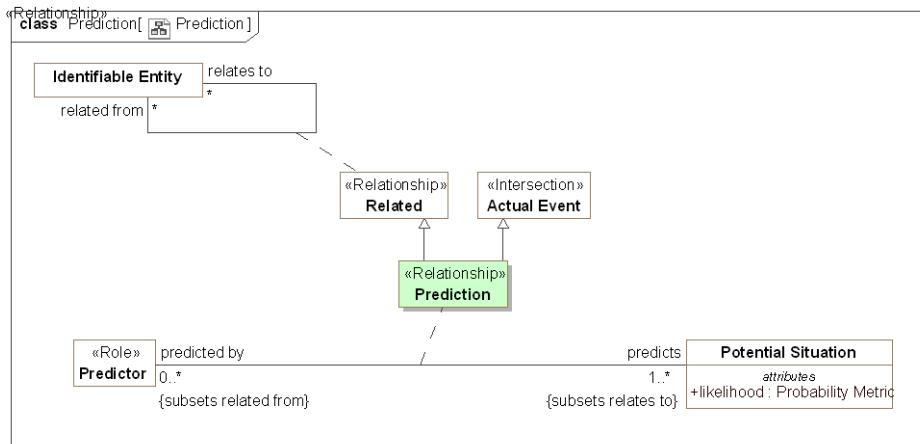


Figure 141. Prediction

Direct Supertypes

[Actual Event](#), [Related](#)

Association Ends

predicts : [Potential Situation](#) [1..*] Subsets: constrains:[Identifiable Entity](#)

The situation that is postulated by a prediction.

predicted by : [Predictor](#) [0..*] Subsets: constrains:[Identifiable Entity](#)

Predictor is the role of the actor who made a prediction.

Attributes

likelihood : [Probability Metric](#)

Metric representing the possibility that the containing element represents reality.

9.25.3 Class Predictor <<Role>>

The role of an actor making predictions.

Direct Supertypes

[Actor](#)

Associations

predicts : [Potential Situation](#) [1..*] Subsets: relates to:[Identifiable Entity](#)

through association: [Prediction](#)

The situation that is postulated by a prediction.

9.26 Threat-risk-conceptual-model::Generic Concept Library::Processes

A package representing concepts about processes. Processes are templates for (descriptions of) a related sets of Events (activities, events, etc.). Processes may be natural, organizational or carried out by an actor. Processes carried out by an actor are plans.

Processes may require resources - noting that resource can be a role of any entity.

Processes are essentially patterns of Events.

Scenarios are typically less formal processes and describe how a series of Events may play out.

9.26.1 Diagram: Process

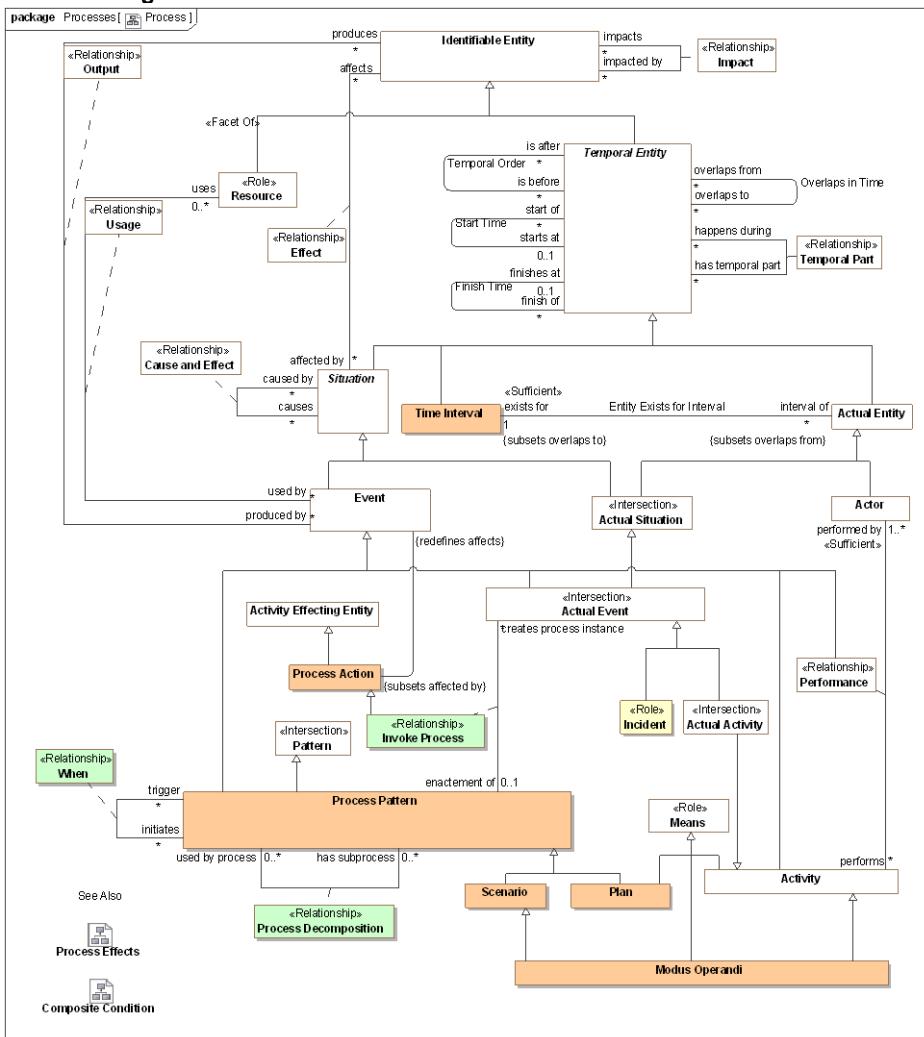


Figure 142. Process

9.26.2 Association Class Invoke Process <>Relationship>>

The activity of initiating the performance of a process.
The process instance will be classified by the process.

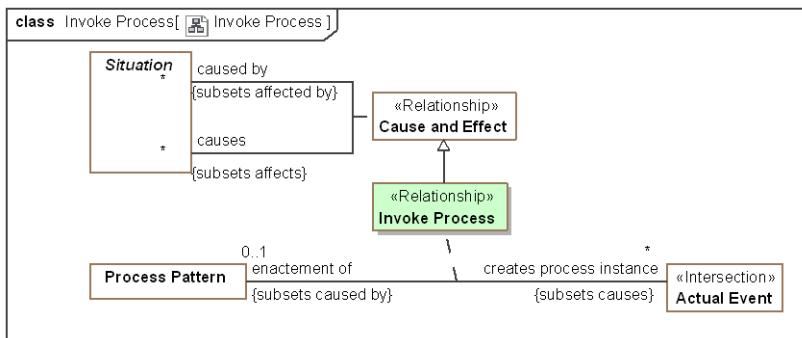


Figure 143. Invoke Process

Direct Supertypes

[Cause and Effect](#), [Create](#), [Process Action](#)

Association Ends

creates process instance : [Actual Event](#) [*] Subsets: relates to:[Identifiable Entity](#)

An actual Event created as the instantiation of a process definition.

enactment of : [Process Pattern](#) [0..1] Subsets: relates to:[Identifiable Entity](#)

Process enacted by an Invoke Process

Associations

/ <>Restriction>> : [When](#) [0..*] Subsets: produced by:[Event](#)

9.26.3 Class Modus Operandi

A particular way or method an actor typically does something, especially one that is characteristic or well-established. It may or may not have a formal definition of the process.

In threat terms, a particular tactic, technique or procedure for achieving a result.

Syn. TTP [STIX]

Direct Supertypes

[Activity](#), [Means](#), [Scenario](#)

9.26.4 Class Plan

A plan is a design for a process that supports a stakeholders objectives. As a process definition a plan is a pattern for a series of activities as well as the resources required to meet objectives.

Scenario's are observed where as plans are designed.

[BMM] Course of Action: A Course of Action is an approach or plan for configuring some aspect of the enterprise involving things, processes, locations, people, timing, or motivation undertaken to achieve Desired Results. In other words, a Course of Action channels efforts towards Desired Results. To help ensure success in this regard, Courses of Action are governed by Directives.

Direct Supertypes

[Means](#), [Process Pattern](#)

9.26.5 Class Process Action

An action impacting a potential or realized process.

Direct Supertypes

[Activity Effecting Entity](#)

Associations

/ : [Event](#) [Redefines](#): affects:[Identifiable Entity](#)

9.26.6 Association Class Process Decomposition <>Relationship>>

Relationship describing the decomposition of a process.

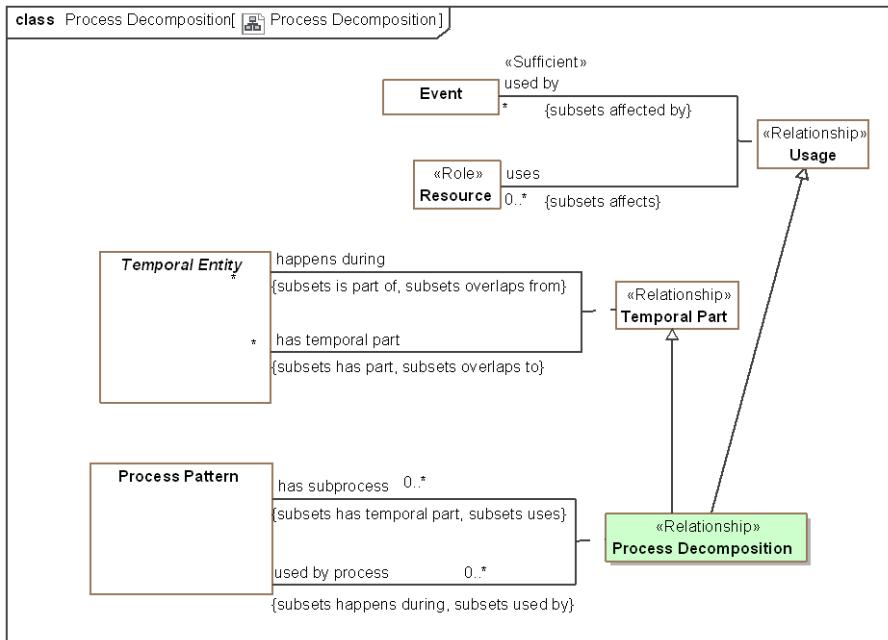


Figure 144. Process Decomposition

Direct Supertypes

[Temporal Part](#), [Usage](#)

Association Ends

has subprocess : [Process Pattern](#) [0..*] Redefines: affects: [Identifiable Entity](#)

Process occurring within the scope of and in support a composite process.

used by process : [Process Pattern](#) [0..*] Redefines: affects: [Identifiable Entity](#)

Composite processes which utilize the subject property as a component part.

9.26.7 Class Process Pattern

A process pattern is a template and definition for a family of Events (i.e. actions, events) that results in an outcome. A process may be natural or caused by the activities of actors, in which case it is a plan. A process may contain other entities, sub-processes and situations to define characteristics and sub-processes of the process. The sub-processes may or may not be known, sub-processes are defined using "Temporal Part".
[ISO 14971:2007] set of interrelated or interacting activities which transforms inputs into outputs

Direct Supertypes

[Event](#), [Pattern](#)

Associations

- / <>Restriction>> : [Software](#) [0..*] Subsets: has record:[Record](#)
- █ creates process instance : [Actual Event](#) [*] Subsets: causes:[Situation](#)
through association: [Invoke Process](#)

An actual Event created as the instantiation of a process definition.

- █ has subprocess : [Actual Event](#) [*] Subsets: causes:[Situation](#)
through association: [Process Decomposition](#)

Process occurring within the scope of and in support a composite process.

- █ used by process : [Actual Event](#) [*] Subsets: causes:[Situation](#)
through association: [Process Decomposition](#)

Composite processes which utilize the subject property as a component part.

- █ initiates : [Actual Event](#) [*] Subsets: causes:[Situation](#)
through association: [When](#)

Processes that will occur if the <trigger> process occurs. Consequent.

- █ trigger : [Actual Event](#) [*] Subsets: causes:[Situation](#)
through association: [When](#)

Processes that may cause the <initiates> process to occur. Antecedent.

9.26.8 Class Scenario

A template for a set of Events (may be but are not always activities) and resource that formally or informally depict how things may happen based on observations of similar occurrences. Scenarios are intended to be descriptive, not prescriptive.

Scenario's are observed where as plans are designed.

Direct Supertypes

[Process Pattern](#)

Attributes

- ◊ likelihood : [Probability Metric](#)

Metric representing the possibility that the scenario did happen, is happening or will happen.

Associations

- / : [Situation](#) [*] Redefines: has type:[Type](#)

Undesirable situation that is a result of a scenario happening.

9.26.9 Association Class When <>Relationship>>

A "When" rule defines an atomic process where by a <trigger> conditionally causes the <initiates> process to be invoked when the <trigger> process is matched under conditions(s) of the context - a proactive cause and effect. This results in an invocation of the <initiates> process.

E.g. when <trigger> do <initiates>

Also known as a "Course of action" or "ECA Rule".

[PRR] ProductionRule: A ProductionRule is a statement of programming logic that specifies the execution of one or more actions in the case that its conditions are satisfied.

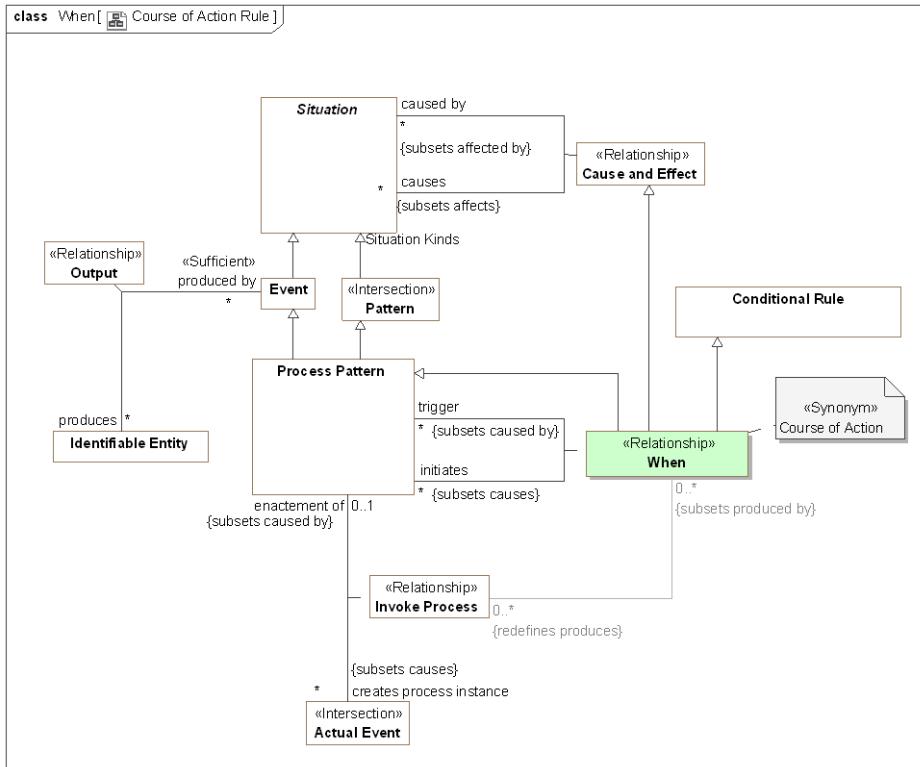


Figure 145. Course of Action Rule

Direct Supertypes

[Cause and Effect](#), [Conditional Rule](#), [Process Pattern](#)

Association Ends

 initiates : [Process Pattern](#) [*] *Redefines:* has type: [Type](#)

Processes that will occur if the <trigger> process occurs. Consequent.

 trigger : [Process Pattern](#) [*] *Redefines:* has type: [Type](#)

Processes that may cause the <initiates> process to occur. Antecedent.

Associations

 <>Restriction>> : [Invoke Process](#) [0..*] *Redefines:* produces:[Identifiable Entity](#)

9.27 Threat-risk-conceptual-model::Generic Concept Library::Processes::Composite Conditions

Composite conditions provide for "and"/"or" evaluation of causality between situations.

9.27.1 Diagram: Composite Condition

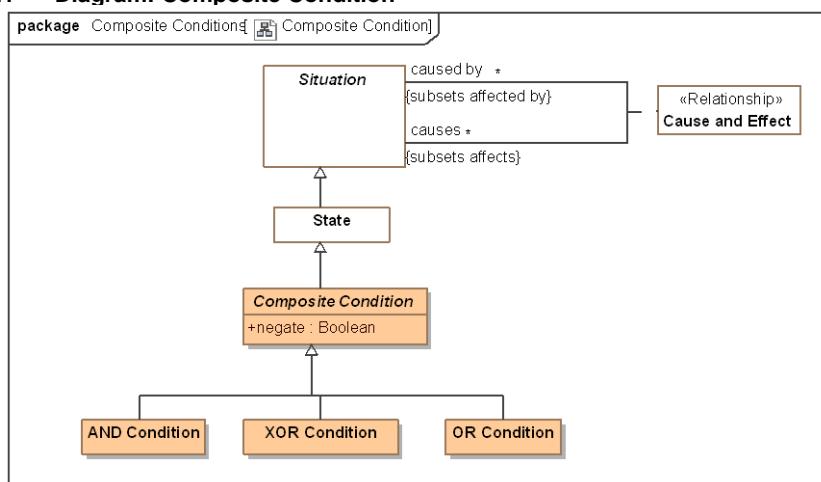


Figure 146. Composite Condition

9.27.2 Class AND Condition

A situation that is true (happening) only when all causes are true - AND

Direct Supertypes

[Composite Condition](#)

9.27.3 Class Composite Condition

A composite condition is a state that is inferred to be true or false based on the set of "caused by" (input) situations and the logic of the specific composite event subtype and the condition (if any).

The composite condition can then be used to trigger a set of "causes" (output) situations.

Combinations of Events, states, and composite conditions be combined with composite conditions to represent fault, flow or dependency graphs.

Direct Supertypes

[State](#)

Attributes

- negate : [Boolean](#)

Negates the logic of a complex event - NOT <condition>

9.27.4 Class OR Condition

A composite condition that is true (occurring) when any cause is true - OR

Direct Supertypes

[Composite Condition](#)

9.27.5 Class XOR Condition

A state that is True only when exactly one of its causes is true - XOR

Direct Supertypes

[Composite Condition](#)

9.28 Threat-risk-conceptual-model::Generic Concept Library::Processes::Process Effects

Actions that impact various kinds of entities in specific ways. Such actions can be the subject of or part of processes, permissions, capabilities, or objectives.

9.28.1 Diagram: Process Effects

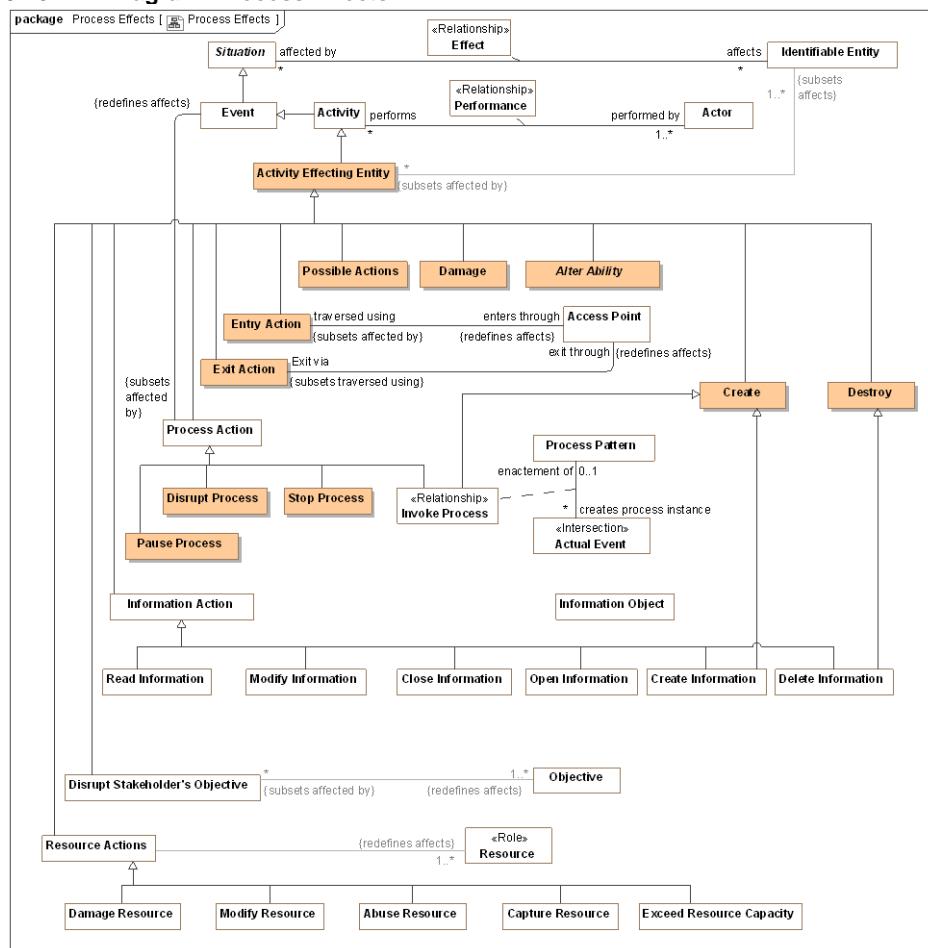


Figure 147. Process Effects

9.28.2 Class Activity Effecting Entity

An event (planned or actual) that affects specific things in specific ways.

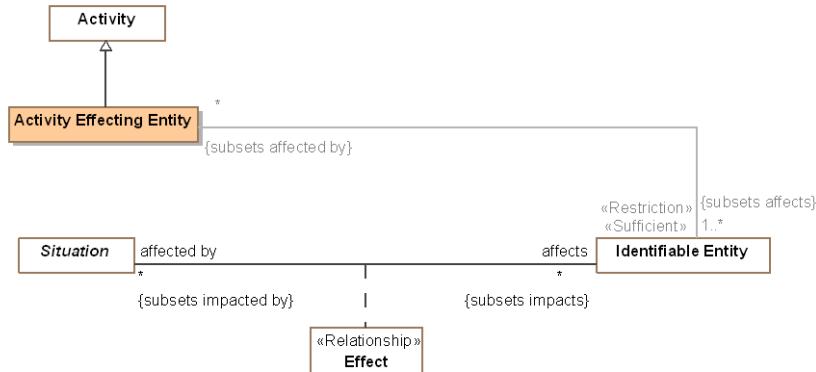


Figure 148. Event Effecting Entity

Direct Supertypes

[Activity](#)

Associations

/ <>Restriction>> : [Identifiable Entity](#) [1..*] Subsets: affects:[Identifiable Entity](#)

9.28.3 Class Create

The creation of something

Direct Supertypes

[Activity Effecting Entity](#)

9.28.4 Class Damage

An action that causes an entity to no longer completely fulfill its purpose.

Direct Supertypes

[Activity Effecting Entity](#)

9.28.5 Class Destroy

The destruction or deletion of something.

Direct Supertypes

[Activity Effecting Entity](#)

9.28.6 Class Disrupt Process

An action intended to cause a process to not achieve its desired affect.

Direct Supertypes

[Damage, Process Action](#)

9.28.7 Class Entry Action

The action of entering through a boundary.

Direct Supertypes

[Activity Effecting Entity](#)

Associations

/ enters through : [Access Point](#) Redefines: affects:[Identifiable Entity](#)

An action of entering into something through an opening in a boundary.

9.28.8 Class Exit Action

An action of exiting through a boundary.

Direct Supertypes

[Activity Effecting Entity](#)

Associations

/ exit through : [Access Point](#) Redefines: affects:[Identifiable Entity](#)

Access point used for exiting a place or system.

9.28.9 Class Pause Process

An action that pauses a process instance such that it can be restarted.

Direct Supertypes

[Process Action](#)

9.28.10 Class Possible Actions

All possible effects to an entity.

Direct Supertypes

[Activity Effecting Entity](#)

9.28.11 Class Stop Process

An action to terminate a process.

Direct Supertypes

[Process Action](#)

9.29 Threat-risk-conceptual-model::Generic Concept Library::Quantities and Units

This package defines quantities and units. Quantities are the basis for units and measurements. Qualities of things are represented with respect to what that thing means, not how it is represented. This introduces multiple "quantity kinds" which derive from Value and Quantity. Quantiles are stereotyped as "Quantity Kind". The representation of a value or quantity will typically use the "primitive types" that are found in I.T. systems such as "Integer", "Real" and "String".

9.29.1 Diagram: Quantities and units

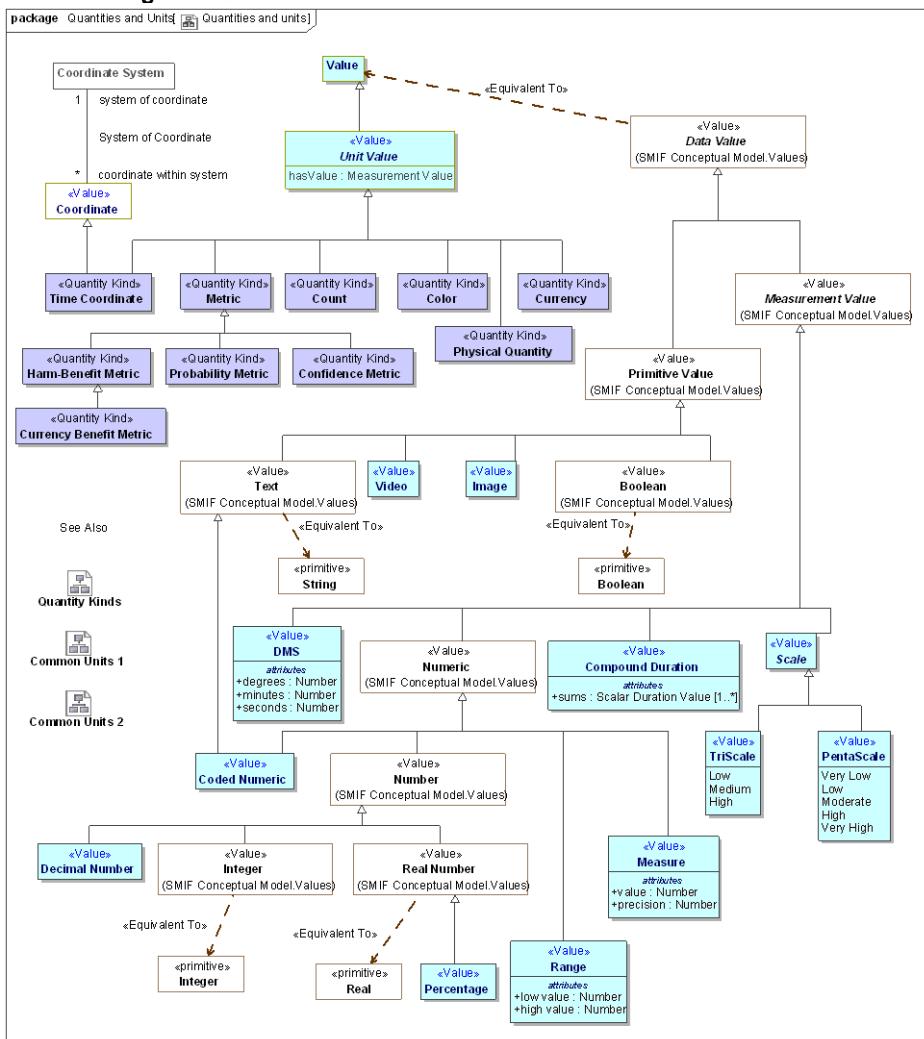


Figure 149. Quantities and units

9.29.2 Class Confidence Metric <<Quantity Kind>>

Any metric of confidence that something is true or valid.

Direct Supertypes

[Metric](#)

9.29.3 Class Count <<Quantity Kind>>

The number of something used as a property or metric, e.g., 5 fish.

Direct Supertypes

[Unit Value](#)

9.29.4 Class Currency Benefit Metric <<Quantity Kind>>

A metric for benefit or harm expressed in terms of a currency, such as dollars or yen.

Direct Supertypes

[Harm-Benefit Metric](#)

9.29.5 Class Harm-Benefit Metric <<Quantity Kind>>

A metric to quantify benefit or harm.

Direct Supertypes

[Metric](#)

9.29.6 Class Metric <<Quantity Kind>>

A standard for measuring or evaluating something in a quantifiable way.

Typical representations of a metric may be a fraction from zero to 1 or a rating such as "high, medium, low". Not to be confused with the "Metric System".

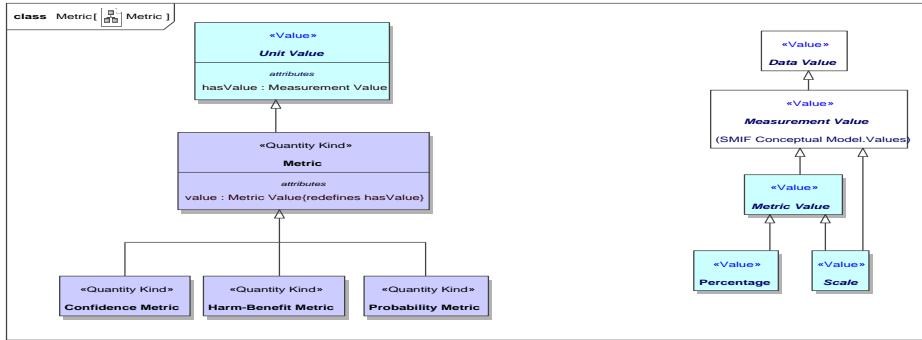


Figure 150. Metric

Direct Supertypes

[Unit Value](#)

Attributes

◊ value : [Metric Value](#)

The value of a quantity that, when multiplied by the unit defined in a subtype of quantity kind, specifies a measurement value such as 3 Meters.

9.29.7 Class Probability Metric <<Quantity Kind>>

A metric that represents the possibility that something uncertain will happen.

Direct Supertypes

[Metric](#)

9.29.8 Class Time Coordinate <<Quantity Kind>>

An identifier for a particular point in time, recognizing that any such point is an interval at a finer level of granularity. Specific time coordinate systems, such as ISO or Internet time, specialize Time Coordinate and relate it to a time scale. [DTV] time point: concept that specializes the concept 'time interval' and that is a member of a time scale [ISO11404] time: is a family of datatypes whose values are points in time to various common resolutions: year, month, day, hour, minute, second, and fractions thereof.

Direct Supertypes

[Coordinate](#), [Unit Value](#)

Attributes

◊ value : [Duration](#)

Associations

- / : [Time Scale](#) [1] Redefines: system of coordinate:[Coordinate System](#)
- / : [Time Point](#) [1] Redefines: identifies:[Identifiable Entity](#)

9.29.81 <>Value>>Enumeration PentaScale <>Value>>

An scale of 5 values the interpretation of which is context specific.

Direct Known Superclasses

Scale

```
package Threat-risk-conceptual-model::Generic Concept Library::Quantities and Units
public enum PentaScale
{Very Low, Low, Moderate, High, Very High}
```

Literals

- Very Low
- Low
- Moderate
- High
- Very High

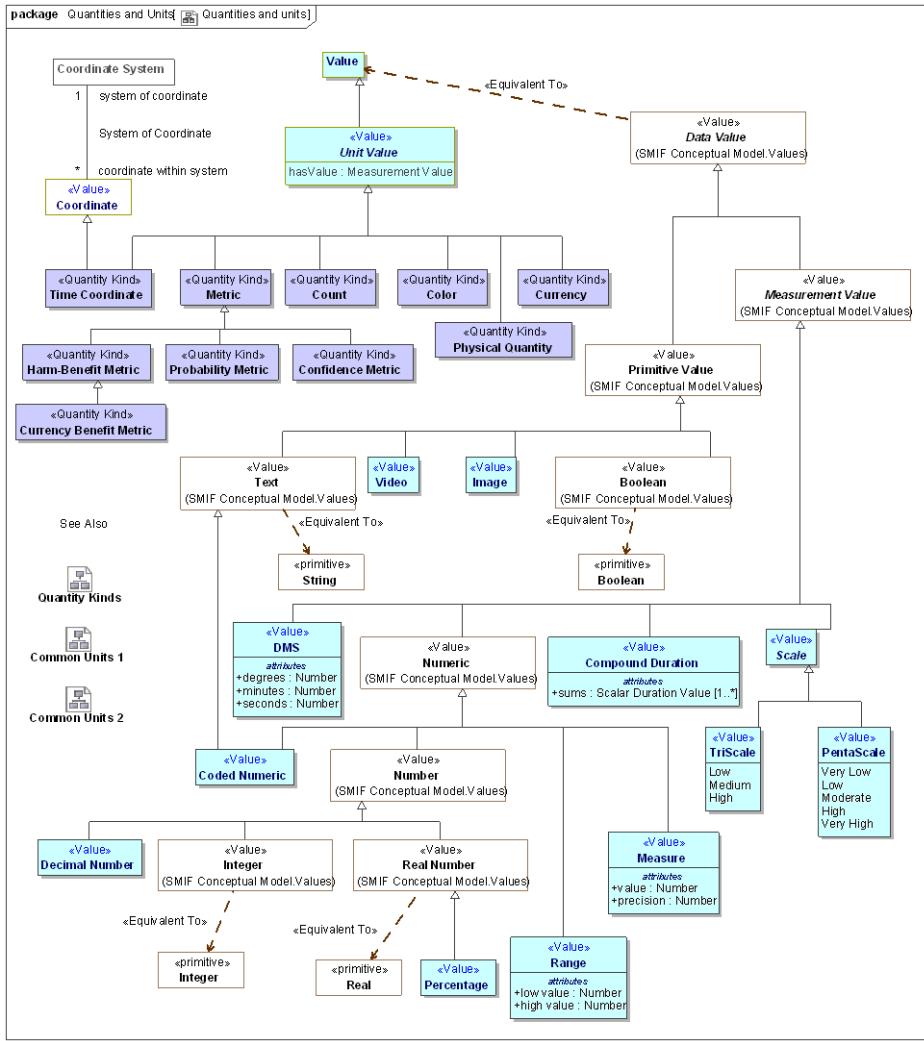


Figure 151. Quantities and units

9.29.82 <>Value>>Enumeration TriScale <>Value>>

A scale of 3 arbitrary levels.

Direct Known Superclasses

Scale

```
package Threat-risk-conceptual-model::Generic Concept Library::Quantities and Units
public enum TriScale
{Low, Medium, High}
```

Literals

- Low
- Medium
- High

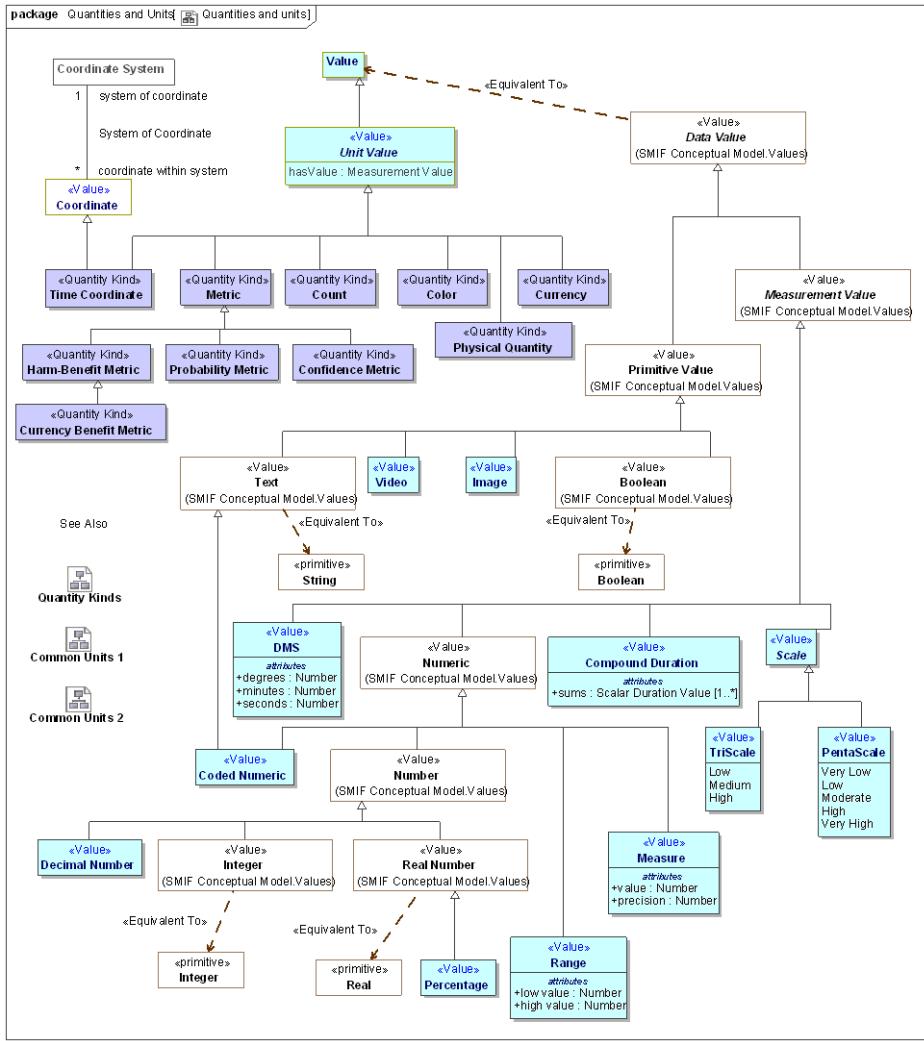


Figure 152. Quantities and units

9.30 Threat-risk-conceptual-model::Generic Concept Library::Quantities and Units::Quantity Kinds

Quantity kinds are abstractions for the way we measure or quantify things, such as mass or length. Units provide specific ways to specify a quantity kind. Note that specific units (non normative) are defined in the OTR model and specified in an ancillary document.

9.30.1 Diagram: Quantity Kinds

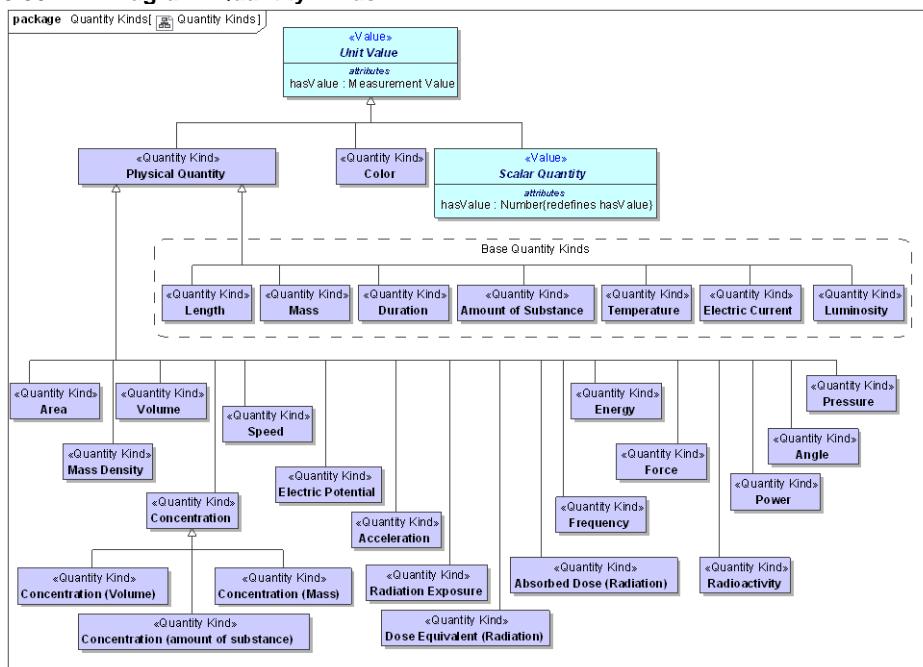


Figure 153. Quantity Kinds

9.30.2 Class Absorbed Dose (Radiation) <<Quantity Kind>>

The energy of ionizing radiation absorbed per unit mass by a body, often measured in rads.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.3 Class Acceleration <<Quantity Kind>>

The rate of change of velocity per unit of time.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.4 Class Amount of Substance <<Quantity Kind>>

The abstract unit of the amount of a substance which is the supertype of all amount units and also acts as its "quantity kind".

Amount of substance is a standards-defined quantity that measures the size of an ensemble of elementary entities, such as atoms, molecules, electrons, and other particles. It is sometimes referred to as chemical amount. The International System of Units (SI) defines the amount of substance to be proportional to the number of elementary entities present. The SI unit for amount of substance is the mole. It has the unit symbol mol.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.5 Class Angle <<Quantity Kind>>

The space (usually measured in radians or degrees) between two intersecting lines or surfaces at or close to the point where they meet.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.6 Class Area <<Quantity Kind>>

[QUDT] Area is a quantity expressing the two-dimensional size of a defined part of a surface, typically a region bounded by a closed curve.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.7 Class Color <<Quantity Kind>>

Color is the visual perceptual property corresponding in humans to the categories called red, blue, yellow, and others. Color derives from the spectrum of light (distribution of light power versus wavelength) interacting in the eye with the spectral sensitivities of the light receptors. Color categories and physical specifications of color are also associated with objects or materials based on their physical properties such as light absorption, reflection, or emission spectra. By defining a color space, colors can be identified numerically by their coordinates.

Direct Supertypes

[Unit Value](#)

9.30.8 Class Concentration <<Quantity Kind>>

The abstract concept of the amount, mass or volume of one substance in another without being specific as to how it is measured.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.9 Class Concentration (amount of substance) <<Quantity Kind>>

Concentration based on amount-of-substance.

Direct Supertypes

[Concentration](#)

9.30.10 Class Concentration (Mass) <<Quantity Kind>>

Concentration based on mass per unit of volume.

Direct Supertypes

[Concentration](#)

9.30.11 Class Concentration (Volume) <<Quantity Kind>>

Volume concentration is defined as the volume of a constituent divided by the volume of the mixture.

Direct Supertypes

[Concentration](#)

9.30.12 Class Currency <<Quantity Kind>>

Any form of money.

[FIBO] Currency: medium of exchange value, defined by reference to the geographical location of the authorities responsible for it

Direct Supertypes

[Unit Value](#)

9.30.13 Class Dose Equivalent (Radiation) <<Quantity Kind>>

A measure of the biological damage to living tissue as a result of radiation exposure. Also known as the "biological dose," the dose equivalent is calculated as the product of absorbed dose in tissue multiplied by a quality factor and then sometimes multiplied by other necessary modifying factors at the location of interest. The dose equivalent is expressed numerically in rems or sieverts (Sv) (see 10 CFR 20.1003). For additional information, see Doses in Our Daily Lives and Measuring Radiation. [NRC]

For practical purposes, 1 R (exposure) = 1 rad (absorbed dose) = 1 rem or 1000 mrem (dose equivalent).

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.14 Class Duration <<Quantity Kind>>

The abstract quantity kind of time which is the supertype of all time duration units.

Time is a measure that allows events to be ordered from the past through the present into the future, and also the measure of durations of events and the intervals between them. Durations are quantities of time, not points or intervals of time.

[DTV] base quantity of the International System of Quantities, used for measuring time intervals.

[IDEAS] Time: A MeasureInstance whose members are Individuals that have a particular temporal dimension of the same length.

[FIBO] Duration: An amount of time.

[UML] Duration

[OWL] xsd:duration

Direct Supertypes

[Physical Quantity](#)

Associations

- granularity of : [Time Scale](#) [*]
through association: [Time Scale Granularity](#)

Duration of each time point on a time scale.

- <<Characteristic>> duration of : [Temporal Entity](#) [*]
through association: [Duration of Entity](#)

Temporal entity for which a duration is applicable.

9.30.15 Class Electric Current <<Quantity Kind>>

The abstract quantity kind of electric current which is the supertype of all current units.

[QUDT]Electric Current is the flow (movement) of electric charge. The amount of electric current through some surface, e.g., a section through a copper conductor, is defined as the amount of electric charge flowing through that surface over

time. Current is a scalar-valued quantity.

The SI unit for measuring an electric current is the ampere, which is the flow of electric charge across a surface at the rate of one coulomb per second.

[IDEAS] ElectricCurrent: A MeasureInstance whose members are Individuals that all have the same electric current flowing through them

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.16 Class Electric Potential <<Quantity Kind>>

[QUOTD] Electric Potential is a scalar valued quantity associated with an electric field.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.17 Class Energy <<Quantity Kind>>

The measure of energy- the ability to perform work (such as moving a mass).

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.18 Class Force <<Quantity Kind>>

(Physical) force is an influence that causes mass to accelerate. It may be experienced as a lift, a push, or a pull.

Force is defined by Newton's Second Law as $F = m \cdot a$, where F is force, m is mass and a is acceleration. Net force is mathematically equal to the time rate of change of the momentum of the body on which it acts. Since momentum is a vector quantity (has both a magnitude and direction).

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.19 Class Frequency <<Quantity Kind>>

Repetitions per unit of time. e.g., Hertz.

[IDEAS] Frequency: A MeasureInstance whose instances are Individuals that all oscillate at the same frequency

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.20 Class Length <<Quantity Kind>>

The abstract unit of distance (or length) which is the supertype of all length units and also acts as its "quantity kind".

In the International System of Quantities, length is any quantity with dimension distance. In other contexts "length" is the measured dimension of an object.

[IDEAS] Length: A MeasureInstance whose instances are Individuals that all have the same length

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.21 Class Luminosity <<Quantity Kind>>

Luminosity (or luminous intensity) is a measure of the wavelength-weighted power emitted by a light source in a particular direction per unit solid angle, based on the luminosity function, a standardized model of the sensitivity of the human eye. The SI unit of luminous intensity is the candela (cd), an SI base unit.

[IDEAS] LuminousIntensity: A MeasureInstance whose members are Individuals that all have the same luminous intensity

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.22 Class Mass <<Quantity Kind>>

The abstract unit of Mass which is the supertype of all mass units and also acts as its "quantity kind".

The mass of a body is a measure of its inertial property or how much matter it contains. The weight of a body is a measure of the force exerted on it by gravity or the force needed to support it. Gravity on earth gives a body a downward acceleration of about 9.8 m/s².The SI unit of mass is the kilogram (kg).

[IDEAS] Mass: A MeasureInstance whose members are Individuals that all have the same mass.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.23 Class Mass Density <<Quantity Kind>>

The density, or more precisely, the volumetric mass density, of a substance is its mass per unit volume. The symbol most often used for density is ρ (the lower case Greek letter rho). Mathematically, density is defined as mass divided by volume.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.24 Class Physical Quantity <<Quantity Kind>>

A measurable property of a physical object.

Direct Supertypes

[Unit Value](#)

9.30.25 Class Power <<Quantity Kind>>

(Physical) power is the rate at which work is performed or energy is transmitted, or the amount of energy required or expended for a given unit of time. As a rate of change of work done or the energy of a subsystem, power is: $P = W/t$ where P is power W is work t is time.

Direct Supertypes

[Physical Quantity](#)

9.30.26 Class Pressure <<Quantity Kind>>

A quantity kind representing the continuous physical force exerted on or against an object by something in contact with it.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.27 Class Radiation Exposure <<Quantity Kind>>

A measure of exposure to radiation.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.28 Class Radioactivity <<Quantity Kind>>

Radioactivity is a quantity kind that refers to the amount of ionizing radiation released by a material. Whether it emits alpha or beta particles, gamma rays, x-rays, or neutrons, a quantity of radioactive material is expressed in terms of its radioactivity (or simply its activity), which represents how many atoms in the material decay in a given time period. The units of measure for radioactivity are the curie (Ci) and Becquerel (Bq).

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.29 Class Speed <<Quantity Kind>>

A Quantity kind representing distance per unit of time.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.30 Class Temperature <<Quantity Kind>>

The abstract quantity kind of Thermodynamic temperature which is the supertype of all temperature units and also acts as its "quantity kind".

Thermodynamic temperature is the absolute measure of temperature and it is one of the principal parameters of thermodynamics.

Thermodynamic temperature is defined by the third law of thermodynamics in which the theoretically lowest temperature is the null or zero point.

[IDEAS] ThermodynamicTemperature:

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.30.31 Class Volume <<Quantity Kind>>

A quantity kind for the amount of space that a substance or object occupies.

Direct Supertypes

[Physical Quantity](#), [Scalar Quantity](#)

9.31 Threat-risk-conceptual-model::Generic Concept Library::Resources

This package represents concepts concerning resources. A resource is a role of any entity such that it supports or impacts in a process, impacts the objectives of stakeholders or is the basis of the capability of an actor. As a role, "Resource" is intended to "mix in" with an entity type such as "Person" or "Process" such that the use of that entity may be understood. Resources that are a Primary Asset are those that are the direct subject of a stakeholder's objectives.

9.31.1 Diagram: Resource

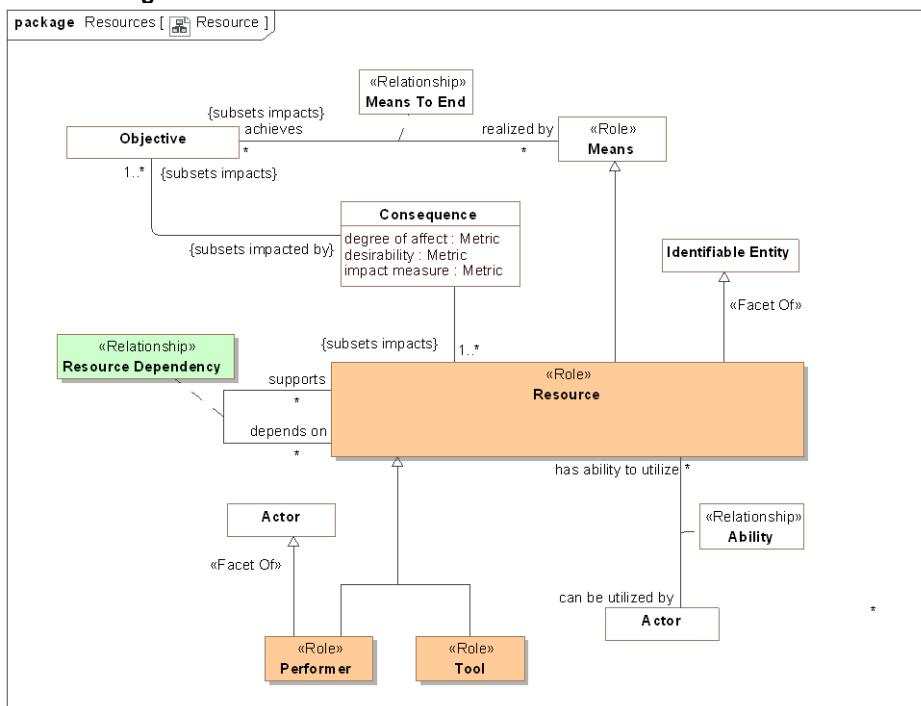


Figure 154. Resource

9.31.2 Diagram: Resource Actions

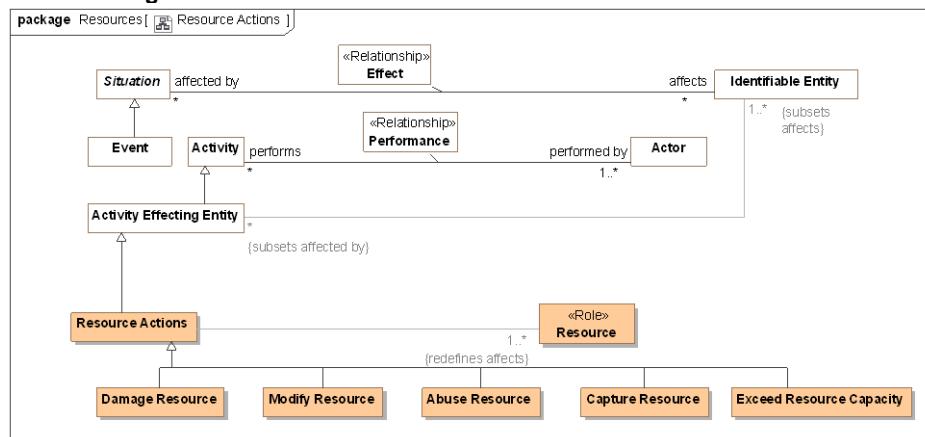


Figure 155. Resource Actions

9.31.3 Class Abuse Resource

An action to misuse a resource.

Direct Supertypes

[Resource Actions](#)

9.31.4 Class Capture Resource

Action to capture or gain control of some resource.

Direct Supertypes

[Resource Actions](#)

9.31.5 Class Damage Resource

An action that causes a resource to no longer completely fulfill its purpose..

Direct Supertypes

[Damage](#), [Resource Actions](#)

9.31.6 Class Exceed Resource Capacity

An action to exceed the capacity of some resource.

Direct Supertypes

[Resource Actions](#)

9.31.7 Class Modify Resource

Action to modify a resource or set of resources.

Direct Supertypes

[Resource Actions](#)

9.31.8 Class Performer <>Role>>

A performer is an actor that is a resource to another entity as the performer of activities.

Direct Supertypes

[Actor](#), [Resource](#)

9.31.9 Class Resource <>Role>>

A resource is a role of an entity required for or helpful to any operation, activity, process or capability - directly or indirectly. Sometimes called an "asset".

Direct Supertypes

[Identifiable Entity](#), [Means](#)

Associations

- █ harmed by : [Undesirable Situation](#) [*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Harms Resource](#)
- █ has failure : [Failure](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Failure of Resource](#)

Realized or potential failures of a resource.

- █ has vulnerability : [Vulnerability](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Vulnerability of Resource](#)

Vulnerabilities of a resource, ways it may be compromised.

- █ attacked by : [Attack](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Target of Attack](#)

Attack on a resource.

 protected by : [Countermeasure](#) [*] Subsets: depends on: [Resource](#)
through association: [Protection](#)

Countermeasure that protects the subject resource.

 has risk of harm : [Risk](#) [0..*] Subsets: assessed by: [Assessment](#)
through association: [Risk To Resource](#)

Potential risk to the subject resource.

 can be utilized by : [Actor](#) [*] Subsets: impacted by: [Identifiable Entity](#)
through association: [Ability](#)

The actor having the ability to utilize a resource for a purpose.

 affected by action : [Alter Ability](#) [*] Subsets: affected by: [Situation](#)
through association: [Affected Available Resource](#)

Actions which impact the availability of a resource to actors.

 : [Consequence](#)

Situations that impact a resource.

 supports : [Consequence](#)
through association: [Resource Dependency](#)

Resources the subject resource supports or enables.

 depends on : [Consequence](#)
through association: [Resource Dependency](#)

A resource that is required to support the operation of purpose of another resource.

 : [Resource Actions](#)
 <>Sufficient>> used by : [Event](#) [*] Subsets: affected by: [Situation](#)
through association: [Usage](#)

A process or actual event that is used by a resource to fulfill its function.

9.31.10 Class Resource Actions

An action impacting a potential or realized resource/asset.

Direct Supertypes

[Activity Effecting Entity](#)

Associations

 : [Resource](#) [1..*] *Redefines: affects:* [Identifiable Entity](#)

9.31.11 Association Class Resource Dependency <>Relationship>>

Relationship between resources where one resource depends on (or uses) another.

A more general concept than [UAF] MapsToCapability: An Abstraction relationship denoting that an Activity contributes to providing a Capability.

[DOLCE] (Subtype of) Dependence

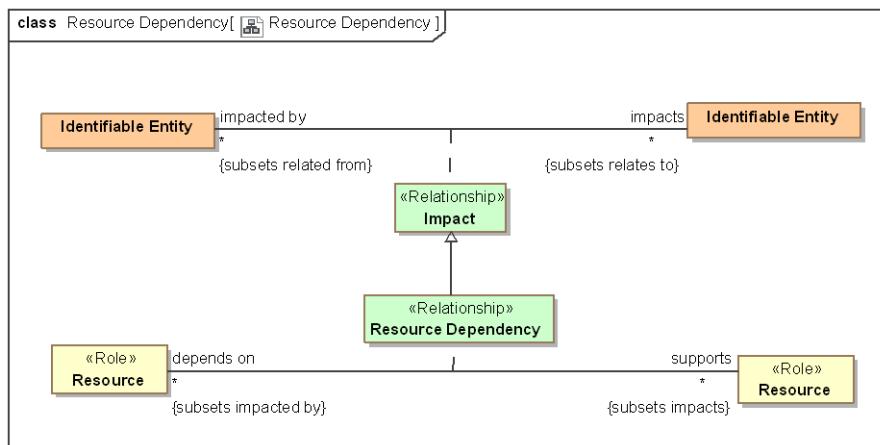


Figure 156. Resource Dependency

Direct Supertypes

[Impact](#)

Association Ends

 supports : [Resource](#) [*] *Redefines: affects:* [Identifiable Entity](#)

Resources the subject resource supports or enables.

 depends on : [Resource](#) [*] *Redefines: affects:* [Identifiable Entity](#)

A resource that is required to support the operation or purpose of another resource.

9.31.12 Class Tool <>Role>>

The role of some inanimate thing used to facilitate a process or activity by an actor performing a process or activity.

Direct Supertypes

[Resource](#)

9.32 Threat-risk-conceptual-model::Generic Concept Library::Situations

Concepts relative to situations. A situation is a particular configuration of things and their relations including spatial, temporal, and logical connections between those things valid over a period of time. Situations form the basis of all complex, time dependent entities.

9.32.1 Diagram: Situation

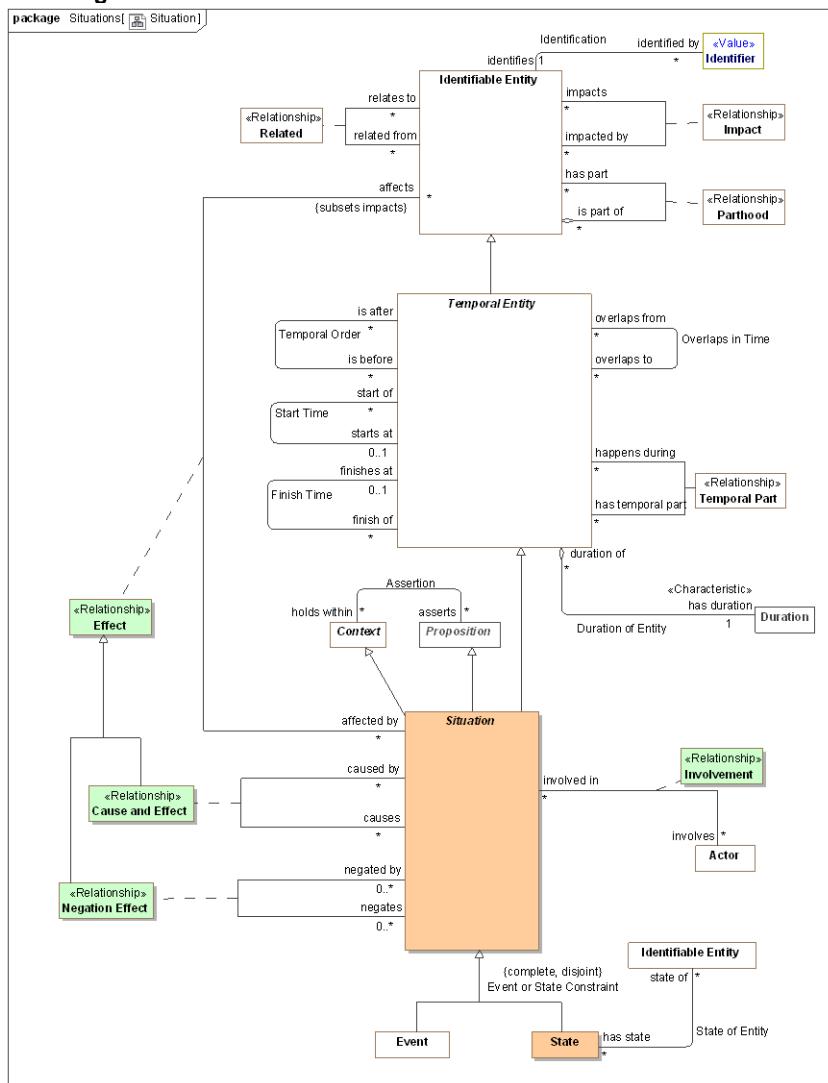


Figure 157. Situation

This diagram shows the primary associations defined for situations as well as its super types: Temporal Entity and Identifiable Entity. The relationships shown here are those deemed defining for the concept of a situation, they are not all the relationships defined for these types.

9.32.2 Diagram: Situation Timeframes

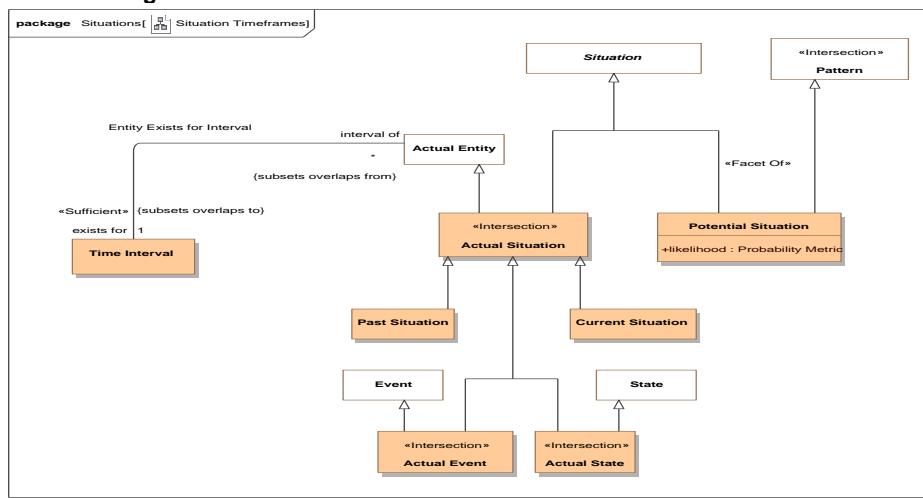


Figure 158. Situation Timeframes

9.32.3 Class Actual State <<Intersection>>

A condition that has, will or does exist.

Direct Supertypes

[Actual Situation](#), [State](#)

9.32.4 Association Class Cause and Effect <<Relationship>>

The causality relation where the <causes> situation is <caused by> a situation.

[FIBO] cause / caused by

[ISO 1087] causal relation: associative relation (3.2.23) involving cause and its effect

NOTE A causal relation exists between the concepts (3.2.1) 'action' and 'reaction', 'nuclear explosion' and 'fall-out'.

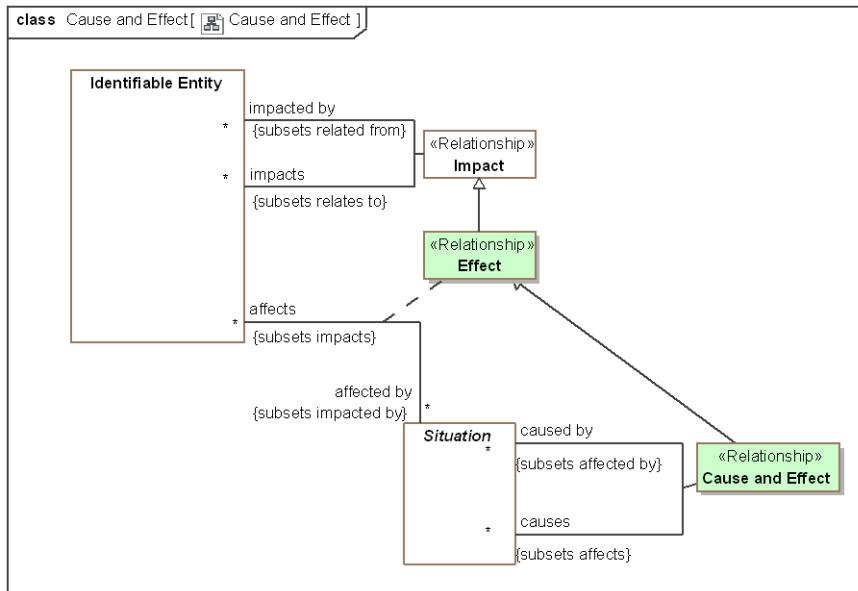


Figure 159. Cause and Effect

Direct Supertypes

[Effect](#)

Association Ends

 caused by : [Situation](#) [*] Redefines: affects: [Identifiable Entity](#)

One of situations that causes the subject situation.

 causes : [Situation](#) [*] Redefines: affects: [Identifiable Entity](#)

A situation caused by another.

9.32.5 Class Current Situation

A situation that is actually occurring at the moment. "the moment" is contextual and interpreted within the context of the model.

Direct Supertypes

[Actual Situation](#), [Situation](#)

9.32.6 Association Class Effect <<Relationship>>

Any impact or alteration of an entity by a situation.

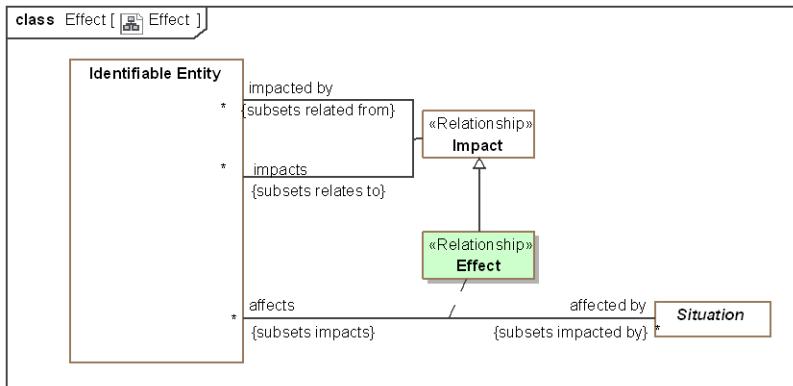


Figure 160. Effect

Direct Supertypes

Impact

Association Ends

affects : [Identifiable Entity](#) [*] *Redefines*: affects: [Identifiable Entity](#)

Entities affected by a action

affected by : [Situation](#) [*] *Redefines*: affects: [Identifiable Entity](#)

Actions that can cause some change in a related entity.

9.32.7 Association Class Involvement <<Relationship>>

The relationship between an actor and situations they are involved in.
[DOLCE] Participation

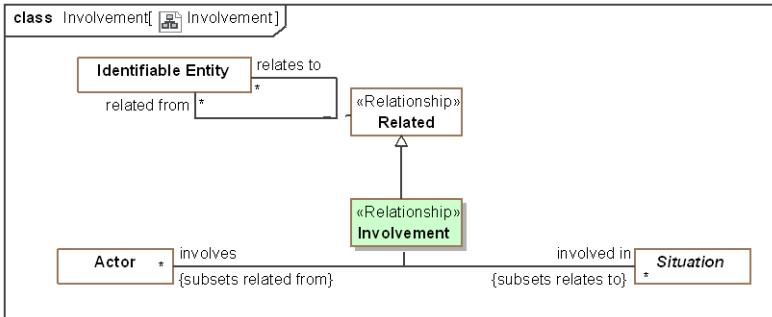


Figure 161. Involvement

Direct Supertypes

[Related](#)

Association Ends

involved in : [Situation](#) [*] Redefines: affects: [Identifiable Entity](#)

Situations in which an actor has any kind of involvement.

involves : [Actor](#) [*] Redefines: affects: [Identifiable Entity](#)

An actor involved in a situation in any way.

9.32.8 Association Class Negation Effect <>Relationship>>

The negative causality relationship - <negated by> prevents or terminates the <negates> situation.

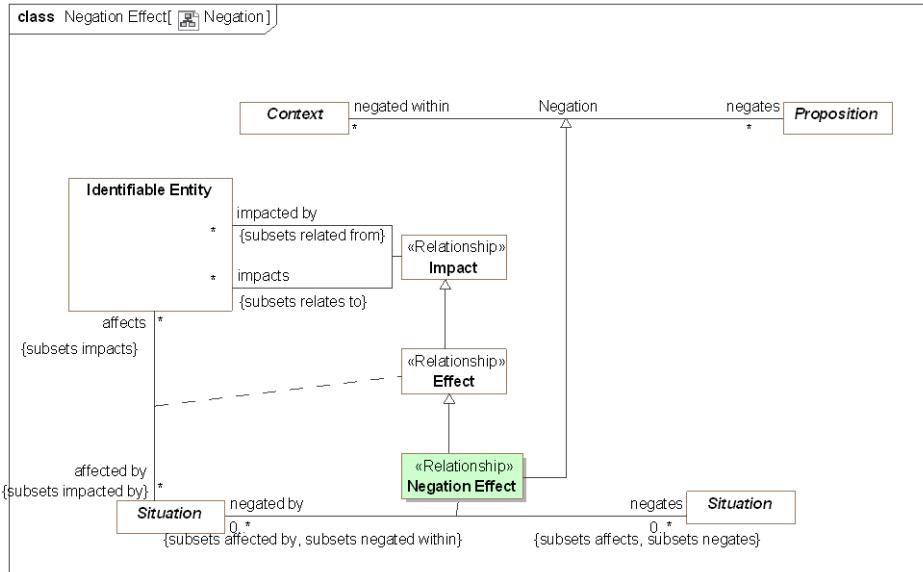


Figure 162. Negation

Direct Supertypes

[Effect](#), [Negation](#)

Association Ends

negated by : [Situation](#) [0..*] Redefines: affects: [Identifiable Entity](#)

A situation that prevents or terminates another.

negates : [Situation](#) [0..*] Redefines: affects: [Identifiable Entity](#)

A situation that is prevented or terminated by another situation.

9.32.9 Class Past Situation

A situation that has actually occurred in the past (recognizing that all such statements are subject to confidence).

Direct Supertypes

[Actual Situation](#), [Situation](#)

9.32.10 Class Potential Situation

A situation that has not yet happened but has a potential to happen.

DTV: Situation Kind

Direct Supertypes

[Pattern](#), [Situation](#)

Attributes

◊ likelihood : [Probability Metric](#)

Metric representing the possibility that the containing element represents reality.

Associations

█ pattern indicated by : [Indicator](#) [*] Subsets: related from:[Identifiable Entity](#)
through association: [Indicator Indicates Situation](#)

Indicator that may be used as evidence that a potential situation has been realized by an actual situation.

█ predicted by : [Predictor](#) [0..*] Subsets: related from:[Identifiable Entity](#)
through association: [Prediction](#)

Predictor is the role of the actor who made a prediction.

9.32.11 Association Class Scope of Indicator <<Relationship>>

Relationship defining the scope of an indicators validity, the indicator is only valid within this context.

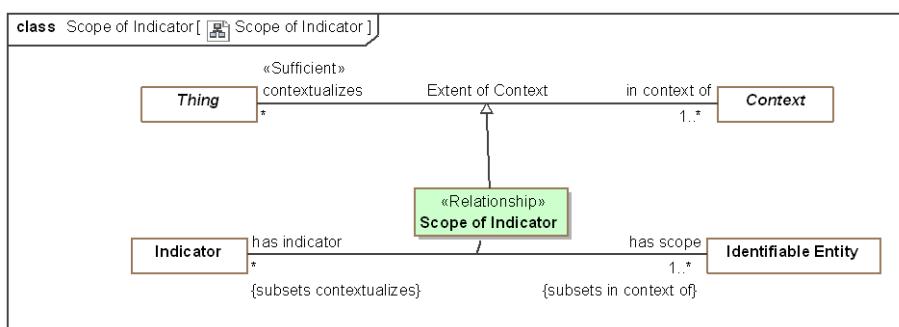


Figure 163. Scope of Indicator

Direct Supertypes

[Extent of Context](#)

Association Ends

 has indicator : [Indicator](#) [*] Subsets: related from:[Identifiable Entity](#)

Indicators that influence the evaluation of the state of an entity.

 has scope : [Identifiable Entity](#) [1..*] Subsets: related from:[Identifiable Entity](#)

An entity that defines a context for where an indicator is valid.

9.32.12 Class State

A state is a static situation - a particular configuration of entities that is static for a time period, including spatial and logical connections between those things {Snapshot of a Perdurant}

Note that states may be of any length, from an instant to infinity and beyond.

[DOLCE] State

Direct Supertypes

[Situation](#)

Associations

 state of : [Identifiable Entity](#) [*] Subsets: relates to:[Identifiable Entity](#)
through association: [State of Entity](#)

The endurant entity for which the subject state is a snapshot.

9.32.13 Association State of Entity

Relationship between a perdurant (something that exists over time) and a "state" of that entity as a snapshot in time.

Association Ends

 state of : [Identifiable Entity](#) [*] Subsets: relates to:[Identifiable Entity](#)

The endurant entity for which the subject state is a snapshot.

 has state : [State](#) [*] Subsets: relates to:[Identifiable Entity](#)

A states (or snapshots) of an entity within its lifetime.

9.33 Threat-risk-conceptual-model::Generic Concept Library::Social Agents

Actor relationships augment the concept of an actor with concepts of identifiers and associations between actors, including organization membership. See also the base actor class.

9.33.1 Diagram: Social Agent

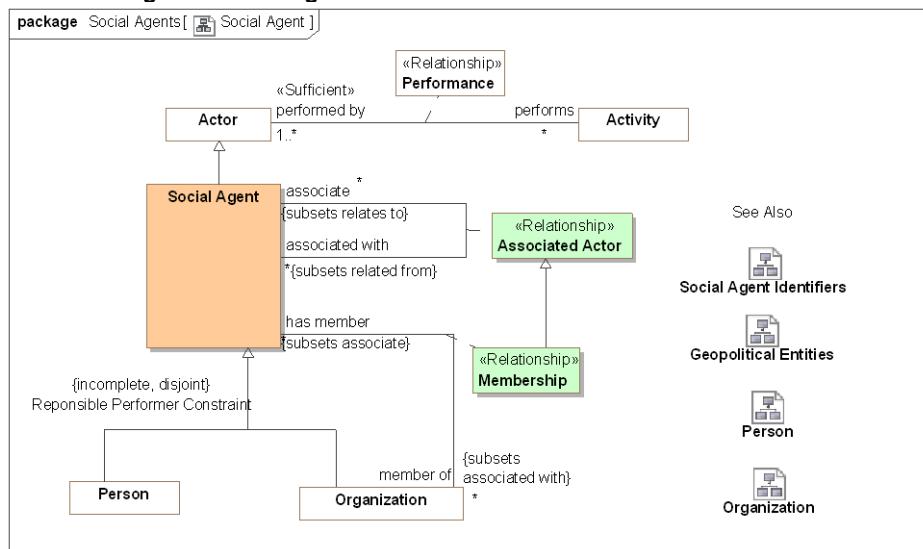


Figure 164. Social Agent

Actor associations define the concept of an organization and provide a general framework for associations between actors with the use of an Actor Association.

9.33.2 Diagram: Social Agent Identifiers

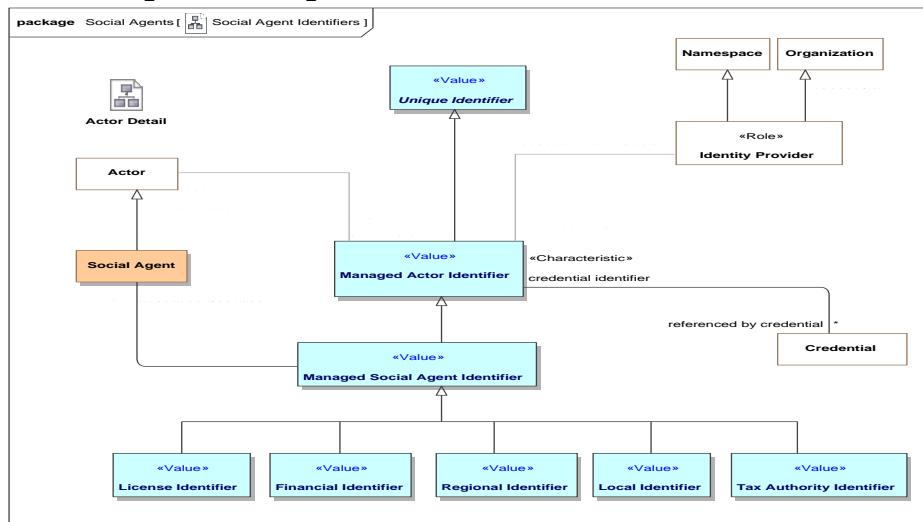


Figure 165. Social Agent Identifiers

9.33.3 Association Class Associated Actor <<Relationship>>

An associated actor relationship defines a connection between an actor and some other actor they are associated with in some way. Subtypes of actor association provide additional semantics about the association. As an association class, Actor Associations may have properties and other relationships. Actor associations will typically have a timeframe.

[NIEM] PersonOrganizationAssociationType (More specific concept)
[NIEM] PersonPersonAssociationType (More specific concept)

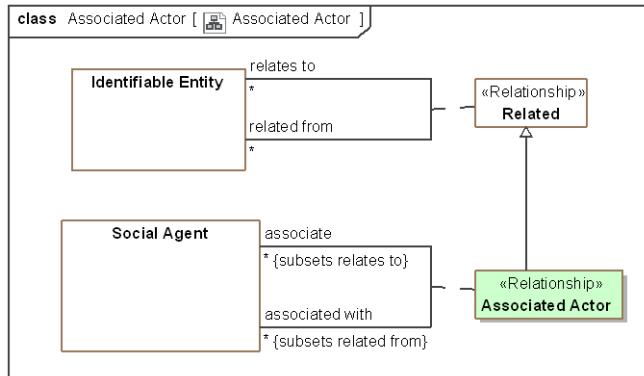


Figure 166. Associated Actor

Direct Supertypes

[Related](#)

Association Ends

associate : [Social Agent](#) [*] Subsets: relates to:[Identifiable Entity](#)

The actor associated with another.

associated with : [Social Agent](#) [*] Subsets: relates to:[Identifiable Entity](#)

Another actor the subject actor is associated with.

9.33.4 Class License Identifier <>Value>>

[NIEM] An identification that references a license certification or registration of a person or organization for some purpose.

Direct Supertypes

[Managed Social Agent Identifier](#)

9.33.5 Class Local Identifier <>Value>>

An identification assigned at a local level (within an organization or community) to a person or organization.

Direct Supertypes

[Managed Social Agent Identifier](#)

9.33.6 Class Managed Social Agent Identifier <>Value>>

An identifier for a social agent where the identifier is managed by some authority.

Direct Supertypes

[Managed Actor Identifier](#)

Associations

/ : [Social Agent](#) [1] Redefines: identifies:[Identifiable Entity](#)

9.33.7 Class Regional Identifier <>Value>>

[NIEM] An identification of a person based on a regional ID.

Direct Supertypes

[Managed Social Agent Identifier](#)

9.33.8 Class Social Agent

An actor that may have responsibilities - people and organizations. Actors in general may include automated entities and even, in some context, animals. Responsible performer excludes these other kinds of actors by including (at this time) only people and organizations.

What responsibilities a particular person or organization may have at any particular time is the subject of law and social constructs. A social agent is distinguished in that a person or organization may have such responsibilities in their lifetime.

[NIEM] EntityType

[DOLCE] Social Agent

Direct Supertypes

[Actor](#)

Associations

 : [Policy](#) [*] Subsets: constrained by:[Rule](#)

 associate : [Policy](#) [*] Subsets: constrained by:[Rule](#)
through association: [Associated Actor](#)

The actor associated with another.

 associated with : [Policy](#) [*] Subsets: constrained by:[Rule](#)
through association: [Associated Actor](#)

Another actor the subject actor is associated with.

 : [Managed Social Agent Identifier](#)
 member of : [Organization](#) [*] Subsets: associated with:[Social Agent](#)
through association: [Membership](#)

Organization a performer belongs to.

[FIBO] memberOf

9.33.9 Class Tax Authority Identifier <>Value>>

An identifier assigned to a person or organization by a tax authority.

Direct Supertypes

[Managed Social Agent Identifier](#)

9.34 Threat-risk-conceptual-model::Generic Concept Library::Systems

A system is a collection of parts and relationships among these parts that may be organized to accomplish some purpose.

The term ‘system’ can refer to an information processing system but it is also applied more generally. Thus a system may include anything: a system of hardware, software, an enterprise, a federation of enterprises, a business process, some combination of parts of different systems, a federation of systems - each under separate control, a program in a computer, a system of programs, a single computer, a system of computers, a computer or system of computers embedded in some machine, etc.

One of the key strengths of modeling, and one that distinguishes it from implementation technologies like software source code, is that it is an excellent way to represent, understand, and specify systems. [OMG MDA Guide]

9.34.1 Diagram: System

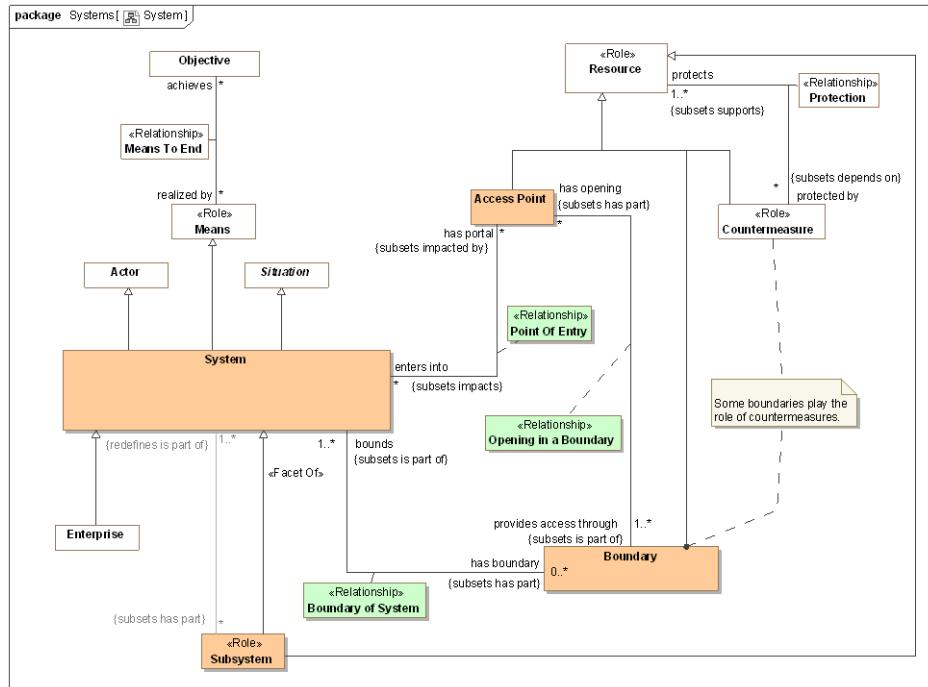


Figure 167. System

9.34.2 Class Access Point

A point of entry into or out of a system such as a door, gate, port, or "interface" into an information system.

Direct Supertypes

[Resource](#)

Associations

█ provides access through : [Boundary](#) [1..*] Subsets: is part of:[Identifiable Entity](#)
through association: [Opening in a Boundary](#)

Boundary through which an entry point provides access. e.g., the wall a door goes through.

█ enters into : [System](#) [*] Subsets: impacts:[Identifiable Entity](#)
through association: [Point Of Entry](#)

System into which an entry point provides access. E.G. A room a door enters into.

↙ traversed using : [Entry Action](#) Subsets: affected by:[Situation](#)

Action that utilizes an access point for passing through a boundary. Such a traversal can be physical or virtual.

↙ Exit via : [Exit Action](#) Subsets: traversed using:[Entry Action](#)

9.34.3 Class Boundary

Something on the edge of a system that serves to contain or protect components of that system.
Some boundaries protect resources of the system/enterprise and may also be countermeasures.
e.g., Fences, firewalls, skin.

Direct Supertypes

[Resource](#)

Associations

█ bounds : [System](#) [1..*] Subsets: is part of:[Identifiable Entity](#)
through association: [Boundary of System](#)

System for which a boundary is an edge.

█ has opening : [Access Point](#) [*] Subsets: has part:[Identifiable Entity](#)
through association: [Opening in a Boundary](#)

A physical or virtual place where access to a system may be provided through a boundary.

9.34.4 Association Class Boundary of System <>Relationship>>

An "edge" of a system affording some level of protection or containment for the system.

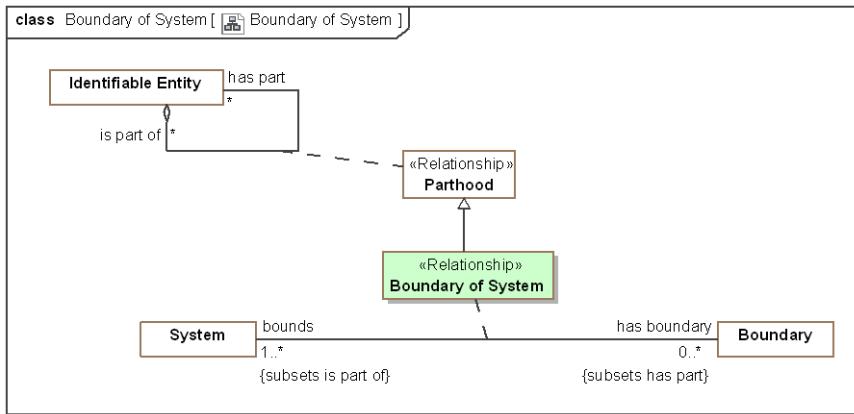


Figure 168. Boundary of System

Direct Supertypes

Parthood

Association Ends

 has boundary : `Boundary` [0..*] Subsets: has part: `Identifiable Entity`

Logical or physical border of a system (or enterprise) that may serve to define, contain or protect the system.

 bounds : `System` [1..*] Subsets: has part: `Identifiable Entity`

System for which a boundary is an edge.

9.34.5 Association Class Opening in a Boundary <<Relationship>>

An access point that provides an opening for passage through a boundary. An opening has the potential to cause a point of entry and a vulnerability.

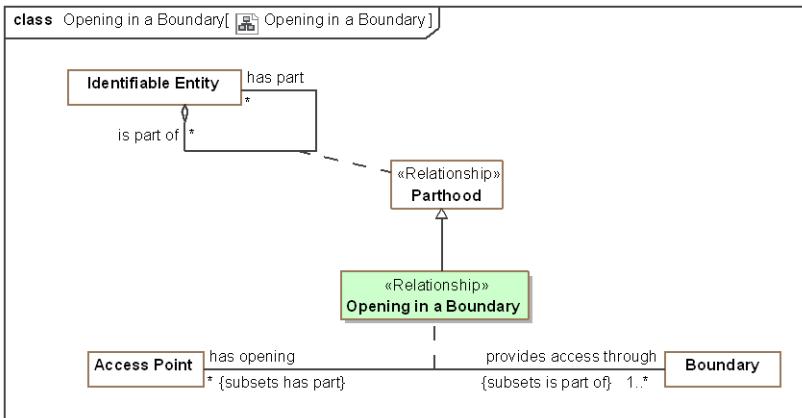


Figure 169. Opening in a Boundary

Direct Supertypes

[Parthood](#)

Association Ends

provides access through : [Boundary](#) [1..*] Subsets: has part:[Identifiable Entity](#)

Boundary through which an entry point provides access. e.g., the wall a door goes through.

has opening : [Access Point](#) [*] Subsets: has part:[Identifiable Entity](#)

A physical or virtual place where access to a system may be provided through a boundary.

9.34.6 Association Class Point Of Entry <<Relationship>>

Relationship between a system and a usable entry point into or out of that system. A point of entry has the potential to cause a vulnerability.

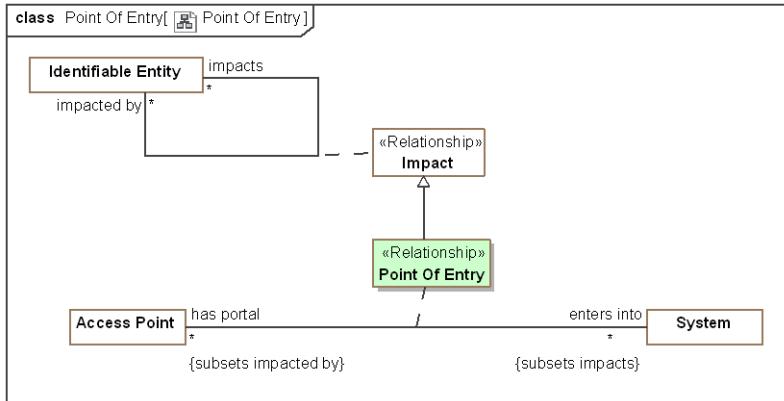


Figure 170. Point Of Entry

Direct Supertypes

[Impact](#)

Association Ends

enters into : [System](#) [*] Subsets: has part: [Identifiable Entity](#)

System into which an entry point provides access. E.G. A room a door enters into.

has portal : [Access Point](#) [*] Subsets: has part: [Identifiable Entity](#)

A point of possible entry into a system.

9.34.7 Class Subsystem <>Role>>

A role of a system as a part of another system as a resource to the owning system.

Direct Supertypes

[Resource](#), [System](#)

Associations

<>Restriction>> : [System](#) [1..*] Redefines: is part of: [Identifiable Entity](#)

9.34.8 Class System

[OMG MDA Guide] A system is a collection of parts and relationships among these parts that may be organized to accomplish some purpose.

[UAF] An integrated set of elements, subsystems, or assemblies that accomplish a defined objective. These elements include products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other

support elements .

A system is a situation in that it has constituent parts working together for a finite period.
A system is a means in that it may achieve objectives for stakeholders.

Direct Supertypes

[Actor](#), [Means](#), [Situation](#)

Associations

 has boundary : [Boundary](#) [0..*] Subsets: has part:[Identifiable Entity](#)

through association: [Boundary of System](#)

Logical or physical border of a system (or enterprise) that may serve to define, contain or protect the system.

 has portal : [Access Point](#) [*] Subsets: impacted by:[Identifiable Entity](#)

through association: [Point Of Entry](#)

A point of possible entry into a system.

 <>Restriction>> : [Subsystem](#) [*] Subsets: has part:[Identifiable Entity](#)

9.35 Threat-risk-conceptual-model::Generic Concept Library::Time & Temporal Entities

The Time package defines the essential concepts of time and the identification of time intervals.

These time concepts are based on the OMG Date Time Vocabulary [DTV] standard but subsets and simplifies DTV for use in defining, federating and exchanging time aspects of entities.

"Temporal Entity" is introduced as an abstraction to capture the common relationships between time elements. Within DTV these relationships are separate for each kind of time element. The relationships defined for Temporal Entity are grounded in DTV Time Interval as each temporal entity exists for a time interval.

Applications that need to reason about time are encouraged to utilize the full DTV semantics. DTV also contains text that more fully elaborates time concepts.

9.35.1 Diagram: Time

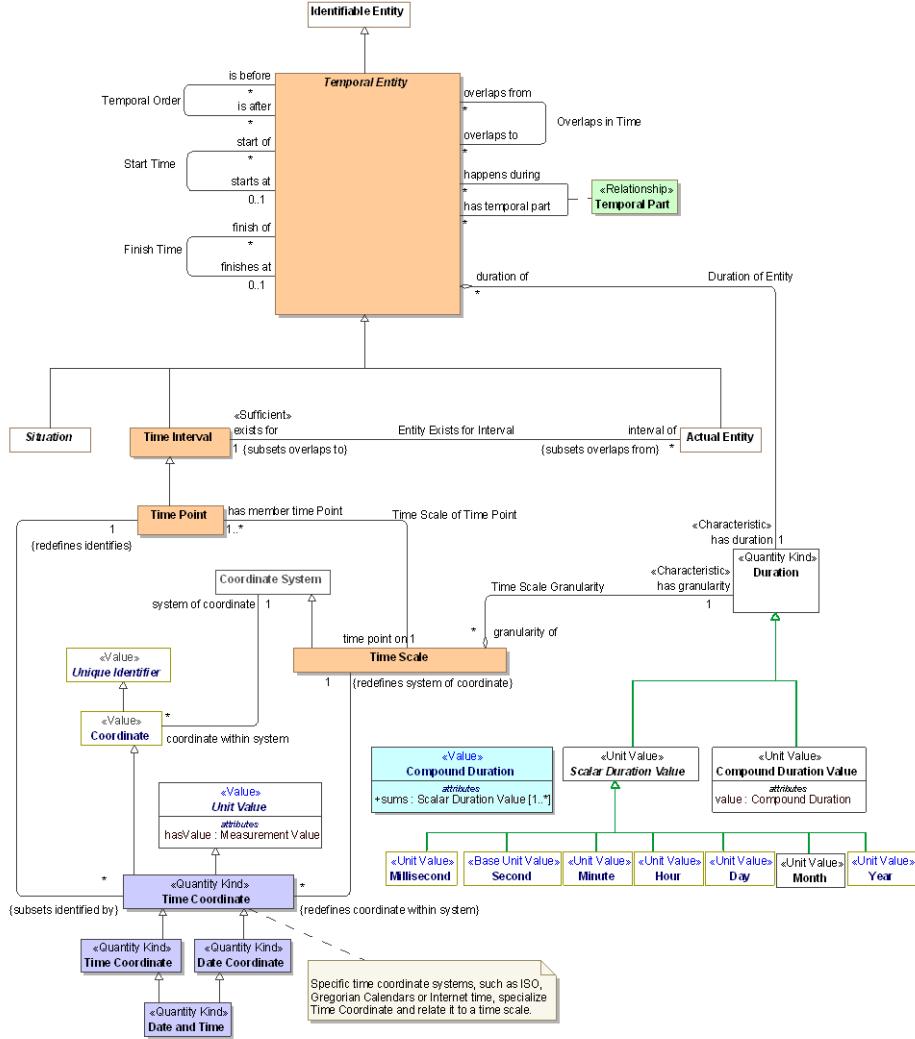


Figure 171. Time

9.35.2 Class Date and Time <<Quantity Kind>>

[FIBO] DateTimeStamp: A DateTimeStamp combines a Date, a time, and a time

Direct Supertypes

[Date Coordinate](#), [Time Coordinate](#)

9.35.3 Class Date Coordinate <<Quantity Kind>>

[FIBO] Date: A Date identifies a calendar day on some calendar.

[NIEM] DateType

Direct Supertypes

[Time Coordinate](#)

9.35.4 Association Duration of Entity

[DTV] time interval [of temporal entity] has particular duration:the particular duration is the duration that is the amount of time in the time interval.

Each time interval [Temporal Entity] has a unique duration attribute that is a measure of its size, i.e., the amount of time the time interval occupies. This attribute is mathematically a function that maps time intervals into durations. This mapping function is sometimes called the “range” of a time interval, and some times called the “measure” of a time interval.

Association Ends

duration of : [Temporal Entity](#) [*] Subsets: has part:[Identifiable Entity](#)

Temporal entity for which a duration is applicable.

has duration : [Duration](#) [1] Subsets: has part:[Identifiable Entity](#)

Difference between the start and end time. A non-zero positive value representing the amount of time a temporal entity exists.

[DTV] time interval [of temporal entity] has particular duration:the particular duration is the duration that is the amount of time in the time interval.

Each time interval [Temporal Entity] has a unique duration attribute that is a measure of its size, i.e., the amount of time the time interval occupies. This attribute is mathematically a function that maps time intervals into durations. This mapping function is sometimes called the “range” of a time interval, and some times called the “measure” of a time interval.

9.35.5 Association Entity Exists for Interval

Relationship defining the time interval in which an entity actually exists.

[DTV] occurrence occurs for occurrence interval: the occurrence occurs throughout the occurrence interval and the occurrence does not occur within some time interval2 that meets the occurrence interval and the occurrence does not occur within some time interval3 that is met by the occurrence interval

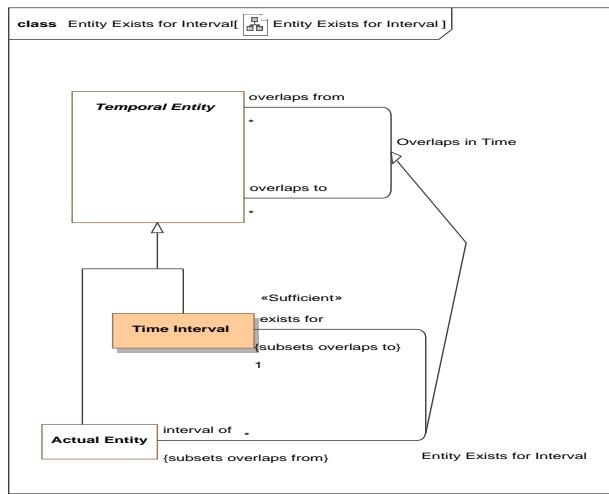


Figure 172. Entity Exists for Interval

Direct Supertypes

Overlaps in Time

Association Ends

/ exists for : [Time Interval](#) [1] Subsets: has part:[Identifiable Entity](#)

Time interval where an entity may be considered "actual", that is existent in the domain of discourse.

/ interval of : [Actual Entity](#) [*] Subsets: has part:[Identifiable Entity](#)

Entity existent for the full extent of a time interval.

9.35.6 Association Finish Time

The time something no longer exists (inclusive).

[DTV] time interval1 finishes time interval2

Synonymous Form:time interval2 is finished by time interval1

Definition:time interval1 is a proper part of time interval2 and there exists no time interval3 that is a proper part of time

interval2 and that is after time interval1

[IDEAS] endBoundary: A temporalBoundary where the boundary is an end boundary of the whole.

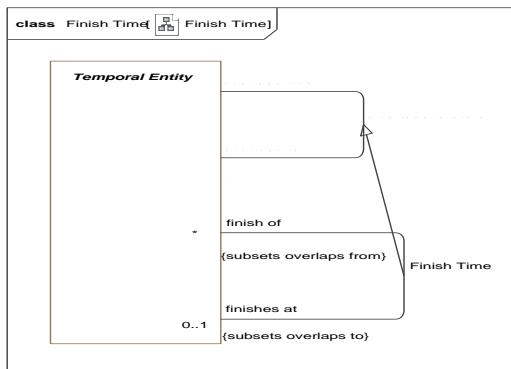


Figure 173. Finish Time

Direct Supertypes

Overlaps in Time

Association Ends

/ finish of : [Temporal Entity](#) [*] Subsets: has part:[Identifiable Entity](#)

Thing which no longer exists at a particular time.

/ finishes at : [Temporal Entity](#) [0..1] Subsets: has part:[Identifiable Entity](#)

Time something no longer exists. (Inclusive)

9.35.7 Association Overlaps in Time

Some or all parts of the related temporal entities exist at the same time. Note that "to" and "from" may be arbitrary. By convention, the containing or prior temporal entity is "from".

[DTV] time interval1 properly overlaps time interval2

An [ISO 1087] temporal relation: sequential relation (3.2.24) involving events in time

[DOLCE] (subtype of) Temporal Quality

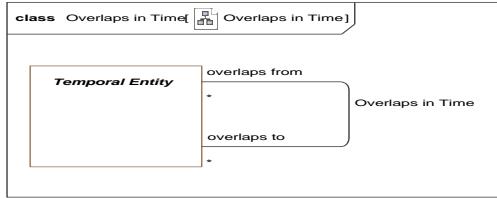


Figure 174. Overlaps in Time

Association Ends

/ overlaps from : [Temporal Entity](#) [*] Subsets: has part:[Identifiable Entity](#)

An overlapping temporal component.

/ overlaps to : [Temporal Entity](#) [*] Subsets: has part:[Identifiable Entity](#)

An overlapping temporal component.

9.35.8 Association Start Time

The time something starts to exist (inclusive).

[DTV] time interval1 starts time interval2

Synonymous Form: time interval2 is started by time interval1

Definition: time interval1 is a proper part of time interval2 and there exists no time interval3 that is a proper part of time interval2 and that is before time interval1.

[IDEAS] startBoundary: A temporalBoundary where the boundary is a start boundary of the whole.

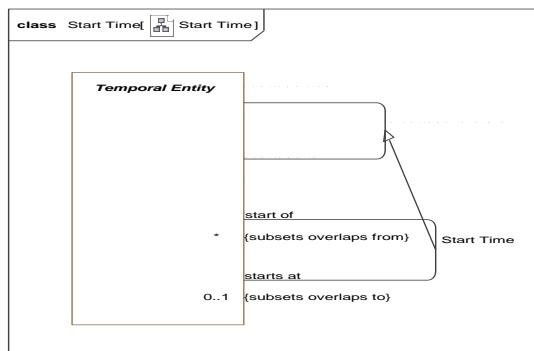


Figure 175. Start Time

Direct Supertypes

[Overlaps in Time](#)

Association Ends

- / start of : [Temporal Entity](#) [*] Subsets: has part:[Identifiable Entity](#)

Thing which begins to exist at a particular time.

- / starts at : [Temporal Entity](#) [0..1] Subsets: has part:[Identifiable Entity](#)

Time something begins to exist. (inclusive).
[FIBO] hasStartDate

9.35.9 Association Temporal Order

A relationship representing ordering of temporal entities in time where the <starts at> of <is after> is greater than or equal to the <finishes at> of <is before>. Related things do not overlap in time.

[DOLCE] (subtype of) Temporal Quality

[DTV] "time interval1 is properly before time interval2": the time interval1 is before the time interval2 and the time interval1 is before a time interval3 and the time interval3 is before the time interval2

[DTV] time interval1 finishes duration after time interval2: The end of one time interval is duration after the end of the other time interval.

[IDEAS] beforeAfter: A couple that asserts one Individual's temporal extent is completely before the temporal extent of another.

An [ISO 1087] temporal relation: sequential relation (3.2.24) involving events in time

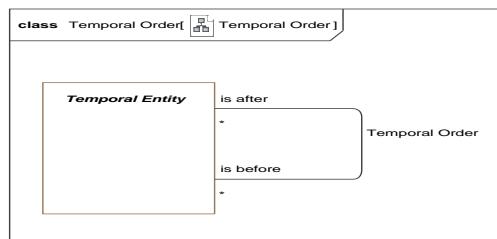


Figure 176. Temporal Order

Association Ends

- / is after : [Temporal Entity](#) [*] Subsets: has part:[Identifiable Entity](#)

A temporal entity that starts after the <is before> entity ends.

- / is before : [Temporal Entity](#) [*] Subsets: has part:[Identifiable Entity](#)

A temporal entity that ends after the <is after> entity starts.

9.35.10 Association Class Temporal Part <>Relationship>>

The time interval of <has temporal part> is within the time interval of <happens during>.

[DTV] time interval1 is proper part of time interval2: the time interval1 is a proper part of the time interval2 and a time interval3 is a proper part of the time interval2 and a time interval4 is a proper part of the time interval2 and the time interval3 is before the time interval1 and the time interval1 is before the time interval4.

[IDAS] temporalWholePart: A wholePart that asserts the spatial extent of the (whole) individual is co-extensive with the spatial extent of the (part) individual for a particular period of time.

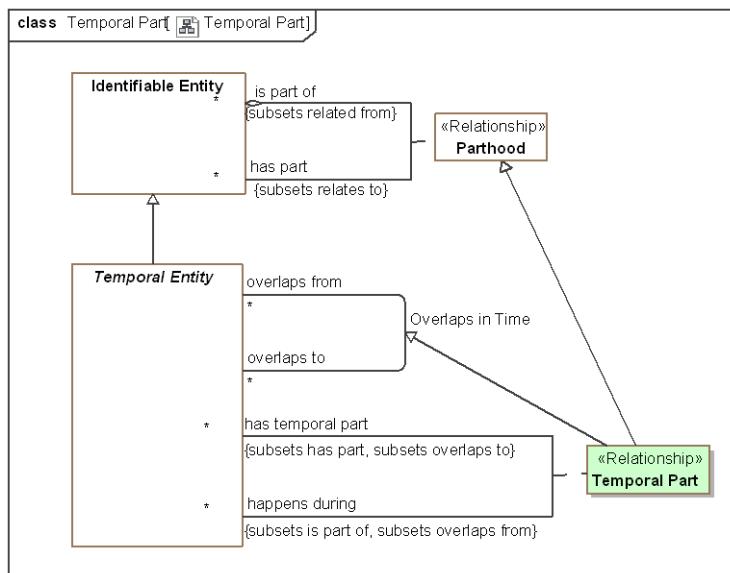


Figure 177. Temporal Part

Direct Supertypes

[Overlaps in Time](#), [Parthood](#)

Association Ends

happens during : [Temporal Entity](#) [*] Subsets: has part:[Identifiable Entity](#)

A situation with overlapping duration (overlapping temporal extent).

has temporal part : [Temporal Entity](#) [*] Subsets: has part:[Identifiable Entity](#)

Sub-durations of anything that happen - a temporal part.

9.35.11 Class Time Coordinate <>Quantity Kind>>

A designation of a particular time.

Direct Supertypes

[Time Coordinate](#)

9.35.12 Class Time Interval

A segment of time.

[DTV] "time interval" : segment of the time axis, a location in time.

Note: Every time interval has a beginning, an end, and a duration, even if not known. Every time interval is "finite", a bounded segment of the Time Axis. The beginning or end of a time interval may be defined by reference to events that occur for a time interval that is not known.

Note: Time intervals may be 'indefinite', meaning that their beginning is 'primordiality' or their end is 'perpetuity', or both ('eternity'). This vocabulary assumes that indefinite time intervals exist and have some duration, but their duration is unknown.

[IDEAS] PeriodOrInstant: An Individual whose spatial extent is infinite, but whose temporal extent is finite or zero.

[UML] TimeInterval

[NIEM] DateRangeType

[DOLCE] Temporal Region

Direct Supertypes

[Temporal Entity](#)

Associations

 : [Incident](#) [*]

 timeframe for : [Credential](#) [0..*] Subsets: interval of: [Actual Entity](#)

through association: [Valid for Time Interval](#)

Credential that is validated within the <valid for time> interval.

 interval of : [Actual Entity](#) [*] Subsets: overlaps from: [Temporal Entity](#)

through association: [Entity Exists for Interval](#)

Entity existent for the full extent of a time interval.

9.35.13 Class Time Point

A portion of time deemed atomic on a time scale. As all points in time may be further subdivided into a finer granularity of time, each point in time is also a time interval on some other scale.

The duration of a time point is the same as the granularity of the time scale of the time point.

[DTV] time point: concept that specializes the concept 'time interval' and that is a member of a time scale.

[IDEAS] CalendarPeriod: A Period that corresponds to a recognized date or time.

Direct Supertypes

[Time Interval](#)

Associations

- / : [Time Coordinate](#) [*] Subsets: identified by: [Identifier](#)
- / time point on : [Time Scale](#) [1]
through association: [Time Scale of Time Point](#)

Time scale used for defining a time point.

[DTV] time scale has time point:

9.35.14 Class Time Scale

A time scale is a way to reckon time as a series of consecutive time points identified by time coordinates. e.g. Time scale defined by the Gregorian calendar.

[DTV] time scale: regular sequence that each member of the regular sequence is a time point

Direct Supertypes

[Coordinate System](#)

Associations

- / : [Time Coordinate](#) [*] Redefines: coordinate within system: [Coordinate](#)
- / has granularity : [Duration](#) [1]
through association: [Time Scale Granularity](#)

[DTV] the smallest duration that can be distinguished with a given time scale

- / has member time Point : [Time Point](#) [1..*]
through association: [Time Scale of Time Point](#)

Time point defined within a time scale

9.35.15 Association Time Scale Granularity

[DTV] Time scale has granularity: The granularity of the time scale is the duration of the time points of the time scale.

Association Ends

- / has granularity : [Duration](#) [1]

[DTV] the smallest duration that can be distinguished with a given time scale

✓ granularity of : [Time Scale](#) [*]

Duration of each time point on a time scale.

9.35.16 Association Time Scale of Time Point

Relationship defining the time scale on which a time point is defined. e.g. December 7th, 1944 is defined on a Gregorian Calendar time scale.

Association Ends

✓ time point on : [Time Scale](#) [1]

Time scale used for defining a time point.

[DTV] time scale has time point:

✓ has member time Point : [Time Point](#) [1..*]

Time point defined within a time scale

9.36 Threat-risk-conceptual-model::Generic Concept Library::Time & Temporal Entities::ISO Time Scale

9.36.1 Diagram: ISO Time

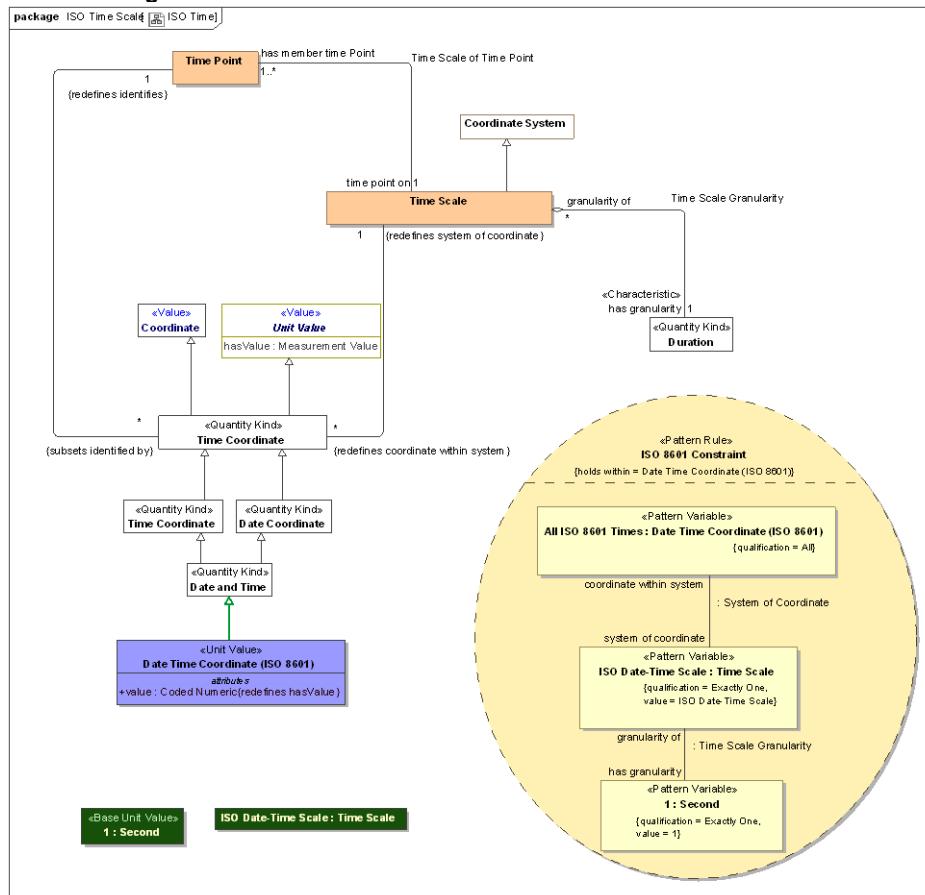


Figure 178. ISO Time

9.36.2 Class Date Time Coordinate (ISO 8601) <>Unit Value>>

[UAF] A date and time specified in the ISO8601 date-time format including timezone designator (TZD): YYYY-MM-DDThh:mm:ssTZD.

Direct Supertypes

[Date and Time](#)

Attributes

◊ value : [Coded Numeric](#)

A text string representing a date and time specified in the ISO8601 date-time format including timezone designator (TZD): YYYY-MM-DDThh:mm:ssTZD.

9.37 Threat-risk-conceptual-model::Generic Concept Library::Time & Temporal Entities::XSD Time Scale

XSD Representations of date and time

9.37.1 Diagram: XSD Time Scale

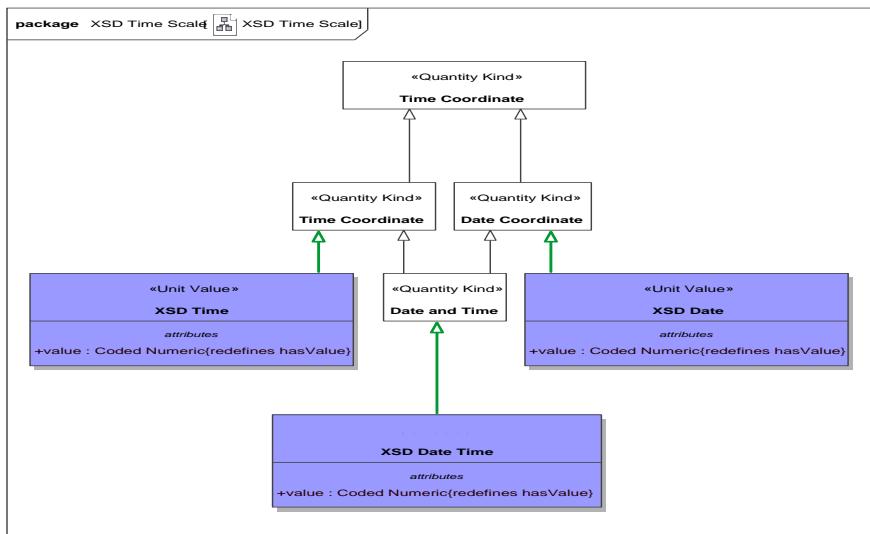


Figure 179. XSD Time Scale

9.37.2 Class XSD Date <<Unit Value>>

An XSD representation of a date
[OWL] xsd:date.

Direct Supertypes

[Date Coordinate](#)

Attributes

◊ value : [Coded Numeric](#)

A text string representing a date and time specified in the ISO8601 date-time format including timezone designator (TZD): YYYY-MM-DDThh:mm:ssTZD.

9.37.3 Class XSD Date Time <>Unit Value>>

An XSD representation of a date and time
[OWL] xsd:dateTime

Direct Supertypes

[Date and Time](#)

Attributes

◊ value : [Coded Numeric](#)

A text string representing a date and time specified in the ISO8601 date-time format including timezone designator (TZD): YYYY-MM-DDThh:mm:ssTZD.

9.37.4 Class XSD Time <>Unit Value>>

An XSD representation of a time
[OWL] xsd:time

Direct Supertypes

[Time Coordinate](#)

Attributes

◊ value : [Coded Numeric](#)

A text string representing a date and time specified in the ISO8601 date-time format including timezone designator (TZD): YYYY-MM-DDThh:mm:ssTZD.

9.38 Threat-risk-conceptual-model::Generic Concept Library::Vendors and Producers

Concepts relating to manufacturers and manufactured things.

9.38.1 Diagram: Vendors and Producers

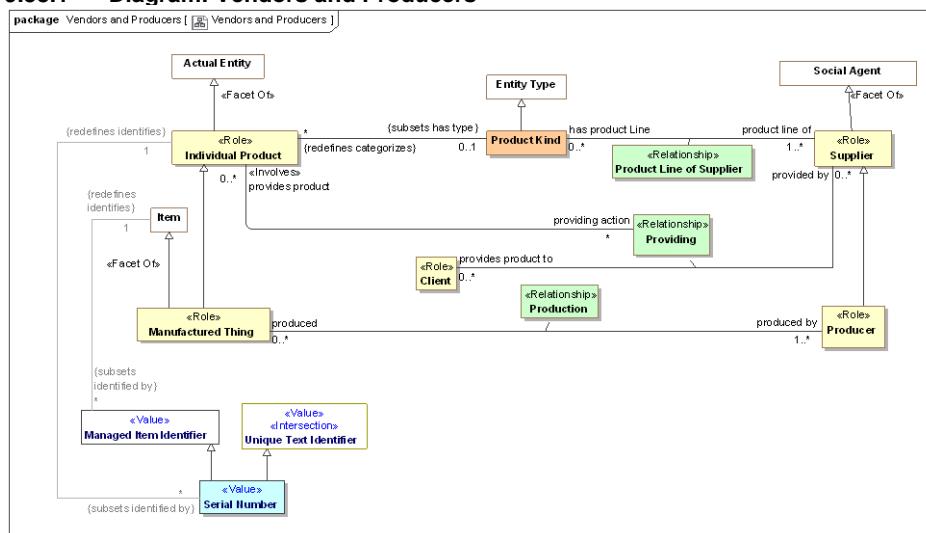


Figure 180. Vendors and Producers

9.38.2 Class Client <>Role>>

The role of a responsible performer receiving goods or services from a provider.

[FIBO] Client: a party that acquires, or agrees to acquire, ownership (in case of goods), or benefit or usage (in case of services), in exchange for money or other consideration under a contract of sale

Associations

- █ provided by : [Supplier](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)
- through association: [Providing](#)

Supplier of a product or service.
[FIBO] isSuppliedBy

9.38.3 Class Individual Product <<Role>>

A specific item or service purchased, sold or offered for sale.

[FIBO] Product: A commercially distributed good that is (1) tangible property, (2) the output or result of a fabrication, manufacturing, or production process, or (3) something that passes through a distribution channel before being consumed or used.

Direct Supertypes

[Actual Entity](#)

Associations

- / : [Product Kind](#) [0..1] Subsets: has type:[Type](#)
- / <<Restriction>> : [Serial Number](#) [*] Subsets: identified by:[Identifier](#)
- / providing action : [Providing](#) [*]

The action that provided a product or service to a consumer.

9.38.4 Class Manufactured Thing <<Role>>

Role of a thing as being made or manufactured.

Direct Supertypes

[Individual Product](#), [Item](#)

Attributes

- ◎ revision : [Primitive Value](#)

The revision of a product or good.

Associations

- ≡ produced by : [Producer](#) [1..*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Production](#)

Entity which manufactured or created an item.

9.38.5 Class Producer <<Role>>

Maker of goods or products, usually for sale. Syn: Manufacturer.

[FIBO] Producer: the manufacturer of a product, also called maker.

Direct Supertypes

[Supplier](#)

Associations

☒ produced : [Manufactured Thing](#) [0..*] Subsets: impacts:[Identifiable Entity](#)
through association: [Production](#)

A products or good made by a manufacturer.

9.38.6 Class Product Kind

A set of similar items or services produced by or delivered by suppliers.

Direct Supertypes

[Entity Type](#)

Associations

↙ : [Individual Product](#) [*] Redefines: categorizes:[Thing](#)
☒ product line of : [Supplier](#) [1..*] Subsets: impacted by:[Identifiable Entity](#)
through association: [Product Line of Supplier](#)

Manufacturer of a product line

9.38.7 Association Class Product Line of Supplier <<Relationship>>

A kind of product or service offered by a supplier.

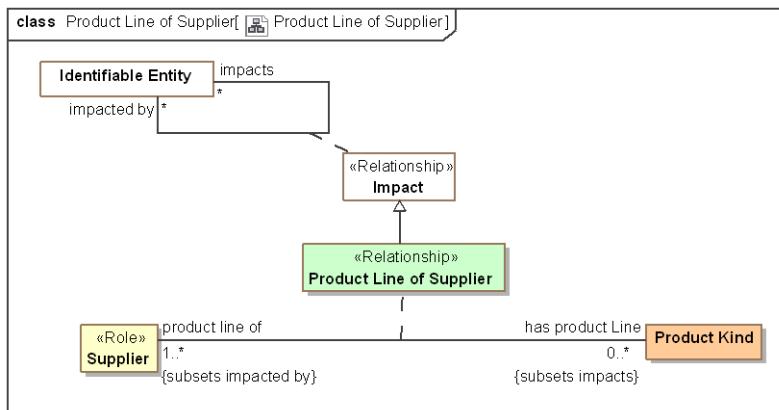


Figure 181. Product Line of Supplier

Direct Supertypes

[Impact](#)

Association Ends

 has product Line : [Product Kind](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)

Product line provided by a manufacturer.

 product line of : [Supplier](#) [1..*] Subsets: impacted by:[Identifiable Entity](#)

Manufacturer of a product line

9.38.8 Association Class Production <<Relationship>>

The making of a <produced> thing <produced by> a producer.

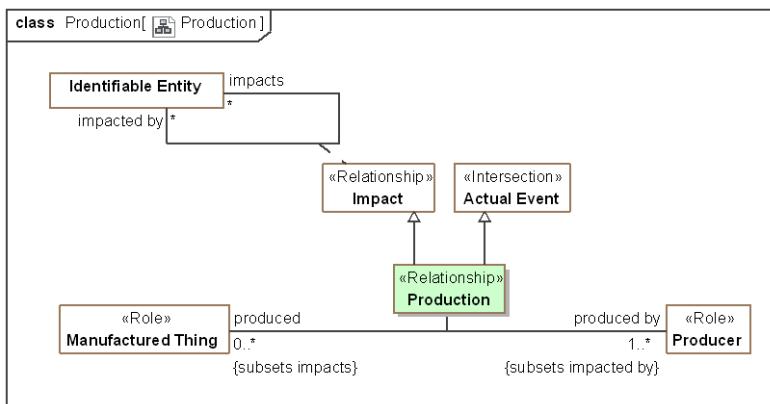


Figure 182. Production

Direct Supertypes

[Actual Event](#), [Impact](#)

Association Ends

 produced by : [Producer](#) [1..*] Subsets: impacted by:[Identifiable Entity](#)

Entity which manufactured or created an item.

 produced : [Manufactured Thing](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)

A products or good made by a manufacturer.

9.38.9 Association Class Providing <<Relationship>>

The providing of a product or service to a consumer.

[FIBO] supplies

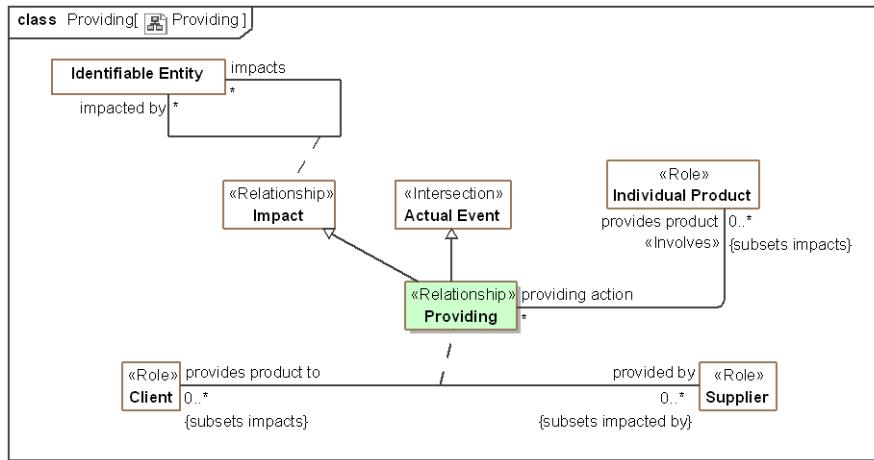


Figure 183. Providing

Direct Supertypes

[Actual Event](#), [Impact](#)

Associations Ends

provided by : [Supplier](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)

Supplier of a product or service.
[FIBO] isSuppliedBy

provides product to : [Client](#) [0..*] Subsets: impacted by:[Identifiable Entity](#)

Consumer who receives a product or service.

Associations

provides product : [Individual Product](#) [0..*] Subsets: impacts:[Identifiable Entity](#)

The products provided to <provides product to> by <provided by>.

9.38.10 Class Serial Number <>Value>>

An identifier of an item provided by its producer or supplier.

Direct Supertypes

[Managed Item Identifier](#), [Unique Text Identifier](#)

Associations

 <>Restriction>> : [Individual Product](#) [1] Redefines: identifies:[Identifiable Entity](#)

9.38.11 Class Supplier <>Role>>

A person or organization that sells products or services.
[FIBO] a party that supplies goods or services

Direct Supertypes

[Social Agent](#)

Associations

 has product Line : [Product Kind](#) [0..*] Subsets: impacts:[Identifiable Entity](#)
through association: [Product Line of Supplier](#)

Product line provided by a manufacturer.

 provides product to : [Client](#) [0..*] Subsets: impacts:[Identifiable Entity](#)
through association: [Providing](#)

Consumer who receives a product or service.

10 STIX Mapping Specification (Normative)

10.1 How STIX is represented

STIX 1.2 is represented as a UML model imported from the STIX XML schema [using an off-the-shelf UML tool and the Eclipse profile for XML schema](#). This model is in the machine readable artifacts as “Stix12.” Mappings are then made between UML models.

10.2 Generic NIEM-STIX Mapping Rules and Conventions

The mapping specification below specifies the semantic relationships between NIEM-STIX and the corresponding conceptual modelconceptual reference model elements. In some cases, these relationships are direct and in other cases indirect, as indicated by the mapping rules. Within the mappings certain assumptions are made with respect to the mapping capability, as follows.

Primitive data types

The detailed mapping and conversion of primitive data types is well defined and implemented by underlying technologies. It is assumed that correct conversions will be made between various representations of strings, numbers, enumerations, dates, and other basic data types. These data types for STIX are specified as XML data types, which are well defined. As such, primitive data mapping is not specified herein.

Quantity values and unit type conversions

In the conceptual modelconceptual reference model quantities are defined in terms of their quantity kinds (e.g., temperature, length, etc.) and appropriate unit types (centigrade, meters, etc.) are expected in any exchange format. The value of properties is stated in terms of these quantity kinds and unit types, not as primitive data, such as “int.” Proper specification of units is critical for correct interpretation of data – quantity kinds should always be utilized in the conceptual modelconceptual reference model. These quantity kinds should be mapped to units in specific data formats.

Each such quantity has a “value” that is a primitive data type, usually a number. Wherever the information is known the mapping specification defines the unit expected of a technology exchange format – thus “age:real” may be mapped to “age:year” if years can be determined to be the unit expected. It is an implementation option to assume units if none are provided or to ignore the underspecified data. If another data format expected “months” as age, the implementation framework should convert between months and years, even if such conversion is an approximation.

The implementation framework is to convert between quantity values and primitive data types based on the mapping specification and externally established conversion factors. It is the responsibility of the mapping implementation to convert between different units for the same quantity kind. Conversion values are not specified in the model so as not to introduce redundant specifications. Implementations are referred to the normative source at NIST for conversion factors and formula: <http://www.nist.gov/pml/wmd/metric/unit-conversion.cfm>.

Some conversions have no normative reference. For example, conversion between a probability percentage for risk and “high, medium, low” risk. Such conversions are implementation defined. Further implementation experience may introduce specific conversions in a later specification.

STIX Relationships

All associations in the ~~conceptual model~~^{conceptual reference model} are considered “first class” situations and may contain dates, context and metadata. STIX reifies certain associations and references to provide this information. These reified relations are not each independently modeled in the mappings. Mappings are expected to comprehend and implement the STX relationship pattern. ~~As part of generic XML mapping, IDs and IDREFS are to be mapped to relationships.~~

10.3 STIX Mapping to the threat/risk conceptual model

10.3.1 Diagram: High Level STIX Mapping

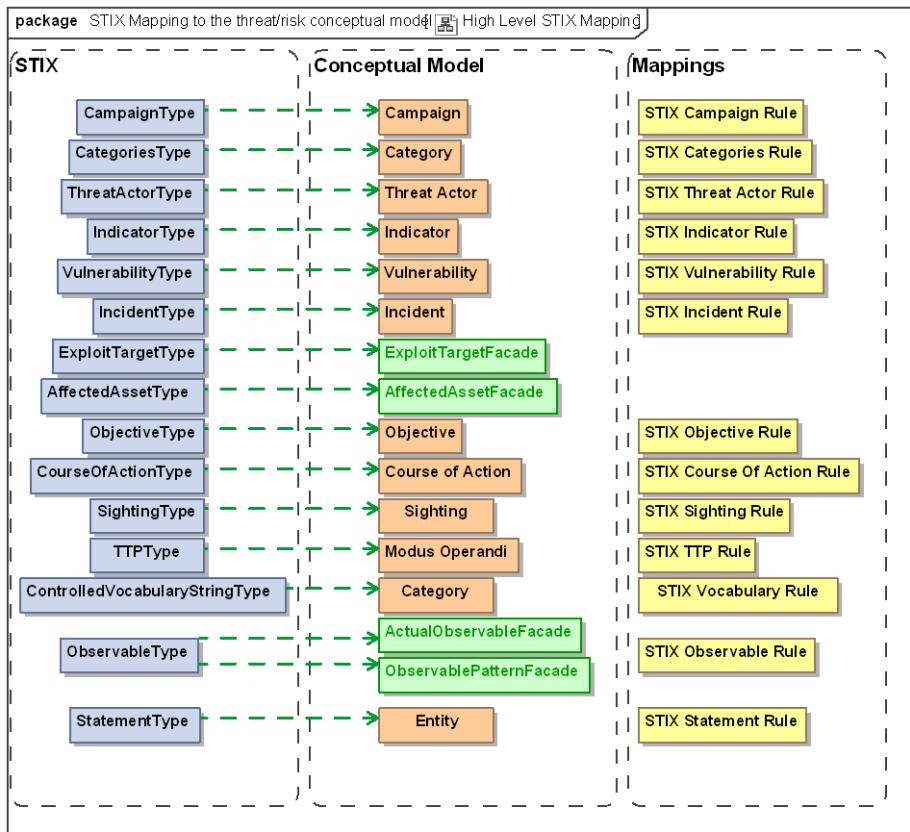


Figure 184. High Level STIX Mapping

10.4 STIX Mapping to the threat/risk conceptual model::Facades

10.4.1 Diagram: Facade Summary

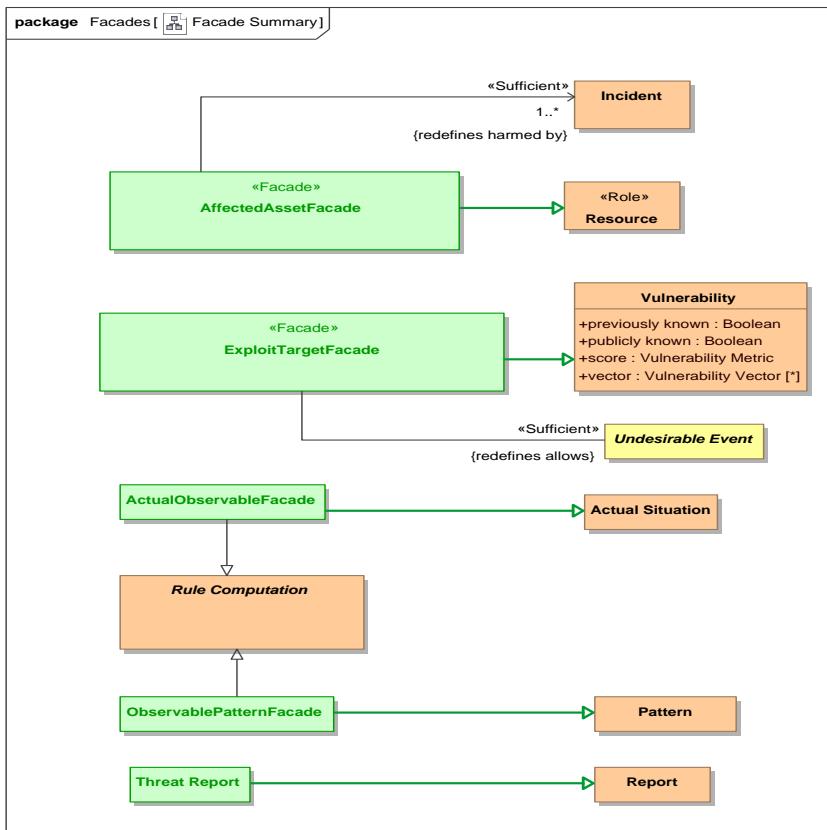


Figure 185. Facade Summary

10.4.2 Class ActualObservableFacade

Computation of an observable from an actual situation. This computation is done by the mapping implementation.

10.4.21 Direct Supertypes

[Actual Situation](#), [Rule Computation](#)

package STIX Mapping to the threat/risk [conceptual model](#)[conceptual reference model](#)::Facades

10.4.3 Class AffectedAssetFacade

10.4.31 Direct Supertypes

[Resource](#)

package STIX Mapping to the threat/risk [conceptual model](#)[conceptual reference model](#)::Facades

10.4.32 Associations

 : [Incident](#) [1..*] *Redefines:* harmed by:[Undesirable Situation](#)

10.4.4 Class ExploitTargetFacade

10.4.41 Direct Supertypes

[Vulnerability](#)

package STIX Mapping to the threat/risk [conceptual model](#)[conceptual reference model](#)::Facades

10.4.42 Associations

 : [Undesirable Event](#) *Redefines:* allows:[Undesirable Event](#)

10.4.5 Class ObservablePatternFacade

Computation of an observable from a situation pattern. This computation is done by the mapping implementation.

10.4.51 Direct Supertypes

[Pattern](#), [Rule Computation](#)

package STIX Mapping to the threat/risk [conceptual model](#)[conceptual reference model](#)::Facades

10.4.6 Class Threat Report

10.4.6.1 Direct Supertypes

[Report](#)

package STIX Mapping to the threat/risk [conceptual model](#)[conceptual reference model](#)::Facades

10.5 STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

10.6 Class STIX Campaign Rule

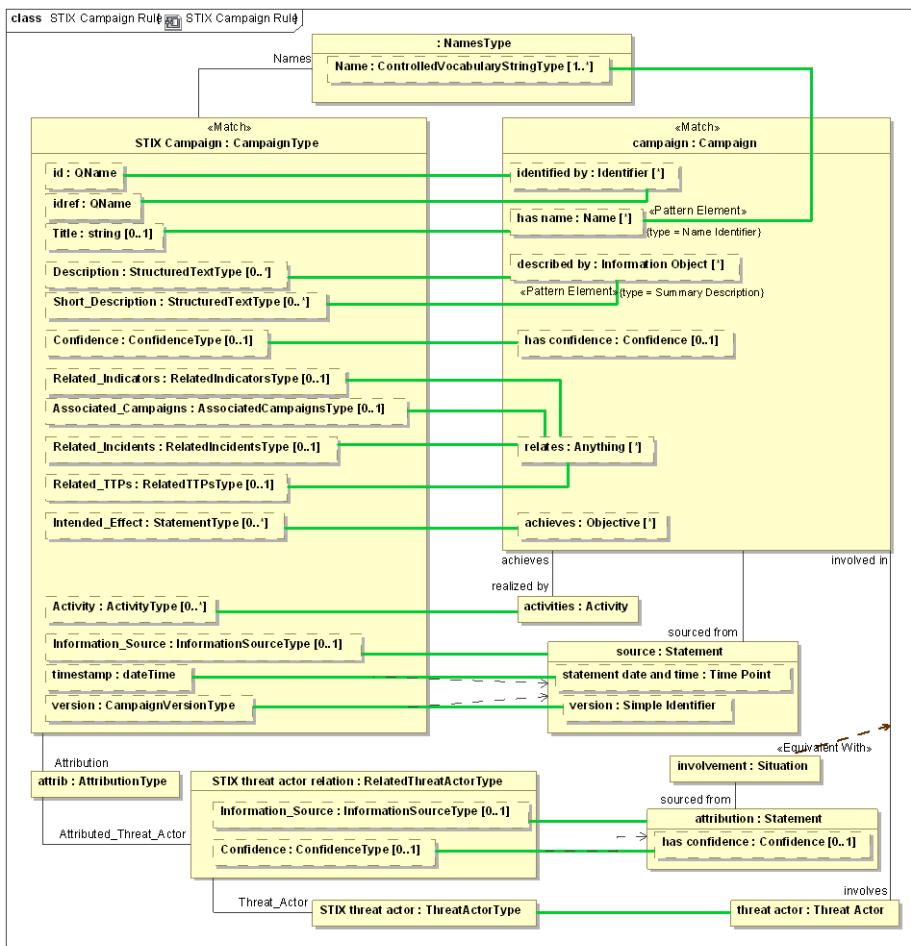


Figure 186. STIX Campaign Rule

package STIX Mapping to the threat/risk conceptual-modelconceptual-reference-model::STIX Mapping Rules

10.7 Class STIX Categories Rule

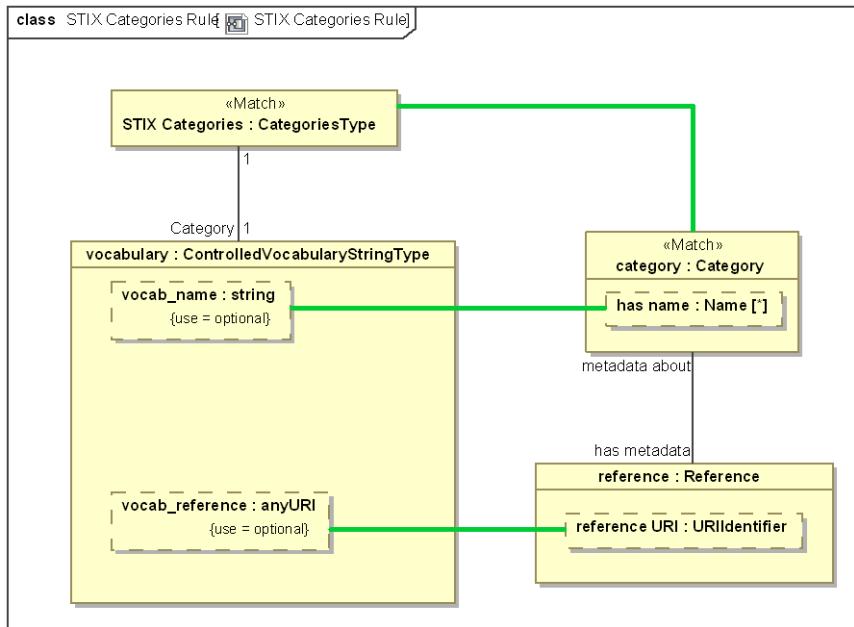


Figure 187. STIX Categories Rule

package STIX Mapping to the threat/risk conceptual-modelconceptual-reference-model::STIX Mapping Rules

10.8 Class STIX Course Of Action Rule

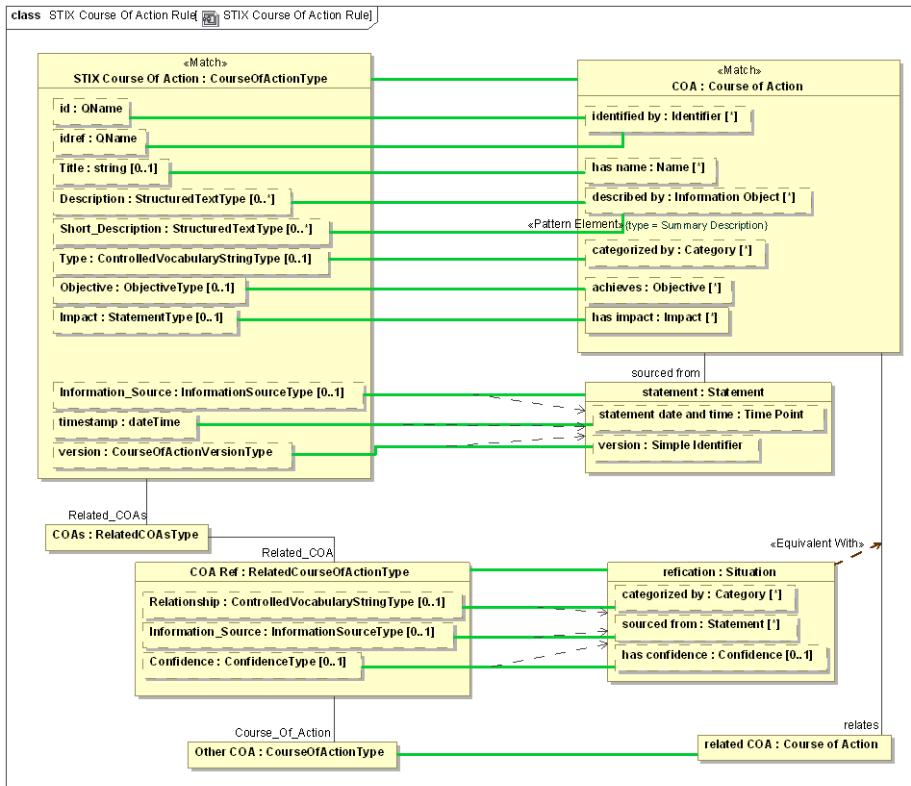


Figure 188. STIX Course Of Action Rule

package STIX Mapping to the threat/risk conceptual modelconceptual reference model::STIX Mapping Rules

10.9 Class STIX Incident Rule

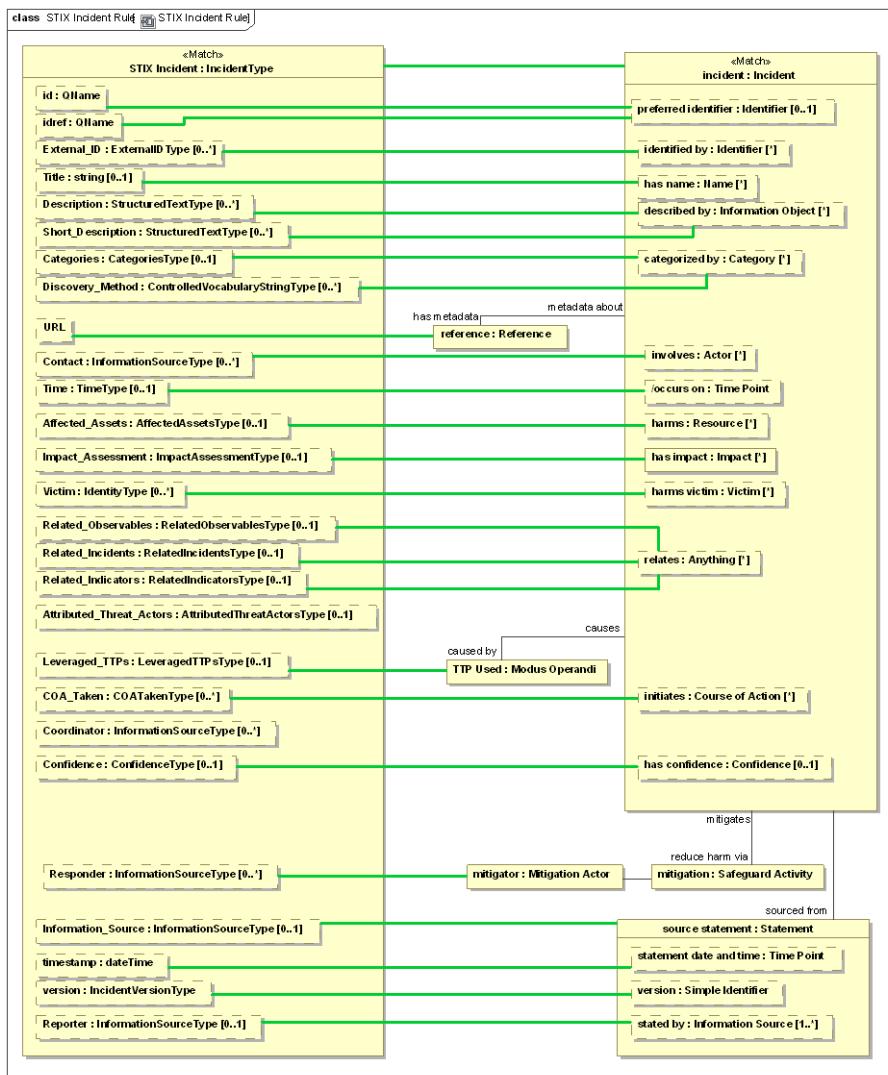


Figure 189. STIX Incident Rule

package STIX Mapping to the threat/risk [conceptual model](#)[conceptual reference model](#)::STIX Mapping Rules

10.10 Class STIX Indicator Rule

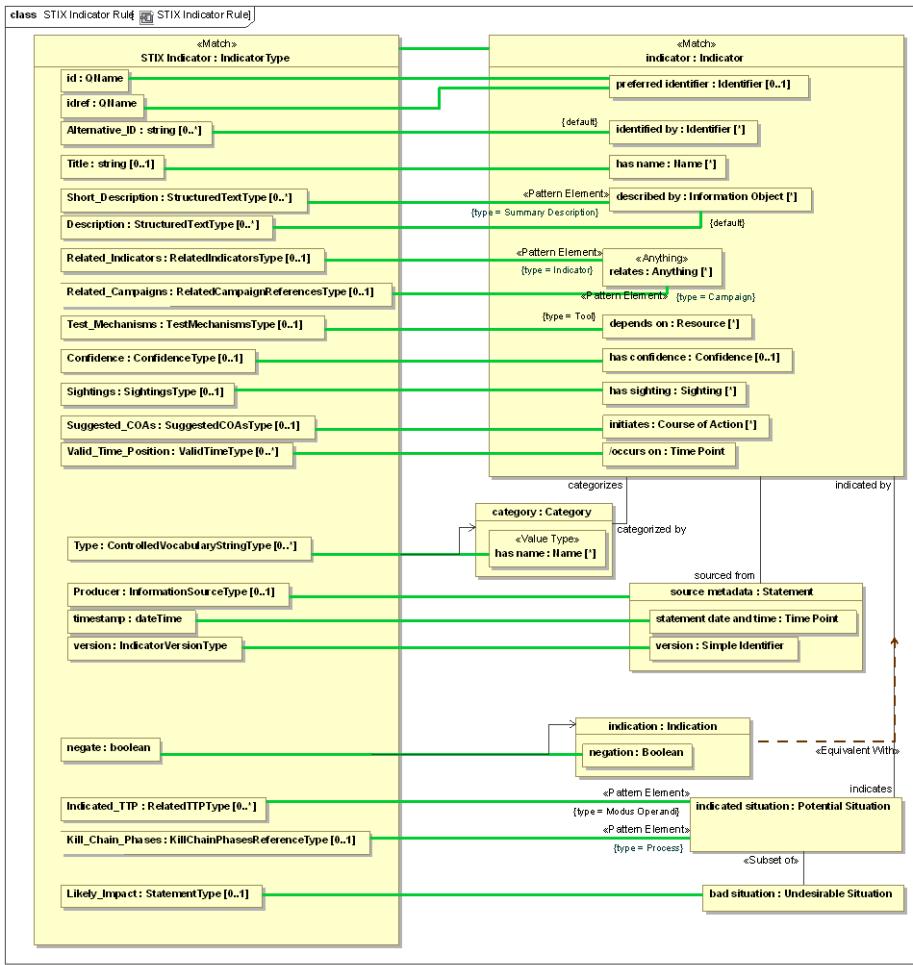


Figure 190. STIX Indicator Rule

package STIX Mapping to the threat/risk [conceptual model](#)[conceptual reference model](#)::STIX Mapping Rules

10.11 Class STIX Objective Rule

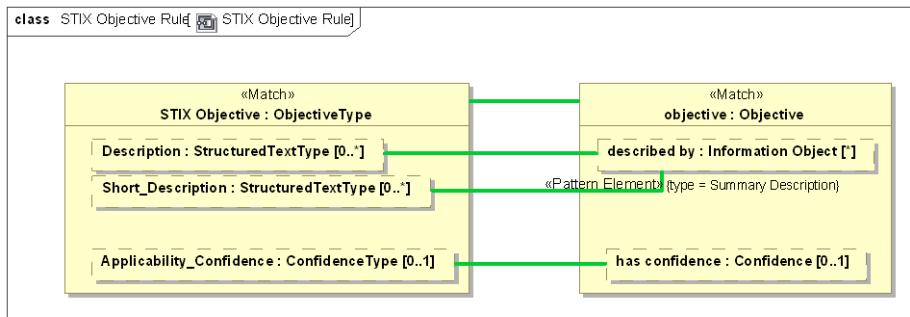


Figure 191. STIX Objective Rule

package STIX Mapping to the threat/risk [conceptual model](#)[conceptual reference model](#)::STIX Mapping Rules

10.12 Class STIX Observable Rule

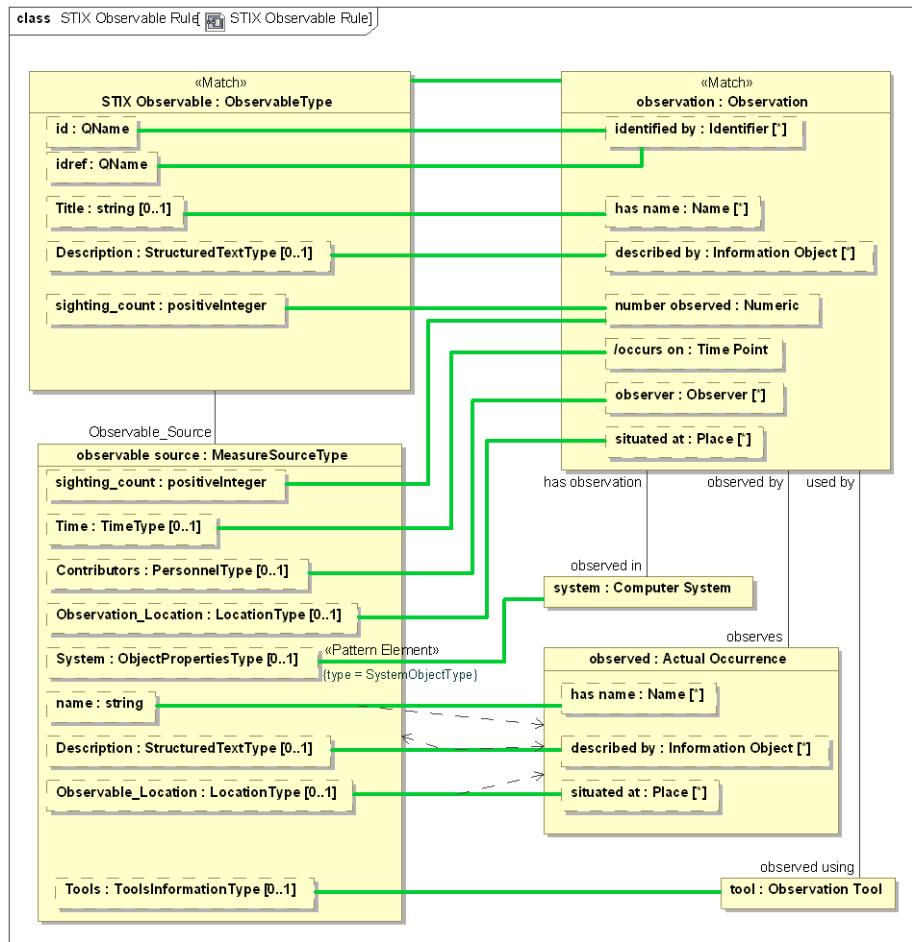


Figure 192. STIX Observable Rule

package STIX Mapping to the threat/risk conceptual model::conceptual reference model::STIX Mapping
Rules

10.13 Class STIX Sighting Rule

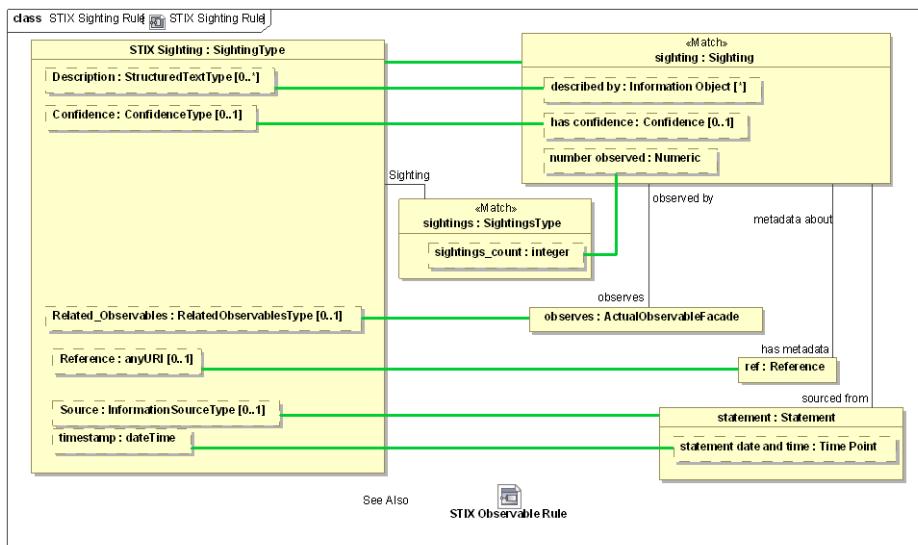


Figure 193. STIX Sighting Rule

package STIX Mapping to the threat/risk conceptual model conceptual reference model::STIX Mapping Rules

10.14 Class STIX Statement Rule

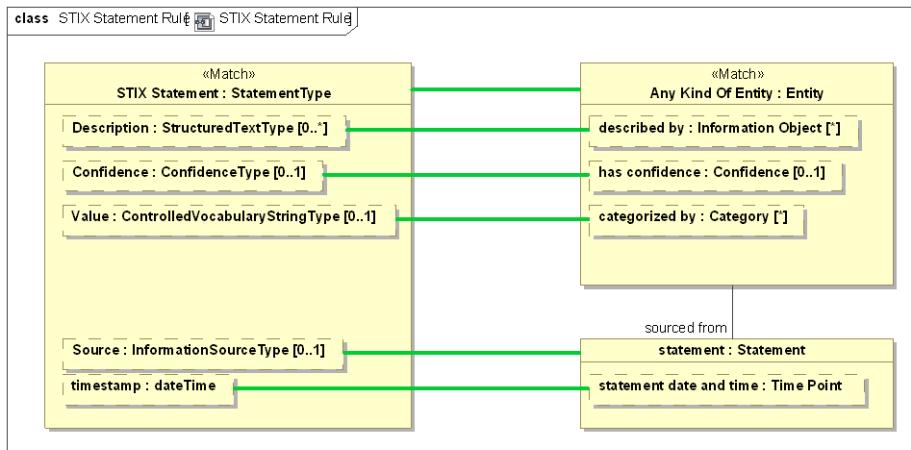


Figure 194. STIX Statement Rule

package STIX Mapping to the threat/risk conceptual model conceptual reference model::STIX Mapping Rules

10.15 Class STIX Threat Actor Rule

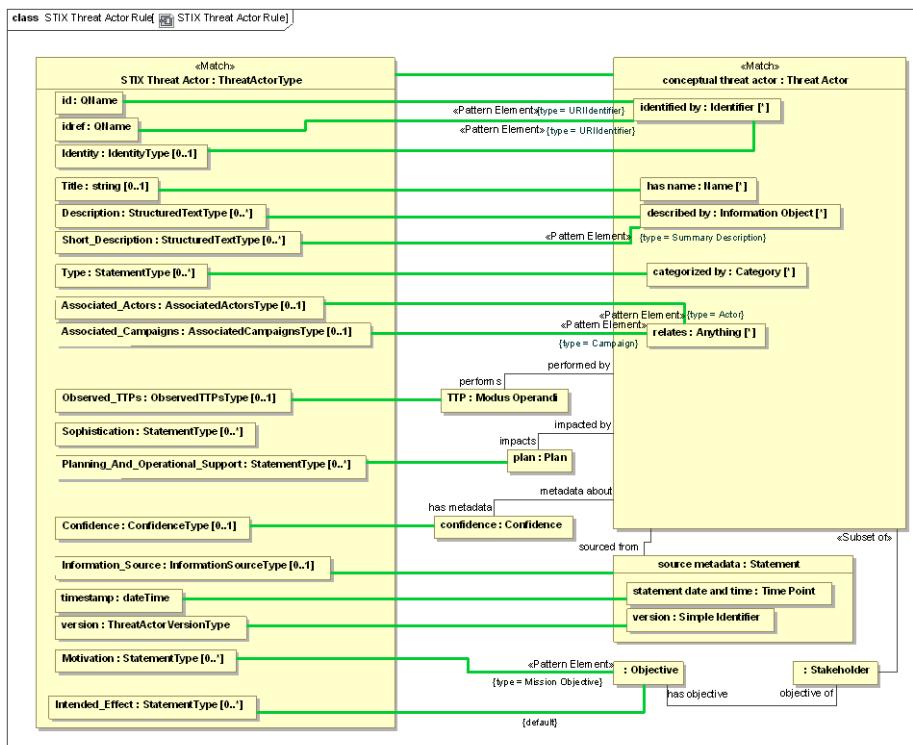


Figure 195. STIX Threat Actor Rule

package STIX Mapping to the threat/risk conceptual model conceptual reference model::STIX Mapping Rules

10.16 Class STIX TTP Rule

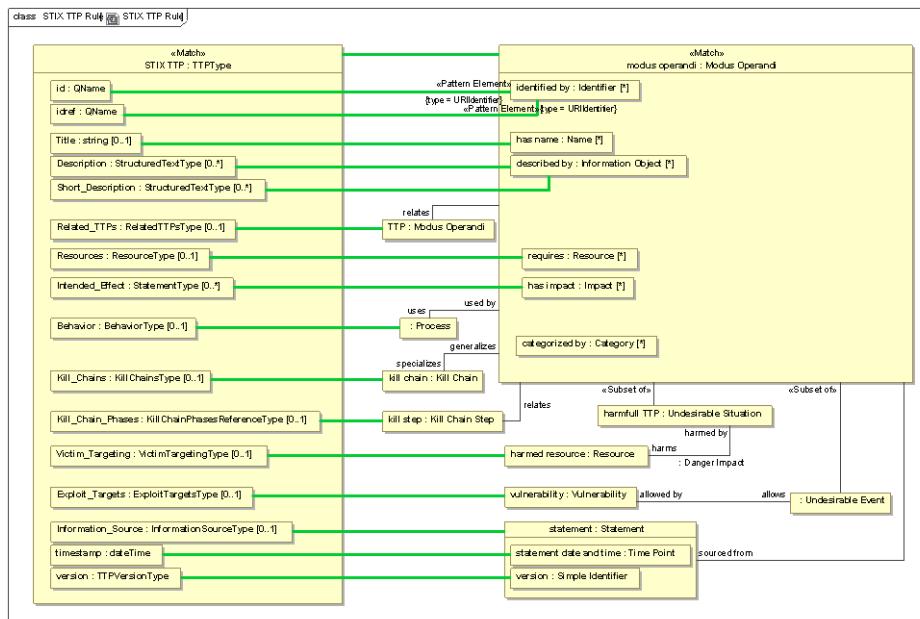


Figure 196. STIX TTP Rule

package STIX Mapping to the threat/risk conceptual model conceptual reference model::STIX Mapping
Rules

10.17 Class STIX Vocabulary Rule

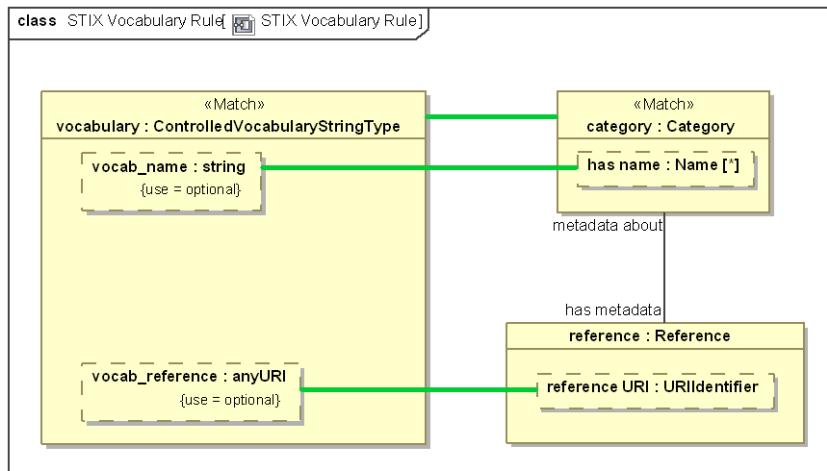


Figure 197. STIX Vocabulary Rule

package STIX Mapping to the threat/risk [conceptual model](#)[conceptual reference model](#)::STIX Mapping Rules

10.18 Class STIX Vulnerability Rule

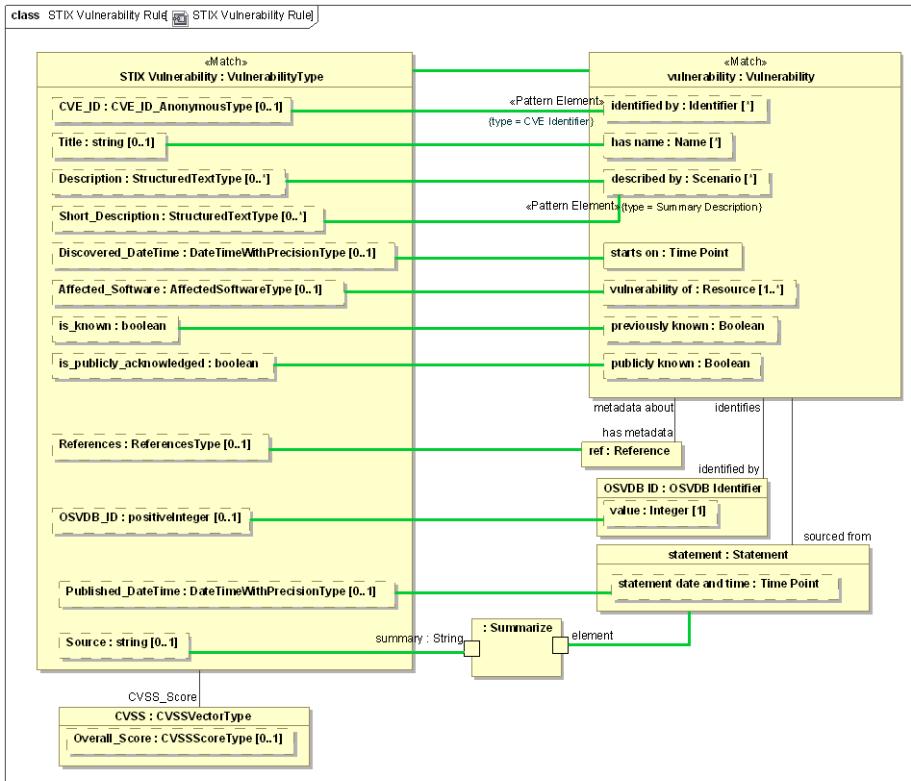


Figure 198. STIX Vulnerability Rule

package STIX Mapping to the threat/risk conceptual model conceptual reference model::STIX Mapping Rules

11 NIEM Mapping Specification (Normative)

This clause specifies the mapping between NIEM-Core and the threat/risk ~~eoneceptual modelconceptual reference model~~ using the mapping profile specified defined in section [Error! Reference source not found.⁴²](#).

11.1 How NIEM is represented

The NIEM reference models in NIEM-UML 3 are used as the normative representation of NIEM. The focus of the mapping is on “NIEM Core” and mapping those classes and properties that are relevant to threat ~~&and~~ risk.

11.2 Generic NIEM mapping rules and conventions

The mapping specification below specifies the semantic relationships between NIEM and the corresponding ~~eoneceptual modelconceptual reference model~~ elements. In some cases these relationships are direct and in other cases indirect, as indicated by the mapping rules. Within the mappings certain assumptions are made with respect to the mapping capability, as follows:

Primitive data types

The detailed mapping and conversion of primitive data types are well defined and implemented by underlying technologies. It is assumed that correct conversions will be made between various representations of strings, numbers, enumerations, dates, and other basic data types. These data types for NIEM are specified as XML data types, which are well defined. As such, primitive data mapping is not specified herein.

Quantity values and unit conversions

In the ~~eoneceptual modelconceptual reference model~~ quantities are defined in terms of their quantity kinds (e.g., temperature, length, etc.) and appropriate units (centigrade, meters, etc.) are expected in any exchange format. The value of properties are stated in terms of these quantity kinds and units, not as primitive data, such as “int.” Proper specification of units is critical for correct interpretation of data – quantity kinds should always be utilized in the ~~eoneceptual modelconceptual reference model~~, these quantity kinds should be mapped to units in specific data formats..

Each such quantity as a “value” that is a primitive data type, usually a number. Wherever the information is known the mapping specification defines the unit expected of a technology exchange format – thus “age:real” may be mapped to “age:year” if years can be determined to be the unit expected. It is an implementation option to assume units if none are provided or to ignore the underspecified data. If another data format expected “months” as age, the implementation framework should convert between months and years, even if such conversion is an approximation.

The implementation framework is to convert between quantity values and primitive data types based on the mapping specification and externally established conversion factors. It is the responsibility of the mapping implementation to convert between different units for the same quantity kind. Conversion values are not specified in the model so as not to introduce redundant specifications. Implementations are referred to the normative source at NIST for conversion factors and formula: <http://www.nist.gov/pml/wmd/metric/unit-conversion.cfm>.

Some conversions have no normative reference. For example, conversion between a probability percentage for risk and “high, medium, low” risk. Such conversions are implementation defined. Further implementation experience may introduce specific conversions in a later specification.

NIEM Augmentations

NIEM provides for augmentations, which are a technology work-around for multiple inheritance. The [conceptual model](#)[conceptual reference model](#) utilizes multiple inheritance (and multiple classification) directly. Implementations shall convert augmentations to a multiple inheritance interpretation when mapping to the [conceptual model](#)[conceptual reference model](#).

NIEM substitution groups

NIEM substitution groups correspond roughly to “subsets” and “redefines” relations in the [conceptual model](#)[conceptual reference model](#). Subsets and redefines provide for a hierarchy of properties. Implementations shall interpret and map the correspondence between substitution groups and the mapped properties with subsets and redefines.

In some cases the combination of generalization and subsets/redefines in the [conceptual model](#)[conceptual reference model](#) alleviates the need for some intermediate types as found in NIEM. For example in contact information NIEM utilizes a first-class relationship to contact information which has a property “contact means” and a substitution group with another set of types for each of those properties. In the [conceptual model](#)[conceptual reference model](#) a relationship is made directly to contact means which then has subclasses that serve the same purpose. Where a substitution group head and a class are mapped to the same concept the implementation shall interpret that the NIEM class contains the property and that each substitue for that property corresponds to a subclass in the [conceptual model](#)[conceptual reference model](#), which will also have a mapping. In this way the implementation shall correctly map between the substitution groups and conceptual class hierarchies.

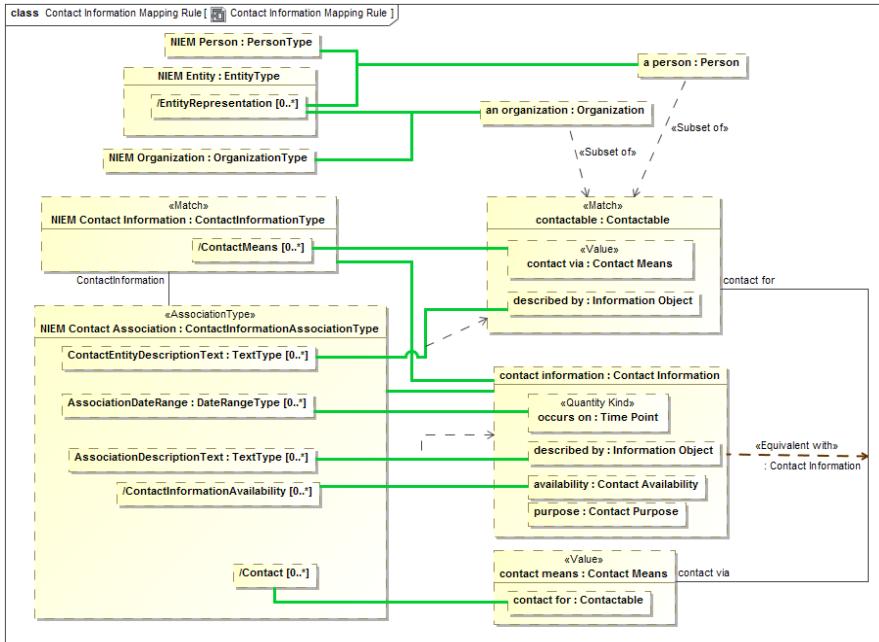


Figure 1014 Example mapping involving substitution groups.

11.3 NIEM Mapping to the threat / risk model::Facades::Contact Information

11.3.1 Diagram: Contact Information Facades

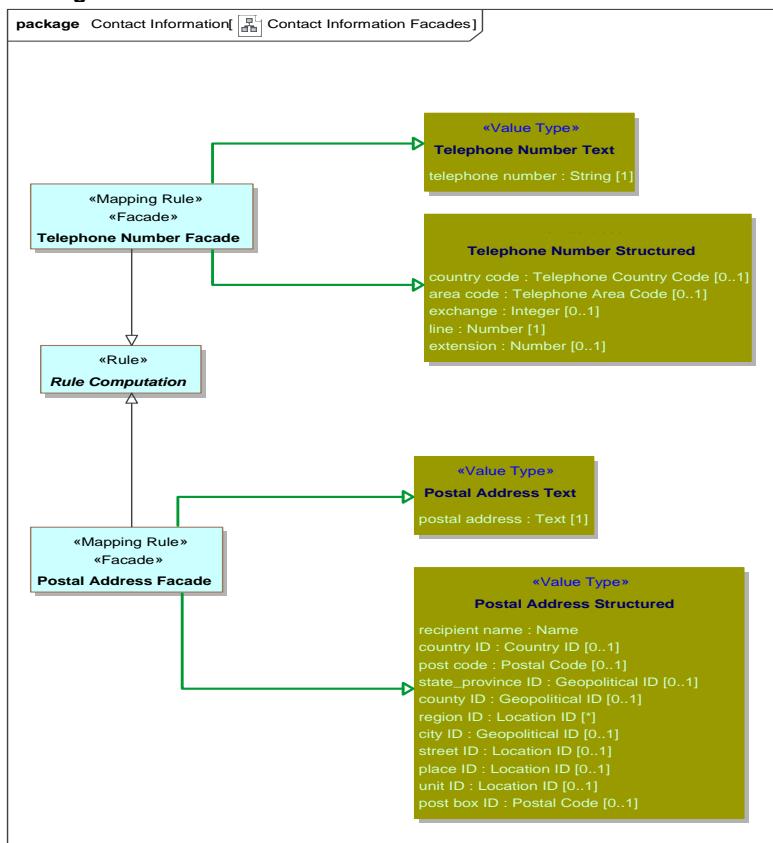


Figure 199. Contact Information Facades

11.3.2 Class Postal Address Facade

The union of textual and structured address. Mapping logic will parse and distribute the fields.

11.3.21 Direct Supertypes

[Postal Address Structured](#), [Postal Address Text](#), [Rule Computation](#)

package NIEM Mapping to the threat / risk model::Facades::Contact Information

11.3.22 Attributes

PostCodeBase : [String](#)

Post code less any local delimiter, such as the U.S. postal code.

PostCodeSuffix : [String](#)

Post code after any local delimiter, such as the U.S. postal code.

DeliveryPoint : [String](#)

Combination of street and place ID.

11.3.3 Class Telephone Number Facade

The union of textual and structured phone number. Mapping logic will parse and distribute the fields.

11.3.31 Direct Supertypes

[Rule Computation](#), [Telephone Number Structured](#), [Telephone Number Text](#)

package NIEM Mapping to the threat / risk model::Facades::Contact Information

11.4 NIEM Mapping to the threat / risk model::Facades::Injury

11.4.1 Diagram: Person Injury Facade

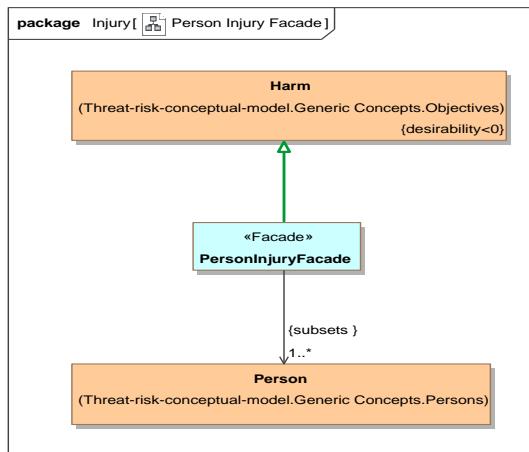


Figure 200. Person Injury Facade

11.4.2 Class PersonInjuryFacade

A form of harm or damage sustained by a person.

Note: Personal injury is made specific to a person in the context of NIEM, but injury as defined in law may be harm to any entity.

11.4.21 Direct Supertypes

[Harm](#)

package NIEM Mapping to the threat / risk model::Facades::Injury

11.4.22 Associations

:[Person](#) [1..*] Subsets: :[Resource](#)

11.5 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships

Mapping specification of NIEM Core to the threat/risk model

11.5.1 Diagram: NIEM Mapping Rules

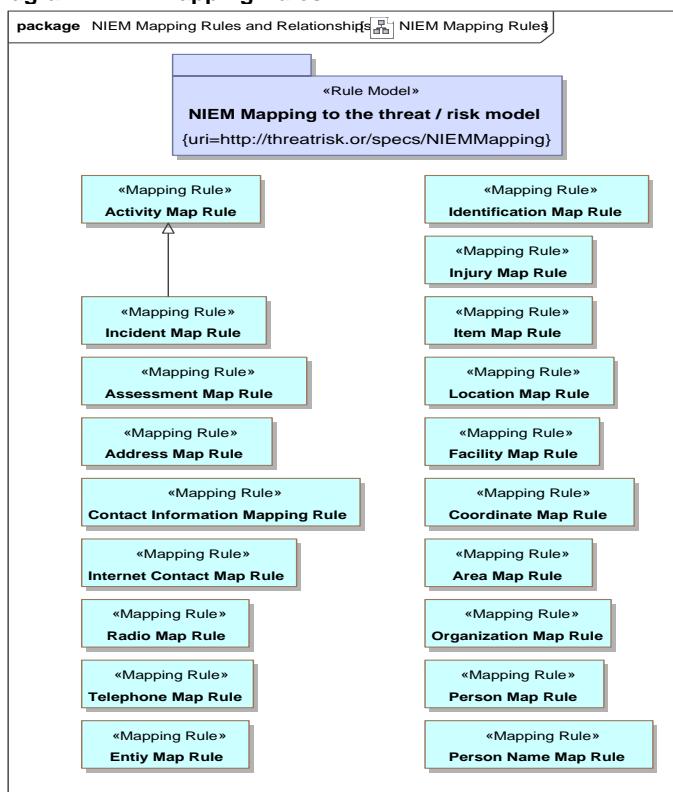


Figure 201. NIEM Mapping Rules

11.5.2 Diagram: NIEM Mapping Summary 1

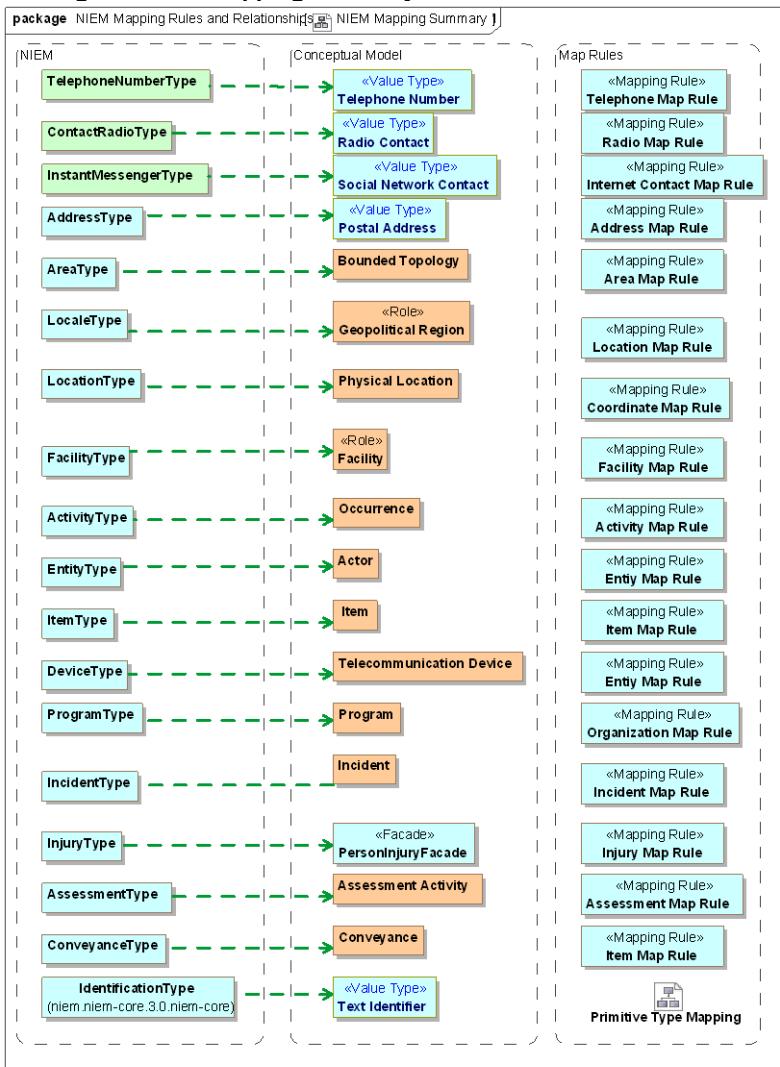


Figure 202. NIEM Mapping Summary 1

11.5.3 Diagram: NIEM Mapping Summary 2

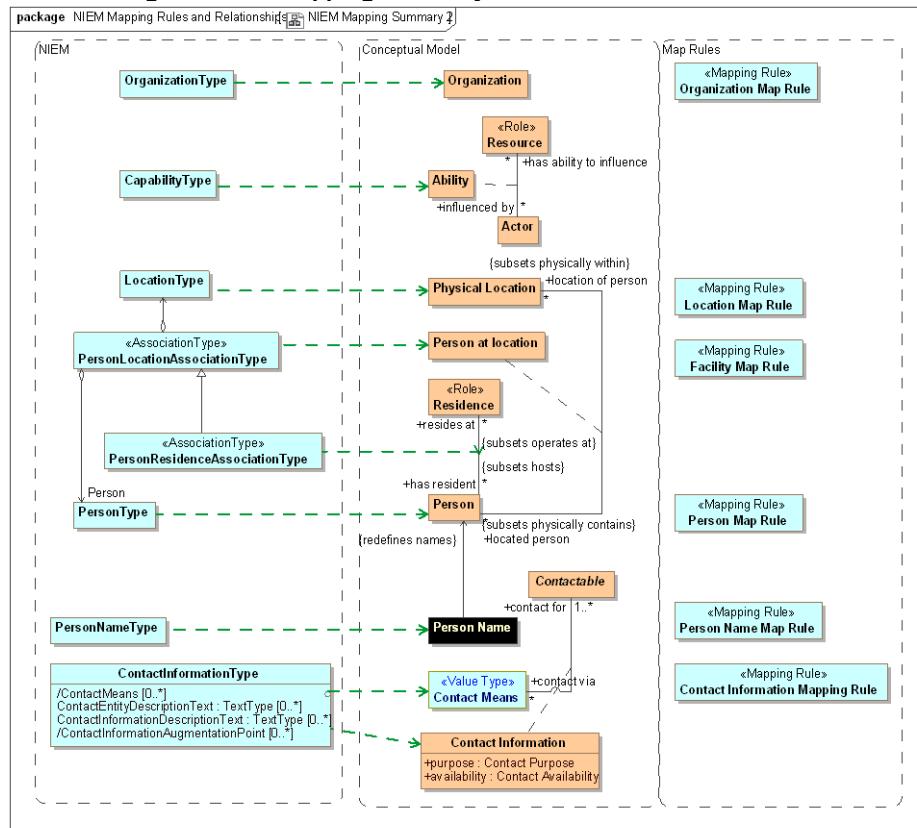


Figure 203. NIEM Mapping Summary 2

11.6 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Activity

Mapping specification of NIEM Activity to the threat/risk model

11.6.1 Diagram: Activity Mapping Summary

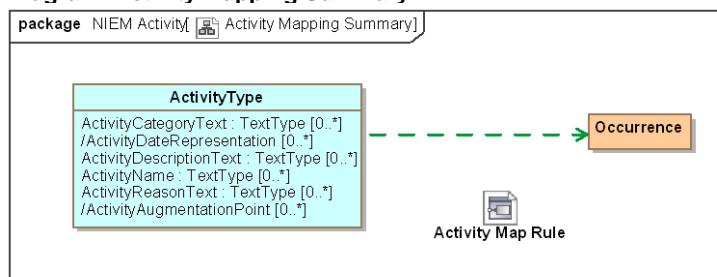


Figure 204. Activity Mapping Summary

11.6.2 Class Activity Map Rule

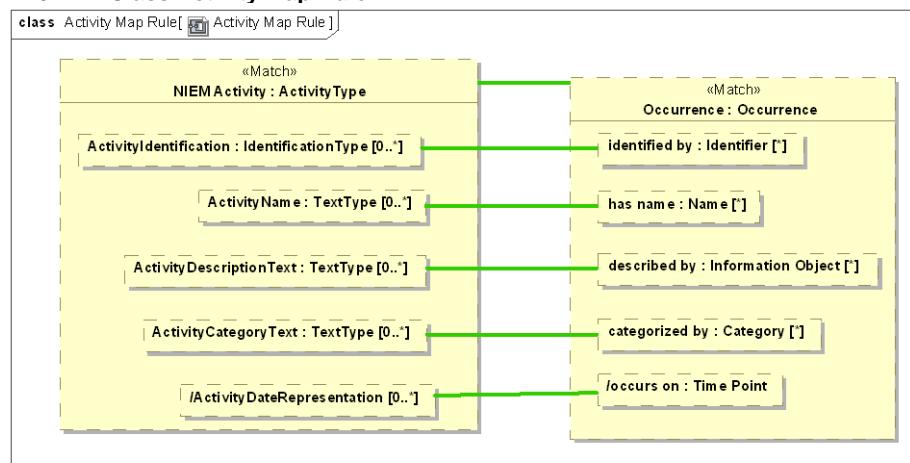


Figure 205. Activity Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Activity

11.7 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Assessment

Mapping specification of NIEM Assessment to the threat/risk model

11.7.1 Diagram: Assessment Mapping Summary

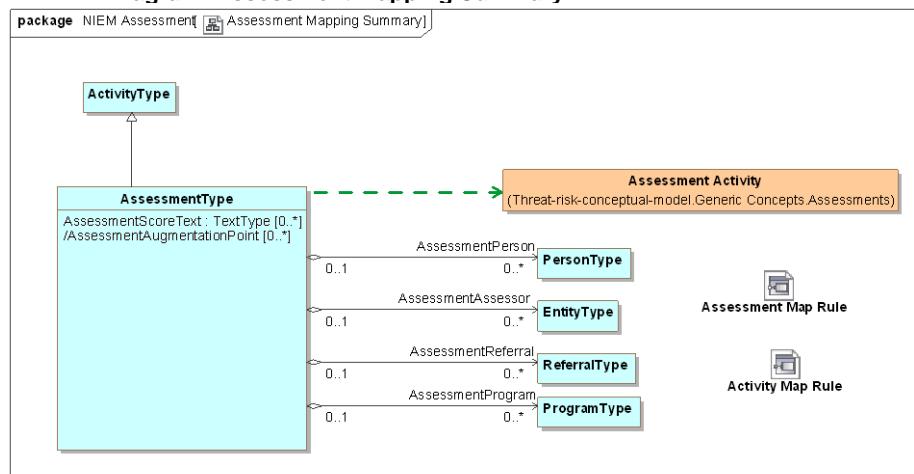


Figure 206. Assessment Mapping Summary

11.7.2 Class Assessment Map Rule

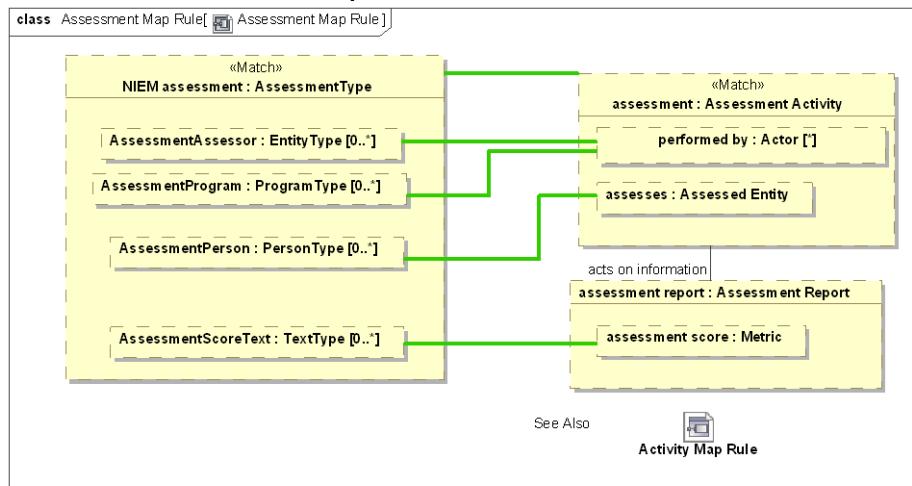


Figure 207. Assessment Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Assessment

11.8 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation

Mapping specification of NIEM Contact Information to the threat/risk model

11.8.1 Diagram: Contact Information Mapping Summary

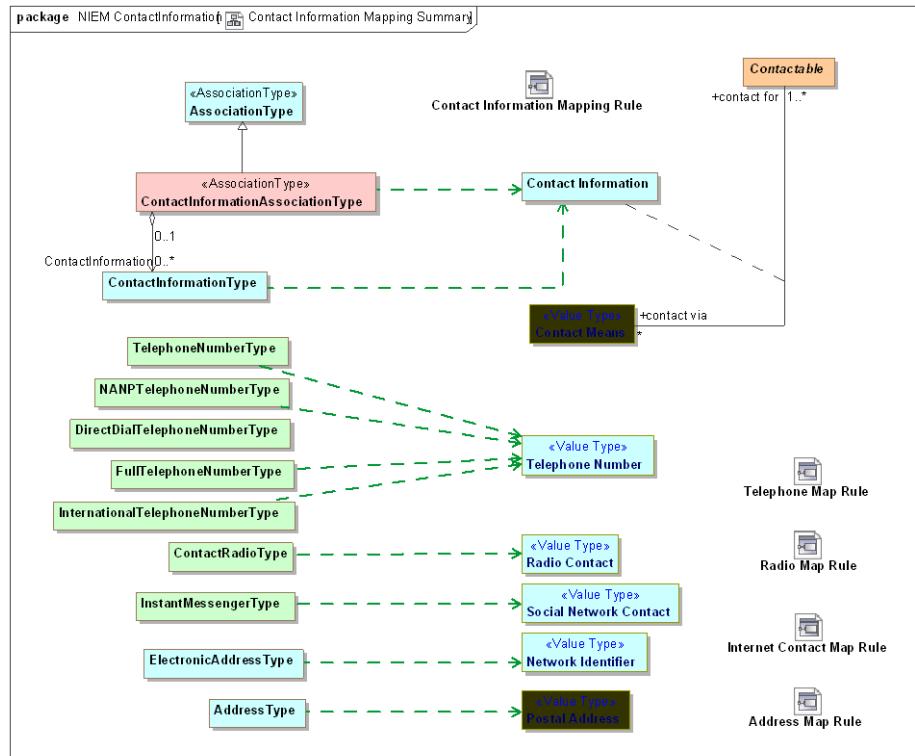


Figure 208. Contact Information Mapping Summary

11.8.2 Class Address Map Rule

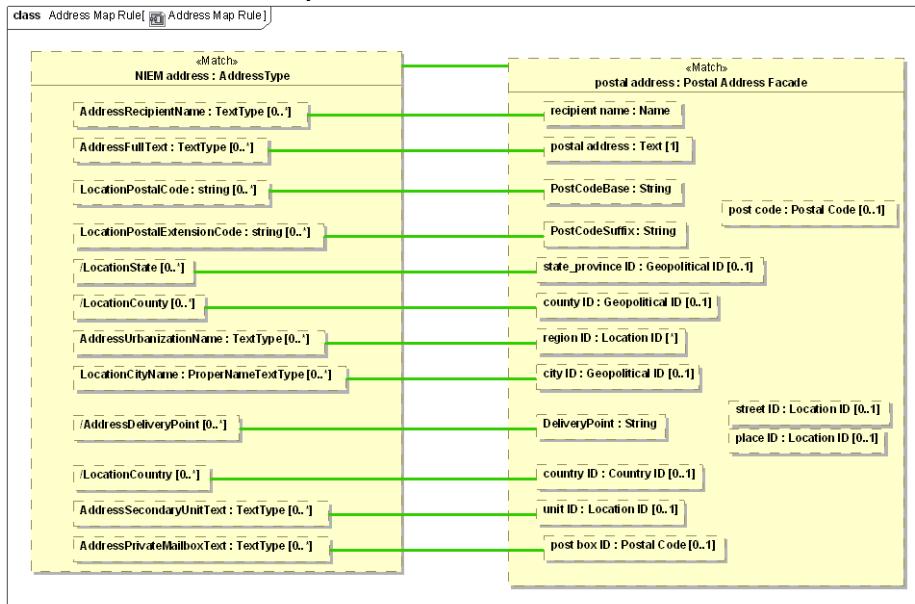


Figure 209. Address Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation

11.8.3 Class Contact Information Mapping Rule

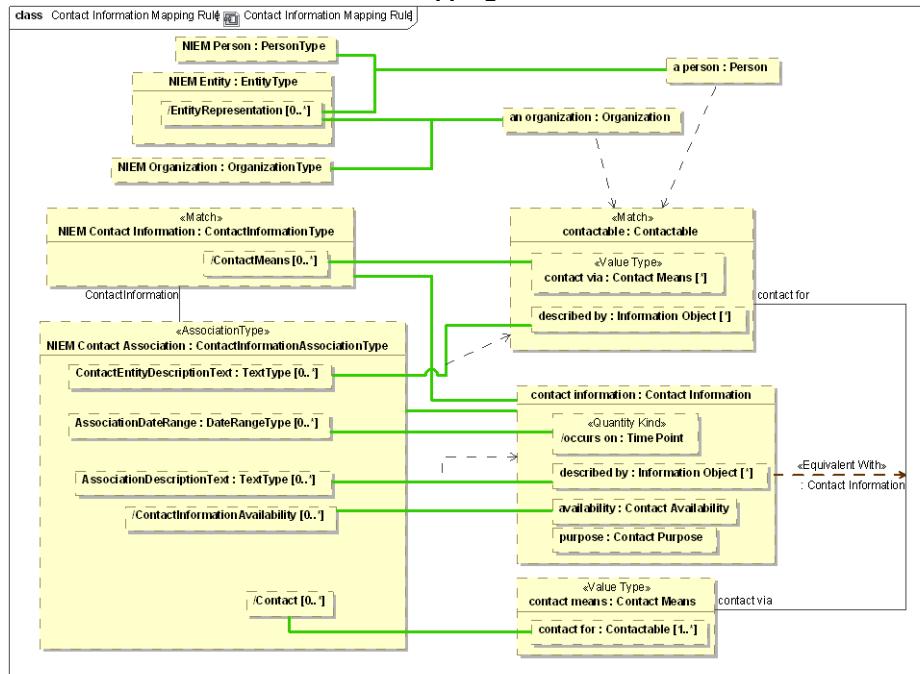


Figure 210. Contact Information Mapping Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation

11.8.4 Class Internet Contact Map Rule

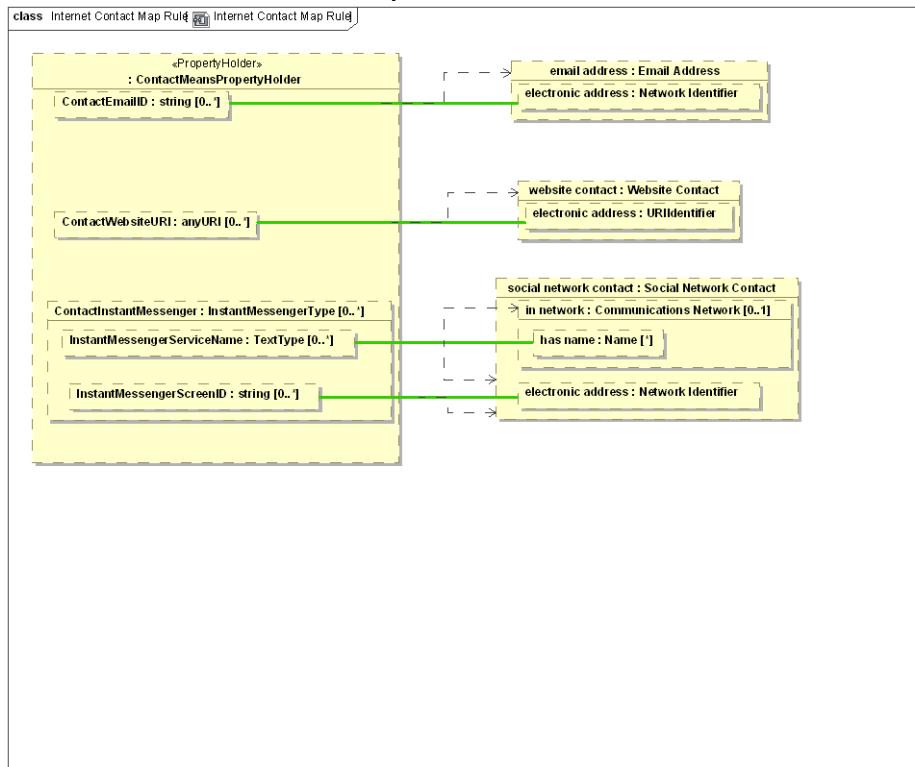


Figure 211. Internet Contact Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation

11.8.5 Class Radio Map Rule

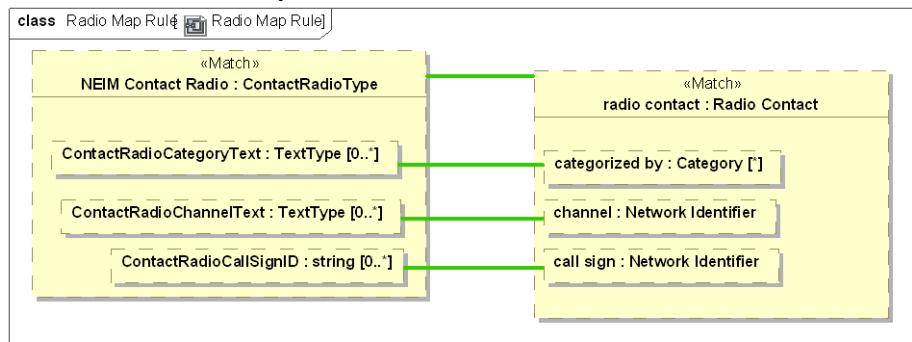


Figure 212. Radio Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation

11.8.6 Class Telephone Map Rule

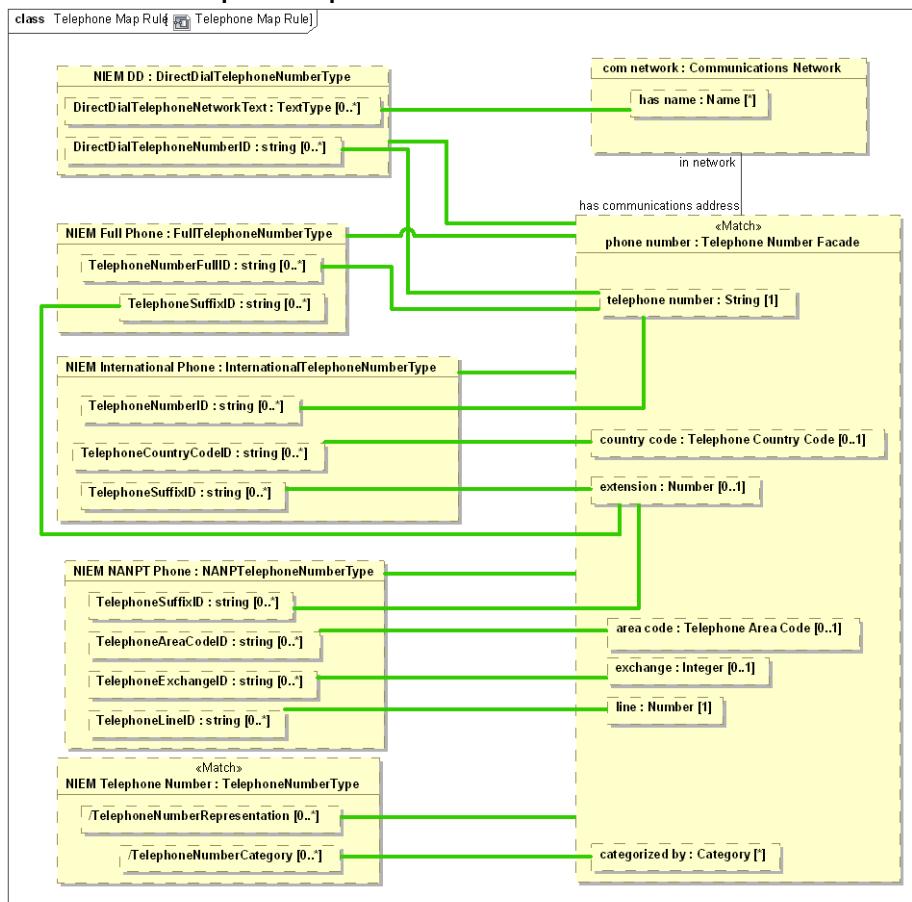


Figure 213. Telephone Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation

11.9 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Entity

Mapping specification of NIEM Entity to the threat/risk model.

11.9.1 Diagram: Entity Mapping Summary

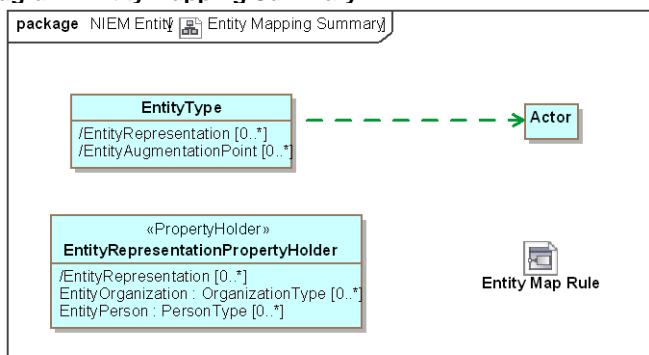


Figure 214. Entity Mapping Summary

11.9.2 Class Entiy Map Rule

Detail is provide in the mappings to person and organization.

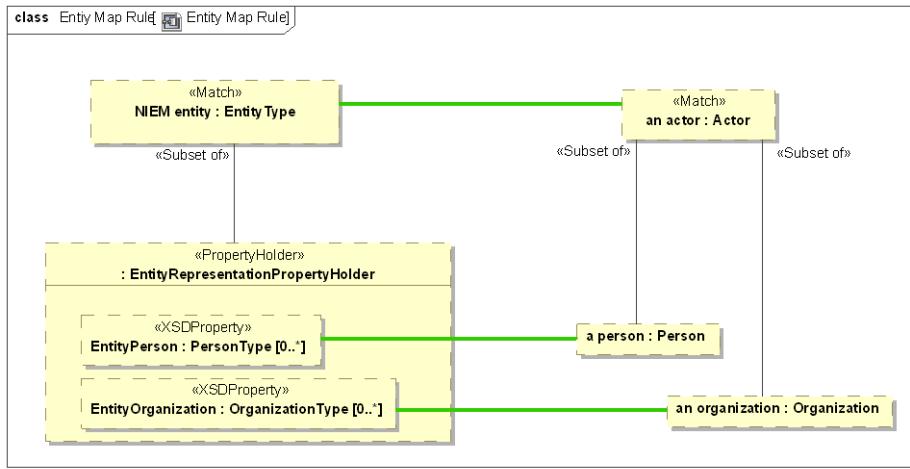


Figure 215. Entity Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Entity

11.10 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Identification

Mapping specification of NIEM Identification and identifiers to the threat/risk model.

11.10.1 Diagram: Identification Mapping Summary

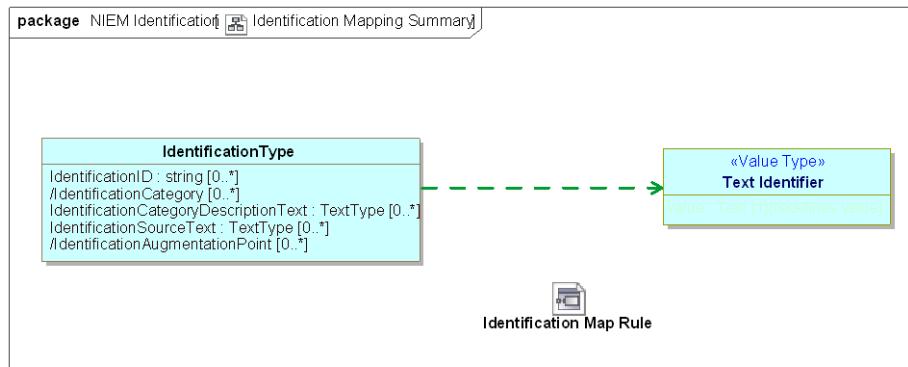


Figure 216. Identification Mapping Summary

11.10.2 Class Identification Map Rule

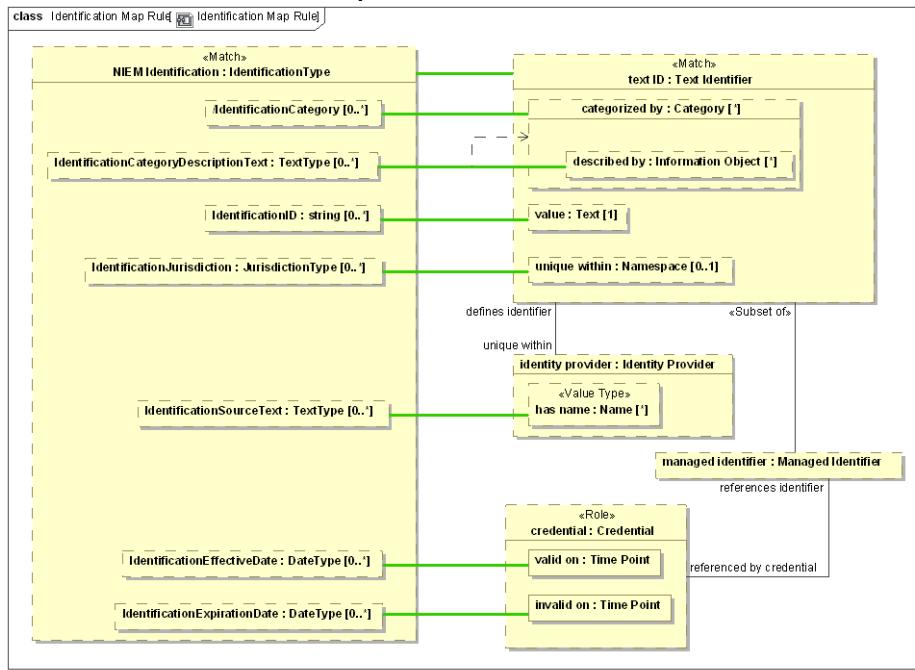


Figure 217. Identification Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Identification

11.11 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Incident

Mapping specification of NIEM Incident to the threat/risk model.

11.11.1 Diagram: Incident mapping summary

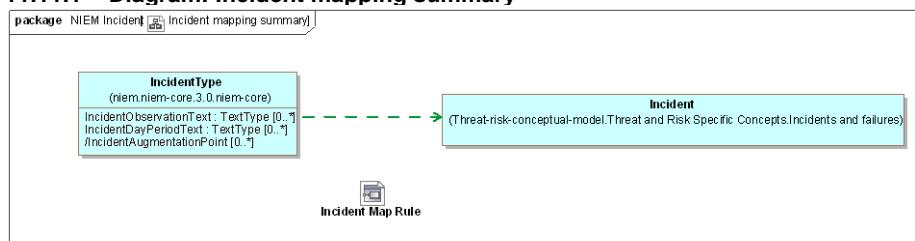


Figure 218. Incident mapping summary

11.11.2 Class Incident Map Rule

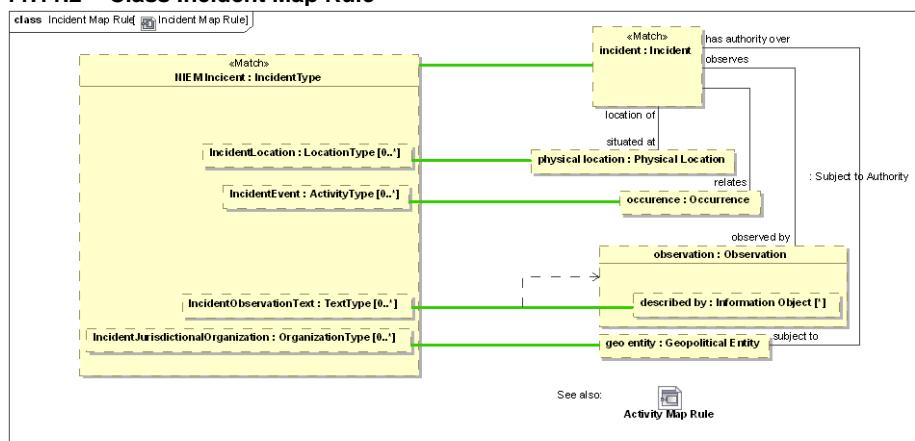


Figure 219. Incident Map Rule

11.11.21 Direct Supertypes

[Activity Map Rule](#)

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Incident

11.12 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Injury

Mapping specification of NIEM Injury to the threat/risk model.

11.12.1 Diagram: Injury Mapping Summary

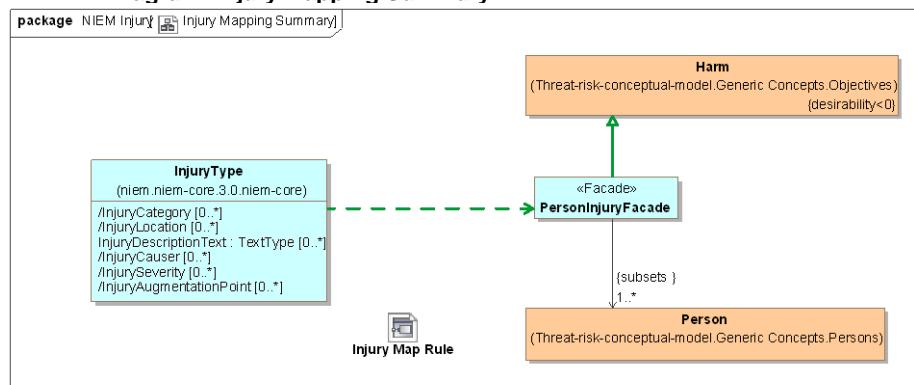


Figure 220. Injury Mapping Summary

11.12.2 Class Injury Map Rule

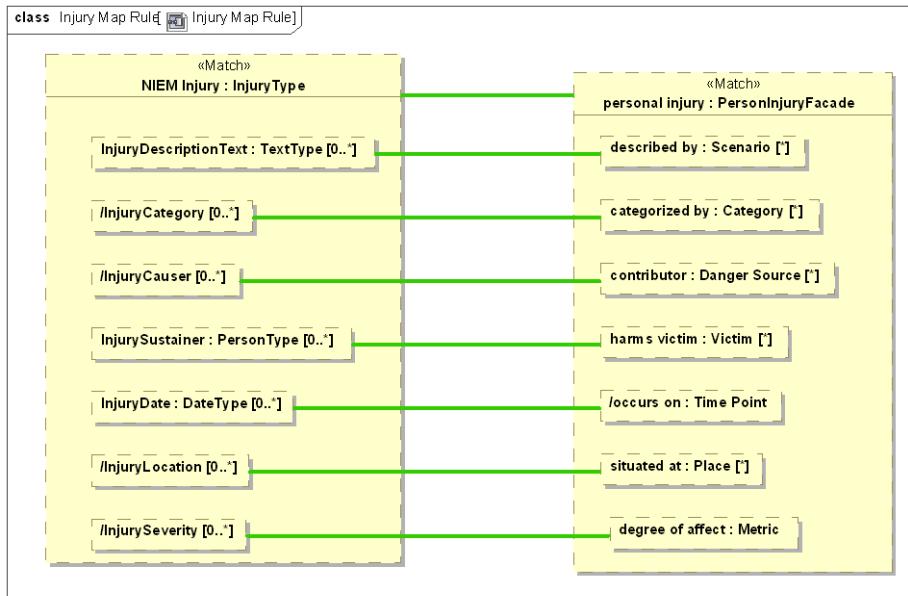


Figure 221. Injury Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Injury

11.13 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Item

Mapping specification of NIEM Item to the threat/risk model.

11.13.1 Diagram: Item Mapping Summary

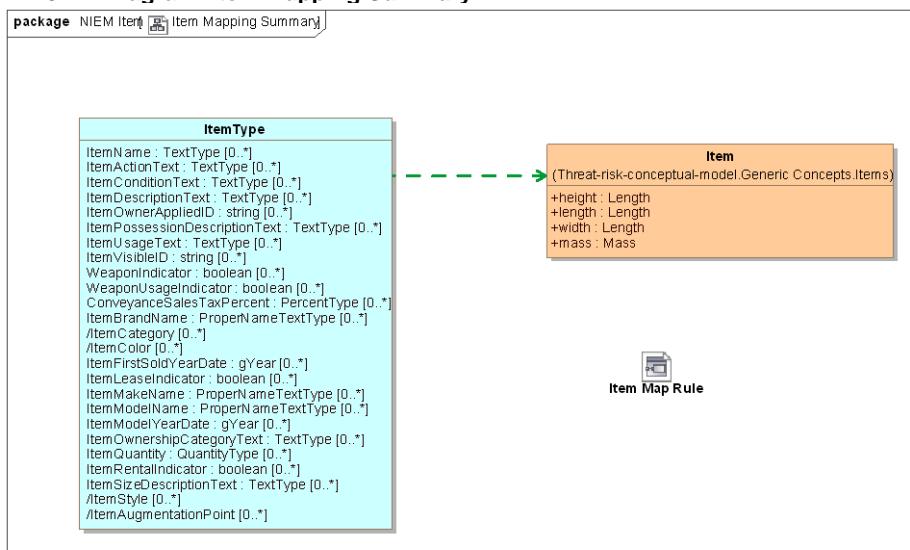


Figure 222. Item Mapping Summary

11.13.2 Class Item Map Rule

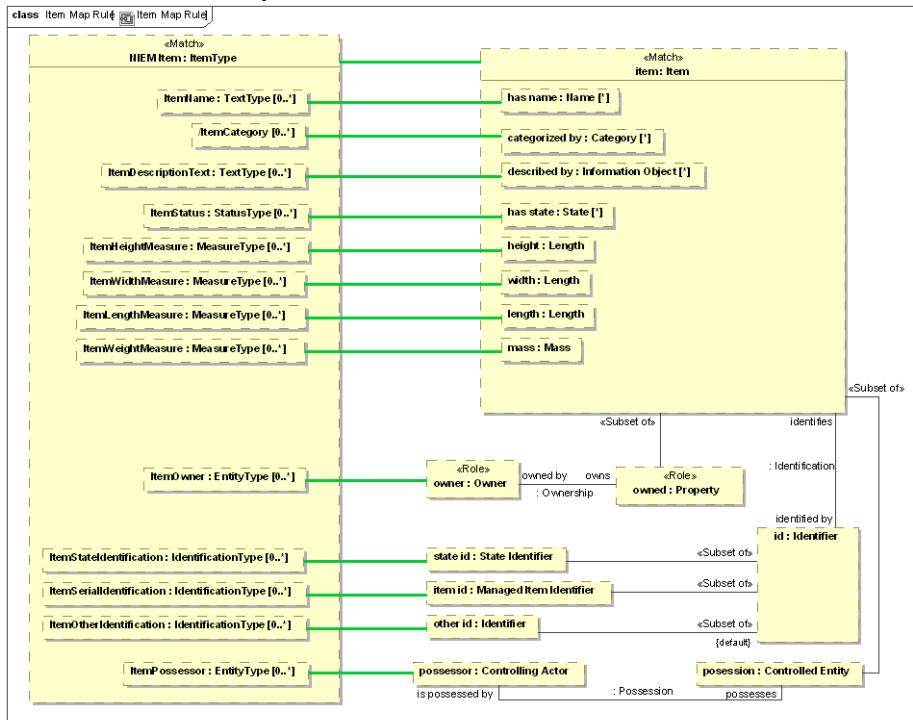


Figure 223. Item Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Item

11.14 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location

Mapping specification of NIEM Location to the threat/risk model.

11.14.1 Diagram: Location mapping summary

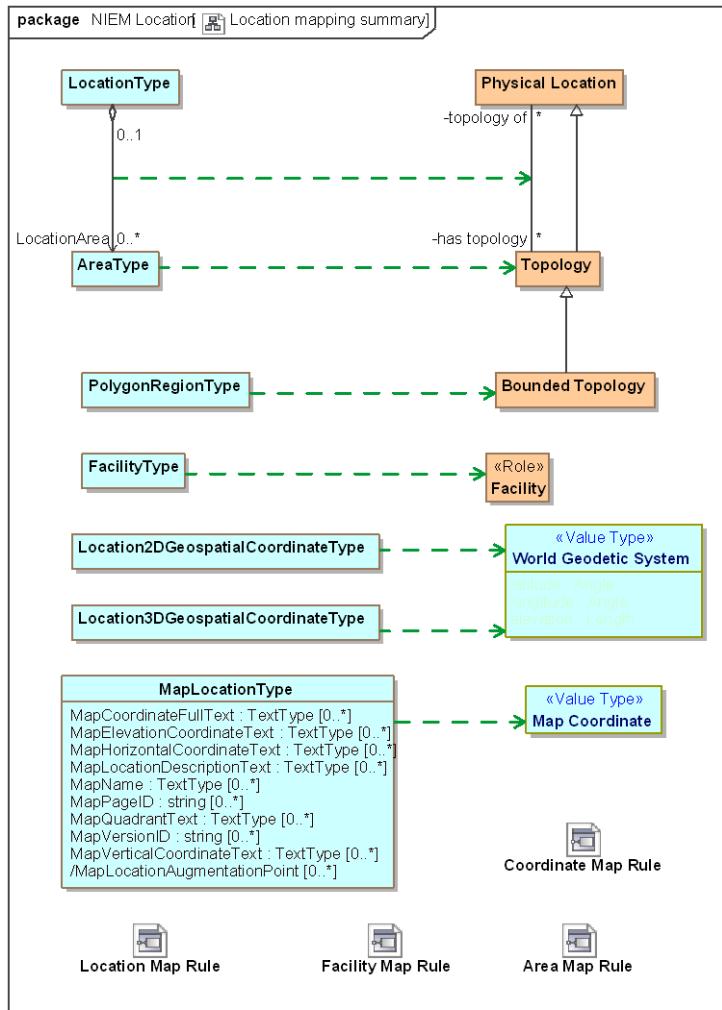


Figure 224. Location mapping summary

11.14.2 Class Area Map Rule

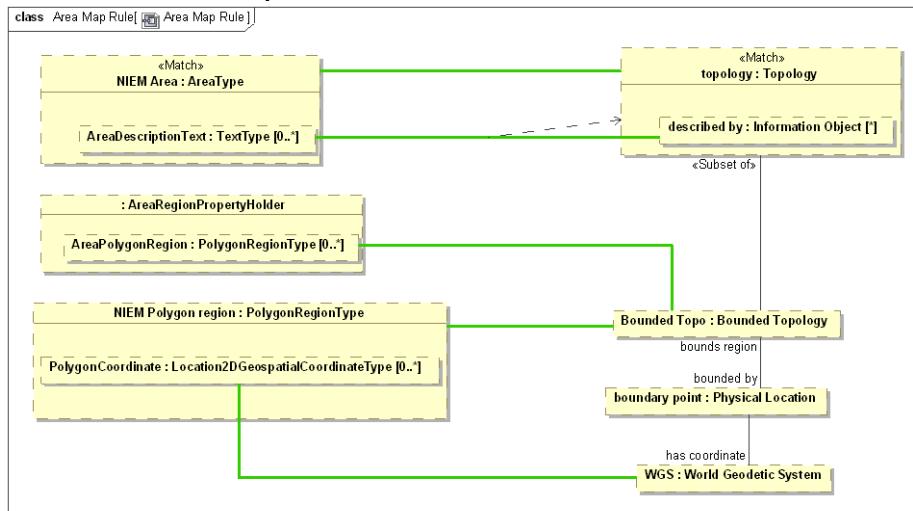


Figure 225. Area Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location

11.14.3 Class Coordinate Map Rule

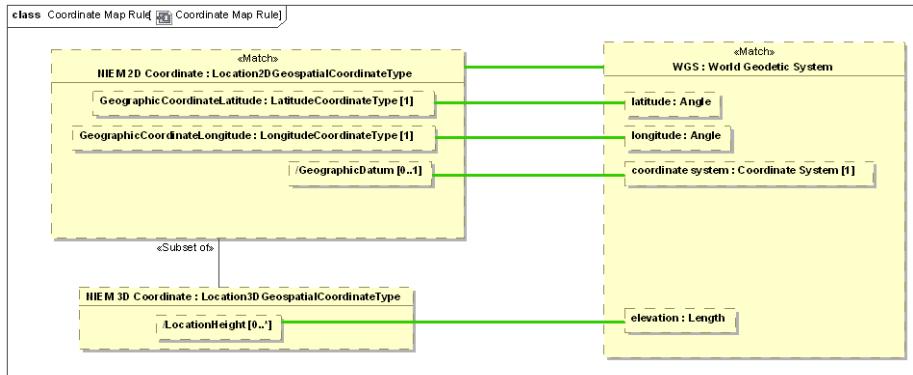


Figure 226. Coordinate Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location

11.14.4 Class Facility Map Rule

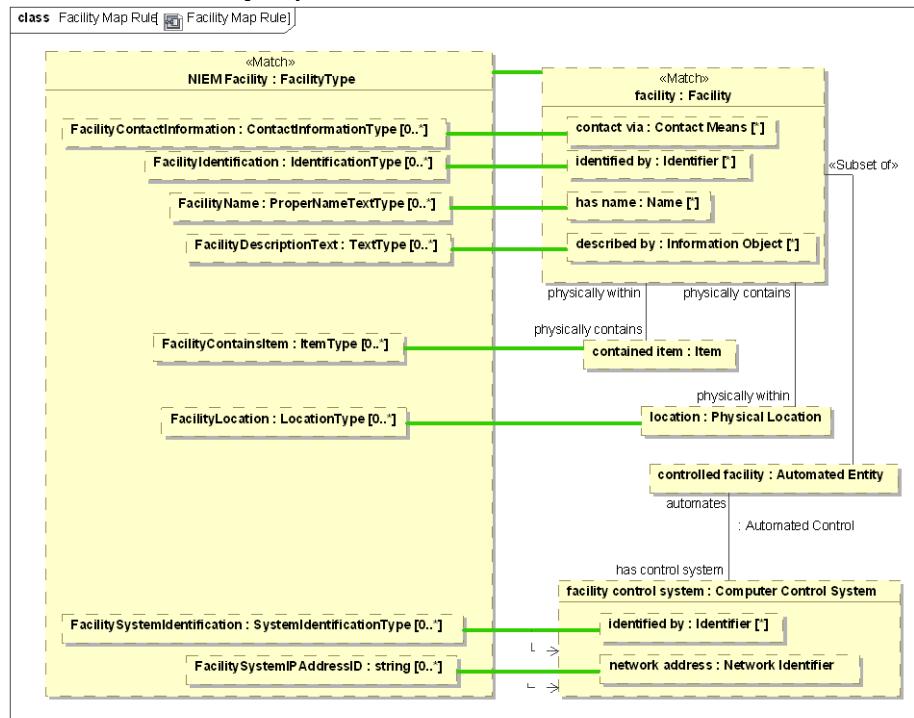


Figure 227. Facility Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location

11.14.5 Class Location Map Rule

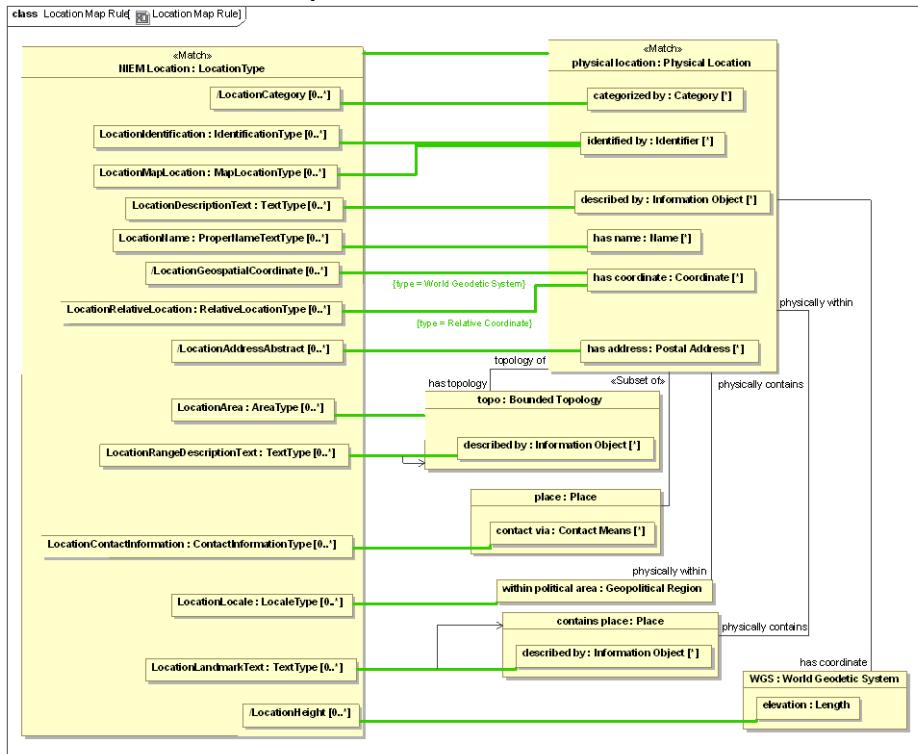


Figure 228. Location Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location

11.15 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Organization

Mapping specification of NIEM Organization to the threat/risk model.

11.15.1 Diagram: NIEM Organization Mapping Summary

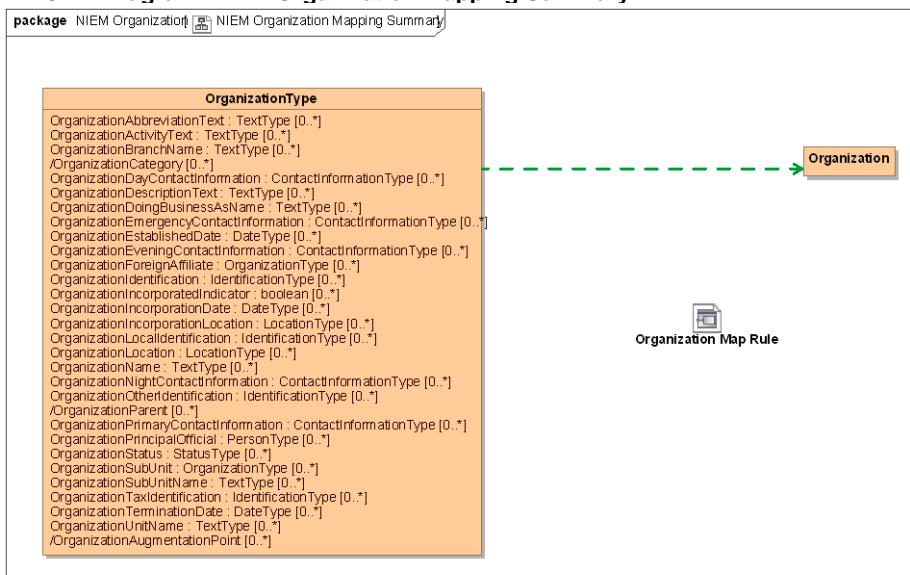


Figure 229. NIEM Organization Mapping Summary

11.15.2 Class Organization Map Rule

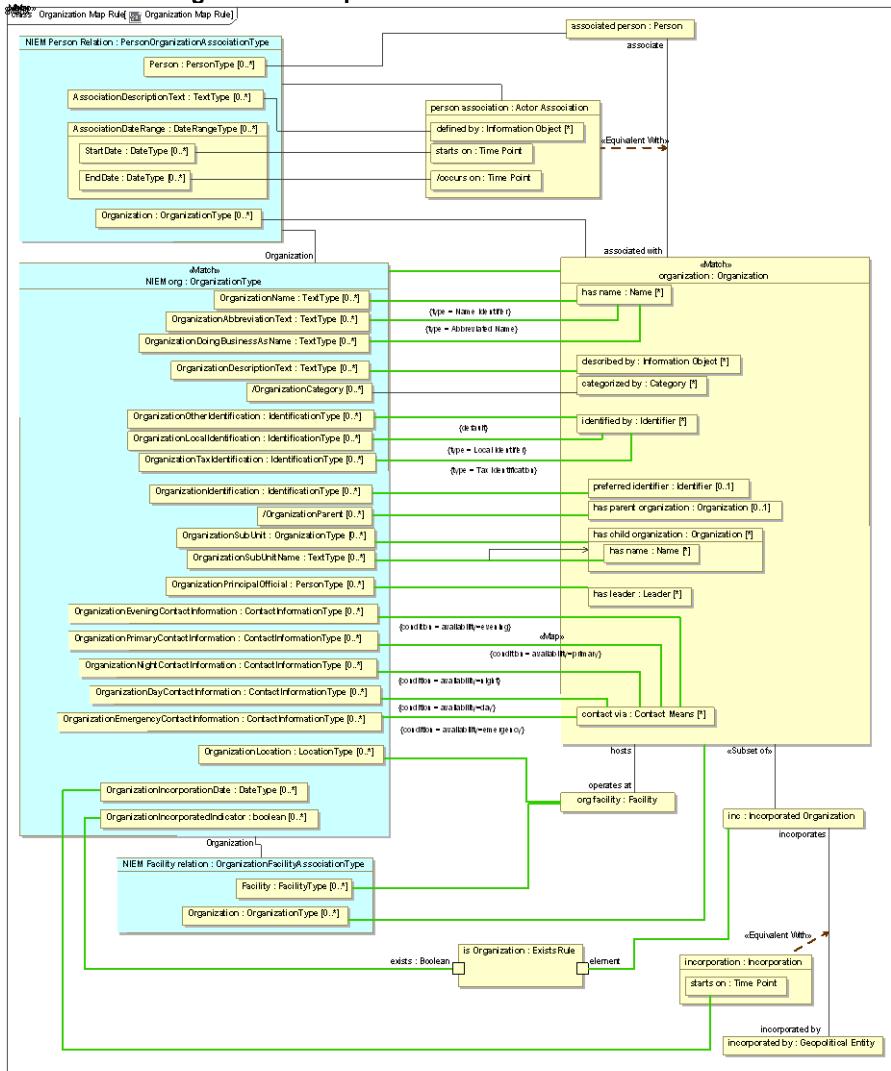


Figure 230. Organization Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Organization

11.16 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Person

Mapping specification of NIEM Person to the threat/risk model.

11.16.1 Diagram: Person Mapping Summary

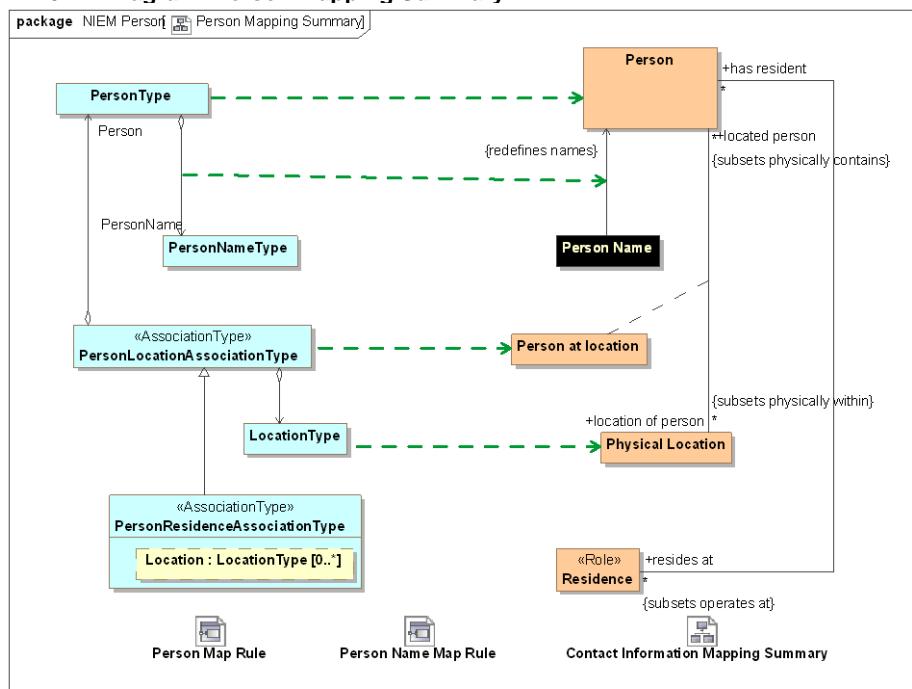


Figure 231. Person Mapping Summary

11.16.2 Class Person Map Rule

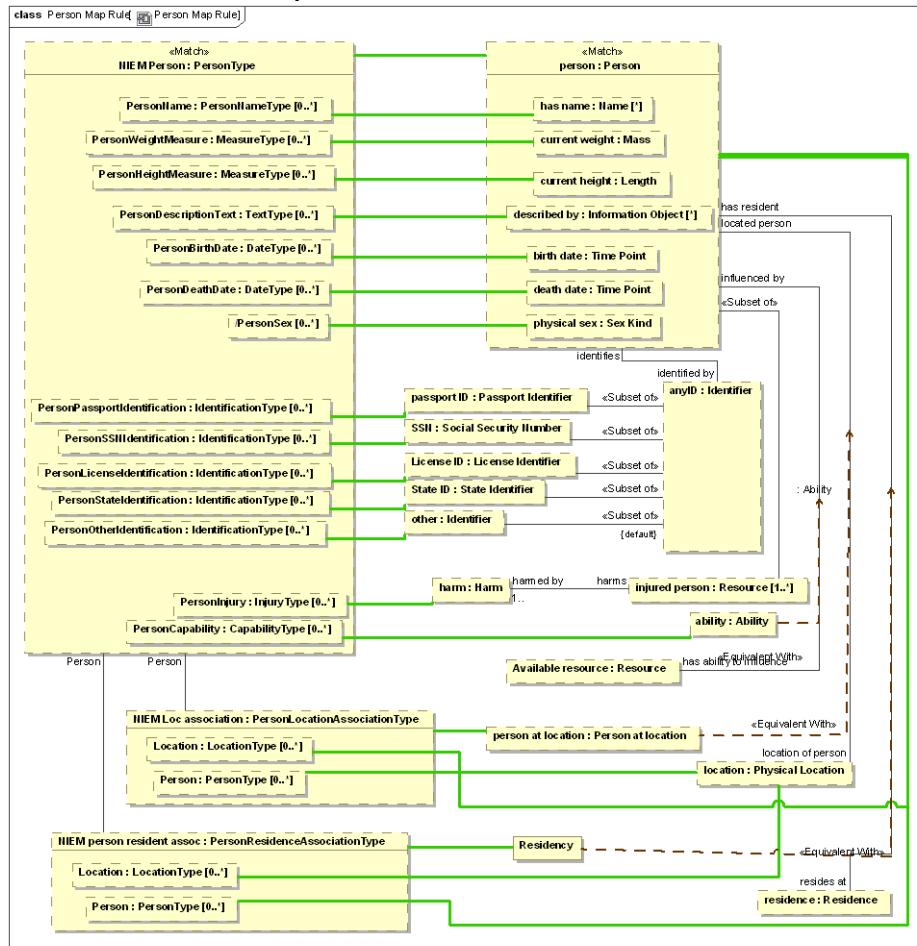


Figure 232. Person Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Person

11.16.3 Class Person Name Map Rule

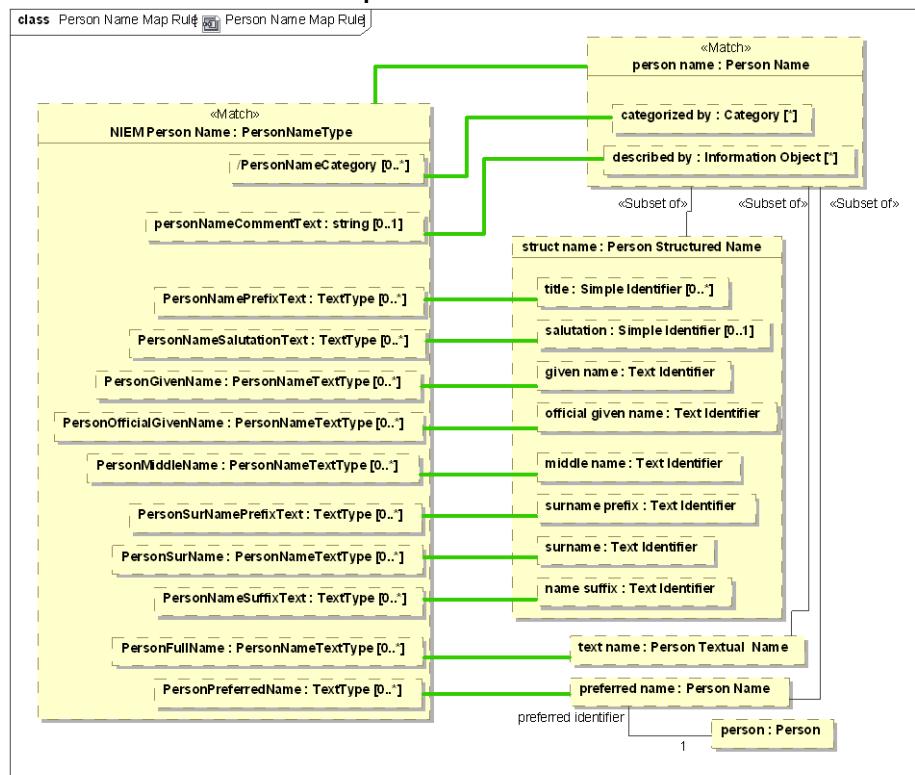


Figure 233. Person Name Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Person

11.17 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM PrimitiveTypes

Mapping for values. Specifics of value mapping within the bounds of the defined representation rules are implementation specific.

11.17.1 Diagram: Primitive Type Mapping

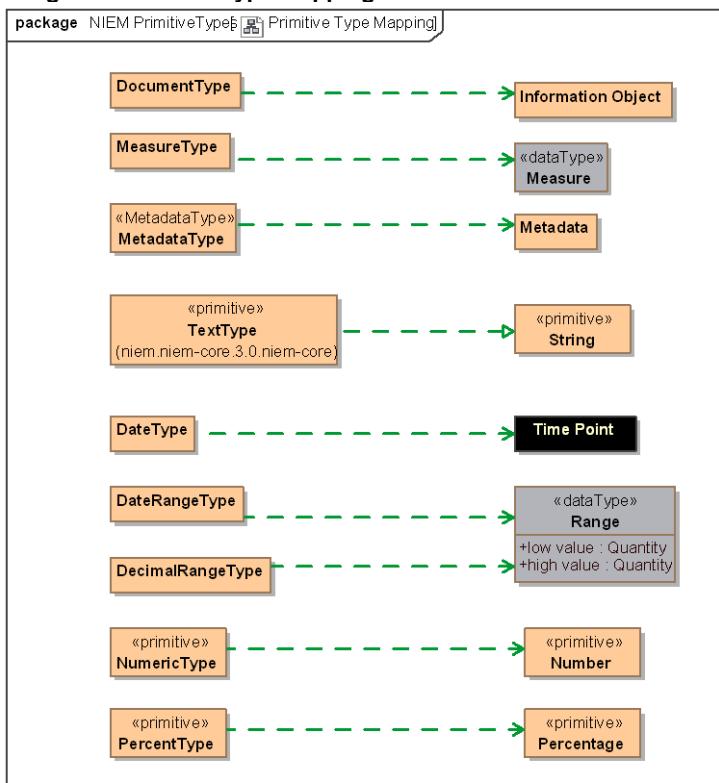


Figure 234. Primitive Type Mapping

12 Threat and Risk Alignment to NIST 800-53

The NIST Special Publication 800-53, Revision 4 are security and privacy controls designed primarily as policy and technology neutral, supporting system development lifecycles and implementations. In this submission, security and privacy terms are represented as a distinct and contemporary concepts e.g., *Security Requirements*, and *Common Vulnerability Scoring System* throughout the model. This is designed to implement a vendor neutral vocabulary of terms that provide a well-defined taxonomy for cross-domain understanding and business competency for the treatment of threats and risk. Linking the threat and risk model to the NIST family of controls provides extensive meaning for analysis through a normative and common platform.

For example;

The 800.53 **Access Control** (AC);

According to 800-53, Revision 4, this control family addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. The threat and risk model can be used to convey the selected security controls in documentation, software, physical, and managerial controls in a consistent manner. The AC control family addresses a myriad of details related in and between both physical and cyber system requirements. To this end, the threat and risk model may be consumed for reporting, analyzing and mitigating threats, as well as assisting in the assessment of risk through scoring and measurement categorization.

Below is a table showing the AC control family mapped to the threat and risk model's Access Property, Control Authority, Security Level, Asserting Policy, Process and Planning. All Control Families map to these areas in the model as a **consistent set of generic information for all 800.53 control families**.

800.53 Control Family	Threat and Risk Model	Comparative Explanation of Use
<p>Access Control (AC) ACCESS CONTROL POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: <i>organization-defined personnel or roles</i>]:</p> <p>1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current:</p> <p>1. Access control policy [Assignment: <i>organization-defined frequency</i>]; and</p> <p>2. Access control procedures [Assignment: <i>organization-defined frequency</i>].</p>	<p> Control Authority Diagram</p> <p> Subject to Authority Association Class</p> <p> Authority Class</p> <p> has authority over Property</p> <p> provides access to Property</p> <p> Association[made available by:Alter Ability - provides access to:Entity]Association</p> <p> Access Identifier Class</p> <p> Access Point Class</p> <p> Association[has opening:Access Point - enters through:Boundary]Association</p> <p> Association[has portal:Access Point - enters into:System]Association</p> <p> Access Complexity Enumeration</p> <p> Access Vector Enumeration</p>	<p>The “Provides Access to” property, and association entities, in relationship to “Access Control” family is exploited as the <i>capability</i> of an actor. As defined within the conceptual Ontology of the Threat and Risk Model. Further, the Access Control (s) family of controls can now be described with specificity of ownership i.e., associations, identifiers, points of entry, complexity and vectors reflecting scores, as well as failures to entities. Other areas of the model shared include Control Authority, Security level, Asserting Policy, and Process Package and Plans.</p>

	<p> Access Control Failure Class</p> <p> Association [traversed using: Entry Action - enters through: Access Point] Association</p> <p> Association [Exit Action - exit through: Access Point] Association</p> <hr/> <p> security level Property</p> <p> Communications Security Level Class</p> <p> security level Property</p> <p> Security Danger Class</p> <hr/> <p>Asserting Policy Association</p> <p> Policy Diagram</p> <p> Policy Class</p> <hr/> <p> Processes Package</p> <p> Process and plans Diagram</p> <p> Process and plans Process and plansElement Value</p> <p> Process and plans Process and plansElement Value</p> <p> Invoke Process Class</p>	
--	---	--

Study of Information Architecture

This section links the top-level of the 800-53 family of controls to specific subject areas of the threat and risk model. Providing vendor and business consumers with the ability to define threats and risk through the lens of information architecture data model. Unlike non-specific models, this provides a variety of enhanced reporting capabilities within and across communities, i.e., Law Enforcement, Cybersecurity, Defense and others. In this way, the threat and risk model enables the integration of information security and privacy concerns into organizational processes including data modeling, analytics and reporting across a myriad of platforms and communities of interest. Ultimately, successful use of this may expose the development of the entire threat and risk field of study, for modern uses in information architecture.

The following table describes how the threat and risk model facilitates the NIST 800-53 controls.

800.53 r4 Control Area/Definition	Threat and Risk Model	Explanations and Association
Access Control (AC) ACCESS CONTROL POLICY AND PROCEDURES <u>Control:</u> The organization: a. Develops, documents, and disseminates to	Control Authority Diagram Subject to Authority Association Class	This control area (Access Control (AC)) of the 800.53 controls map to the Authority Class of the Threat and Risk Conceptual Model Conceptual reference model . The Control Authority , Security

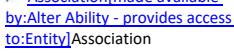
<p>[Assignment: organization-defined personnel or roles]:</p> <p>1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current:</p> <p>1. Access control policy [Assignment: organization-defined frequency]; and</p> <p>2. Access control procedures [Assignment: organization-defined frequency].</p>	<p> Authority Class</p> <p> has authority over Property</p> <hr/> <p> provides access to Property</p> <p> Association[made available by:Alter Ability - provides access to:Entity] Association</p> <p> Access Identifier Class</p> <p> Access Point Class</p> <p> Association[has opening:Access Point - enters through:Boundary] Association</p> <p> Association[has portal:Access Point - enters into:System] Association</p> <p> Access Complexity Enumeration</p> <p> Access Vector Enumeration</p> <p> Access Control Failure Class</p> <p> Association[traversed using:Entry Action - enters through:Access Point] Association</p> <p> Association[Exit Action - exit through:Access Point] Association</p> <hr/> <p> security level Property</p> <p> Communications Security Level Class</p> <p> security level Property</p> <p> Security Danger Class</p> <hr/> <p>Asserting Policy Association</p> <p> Policy Diagram</p> <p> Policy Class</p> <hr/> <p> Processes Package</p> <p> Process and plans Diagram</p> <p> Process and plans Process and plansElement Value</p> <p> Process and plans Process and plans</p>	<p><i>and Policy Classes and Property of the model address the assignment of the access authority and policies /procedures to facilitate the access or the prevention of access to organizational entities.</i></p>
---	---	---

	<i>plansElement</i> Value	
	 Invoke Process Class	
Awareness and Training (AT) SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [Assignment: organization-defined frequency]; and 2. Security awareness and training procedures [Assignment: organization-defined frequency].	<p> Observation Package</p> <p> Observation Diagram</p> <p> Observation Class</p> <p> Observation Tool Class</p> <p> performs observation Property</p> <p> observation Property</p> <hr/> <p> Contact Information Package</p> <p> Contact Information Diagram</p> <p> Contact Information Association Class</p> <p> Contact Means Class</p> <p> contact for Property</p> <hr/> <p> Control Authority Diagram</p> <p> Subject to Authority Association Class</p> <p> Authority Class</p> <p> has authority over Property</p> <hr/> <p> provides access to Property Association[made available by:Alter Ability - provides access to:Entity]Association</p> <p> Access Identifier Class</p> <p> Access Point Class</p> <p> Association[has opening:Access Point - enters through:Boundary]Association</p> <p> Association[has portal:Access Point - enters into:System]Association</p> <p> Access Complexity Enumeration</p>	<p>This control area (Awareness and Training (AT)) of the 800.53 controls map to the Observation Class and Basic Packages (Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning) in the Threat and Risk Conceptual Model. The Observation package, and Contact Information Package of <i>classes and properties</i> address the responsibility, information and coordination among organizational entities for SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES.</p> <p>.</p>

	<p> Access Vector Enumeration</p> <p> Access Control Failure Class</p> <hr/> <p> Association [traversed using:Entry Action - enters through:Access Point] Association</p> <p> Association [Exit Action - exit through:Access Point] Association</p> <hr/> <p> security level Property</p> <p> Communications Security Level Class</p> <p> security level Property</p> <p> Security Danger Class</p> <hr/> <p>Asserting Policy Association</p> <p> Policy Diagram</p> <p> Policy Class</p> <hr/> <p> processes Package</p> <p> Process and plans Diagram</p> <p> process and plans Process and plansElement Value</p> <p> process and plans Process and plansElement Value</p> <p> Invoke Process Class</p>	
<p>Audit and Accountability (AU)</p> <p>AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <ol style="list-style-type: none"> Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <ol style="list-style-type: none"> An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and Reviews and updates the current: 	<p>Observation Package</p> <p> Observation Diagram</p> <p> Observation Class</p> <p> Observation Tool Class</p> <p> performs observation Property</p> <p> observation Property</p> <hr/> <p> Control Authority Diagram</p> <p> Subject to Authority Association Class</p>	<p>This control area (Audit and Accountability (AU)) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and Observation Package of the Threat and Risk Conceptual Model. The Observation package and Contact Information Package of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES.</p>

<p>1. Audit and accountability policy [<i>Assignment: organization-defined frequency</i>]; and</p> <p>2. Audit and accountability procedures [<i>Assignment: organization-defined frequency</i>].</p>	<p> Authority Class</p> <p> has authority over Property</p> <hr/> <p> provides access to Property</p> <p> Association[made available by:Alter Ability - provides access to:Entity] Association</p> <p> Access IdentifierClass</p> <p> Access PointClass</p> <p> Association[has opening:Access Point - enters through:Boundary] Association</p> <p> Association[has portal:Access Point - enters into:System] Association</p> <p> Access ComplexityEnumeration</p> <p> Access VectorEnumeration</p> <p> Access Control FailureClass</p> <p> Association[traversed using:Entry Action - enters through:Access Point] Association</p> <p> Association[Exit Action - exit through:Access Point] Association</p> <hr/> <p> security levelProperty</p> <p> Communications Security LevelClass</p> <p> security levelProperty</p> <p> Security DangerClass</p> <hr/> <p> Asserting Policy Association</p> <p> Policy Diagram</p> <p> Policy Class</p> <hr/> <p> ProcessesPackage</p> <p> Process and plansDiagram</p> <p> Process and plans Element Value</p> <p> Process and plans Process and</p>	
---	---	--

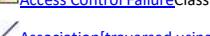
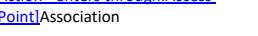
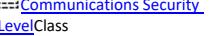
	<p><i>plansElement</i> Value</p>  Invoke Process Class	
Security Assessment and Authorization (CA) SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]; 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and 2. Security assessment and authorization procedures [Assignment: organization-defined frequency].	 Control Authority Diagram  Subject to Authority Association Class  Authority Class  has authority over Property <hr/>  provides access to Property  Association[made available by:Alter Ability - provides access to:Entity]Association  Access Identifier Class  Access Point Class  Association[has opening:Access Point - enters through:Boundary]Association  Association[has portal:Access Point - enters into:System]Association  Access Complexity Enumeration  Access Vector Enumeration  Access Control Failure Class  Association[traversed using:Entry Action - enters through:Access Point]Association  Association[Exit Action - exit through:Access Point]Association <hr/>  security level Property  Communications Security Level Class  security level Property  Security Danger Class <hr/>  Asserting Policy Association  Policy Diagram	This control area (Security Assessment and Authorization (CA)) of the 800.53 maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and Assessment areas of the Threat and Risk Conceptual Model . The Control Authority, Asserting Policy and Assessment Package of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES .

	<p> policy Class</p> <hr/> <p> Assessment Package  Assessment Diagram  has assessment Property  Assessment Activity Class  Assessment Report Class  assessment of Property  assessment score Property</p> <hr/> <p> processesPackage  process and plansDiagram  process and plans Process and plansElement Value  process and plans Process and plansElement Value  Invoke ProcessClass</p>	
<p>Configuration Management (CM) CONFIGURATION MANAGEMENT POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Configuration management policy [Assignment: organization-defined frequency]; and 2. Configuration management procedures [Assignment: organization-defined frequency]. 	<p> Control Authority Diagram  Subject to Authority Association Class  Authority Class  has authority over Property</p> <hr/> <p> provides access to Property  Association[made available by:Alter Ability - provides access to:Entity]Association  Access IdentifierClass  Access PointClass  Association[has opening:Access Point - enters through:Boundary]Association  Association[has portal:Access Point - enters into:System]Association  Access ComplexityEnumeration</p>	<p>This control area (Configuration Management (CM)) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and Patterns of the Threat and Risk Conceptual Model reference model. The Control Authority, Asserting Policy and Assessment Package of classes and properties addresses the responsibility, information and coordination among organizational entities for the SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES.</p>

	<p> Access Vector Enumeration</p> <p> Access Control Failure Class</p> <hr/> <p> Association[traversed using:Entry Action - enters through:Access Point] Association</p> <p> Association[Exit Action - exit through:Access Point] Association</p> <hr/> <p> security level Property</p> <p> Communications Security Level Class</p> <p> security level Property</p> <p> Security Danger Class</p> <hr/> <p>Asserting Policy Association</p> <p> Policy Diagram</p> <p> Policy Class</p> <hr/> <p> Assessment Package</p> <p> Assessment Diagram</p> <p> has assessment Property</p> <p> Assessment Activity Class</p> <p> Assessment Report Class</p> <p> assessment of Property</p> <p> assessment score Property</p> <hr/> <p> Patterns Package</p> <p> Patterns Diagram</p> <p> Patterning Generalization Set</p> <p> Pattern Involvement Class</p> <p> Situation Pattern Class</p> <p> Indicator Pattern Class</p> <p> ObservablePatternFacade Class</p> <hr/> <p> Processes Package</p>
--	--

	<p> Process and plansDiagram</p> <p> process and plans <i>Process and plansElement Value</i></p> <p> Process and plans <i>Process and plansElement Value</i></p> <p> Invoke ProcessClass</p>	
<p>Contingency Planning (CP) CONTINGENCY PLANNING POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: <i>organization-defined personnel or roles</i>]:</p> <p>1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and</p> <p>b. Reviews and updates the current:</p> <p>1. Contingency planning policy [Assignment: <i>organization-defined frequency</i>]; and</p> <p>2. Contingency planning procedures [Assignment: <i>organization-defined frequency</i>].</p>	<p> Control Authority Diagram</p> <p> Subject to Authority Association Class</p> <p> Authority Class</p> <p> has authority over Property</p> <hr/> <p> provides access to Property</p> <p> Association[made available by:Alter Ability - provides access to:Entity]Association</p> <p> Access IdentifierClass</p> <p> Access PointClass</p> <p> Association[has opening:Access Point - enters through:Boundary]Association</p> <p> Association[has portal:Access Point - enters into:System]Association</p> <p> Access ComplexityEnumeration</p> <p> Access VectorEnumeration</p> <p> Access Control FailureClass</p> <p> Association[traversed using:Entry Action - enters through:Access Point]Association</p> <p> Association[Exit Action - exit through:Access Point]Association</p> <hr/> <p> security levelProperty</p> <p> Communications Security LevelClass</p> <p> security levelProperty</p>	<p>This control area (Contingency Planning (CP)) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and Assessment areas of the Threat and Risk Conceptual Model[Conceptual reference model]. The Control Authority, Asserting Policy and Assessment Package of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES.</p>

	<p> Security Danger Class</p> <hr/> <p> Asserting Policy Association</p> <p> Policy Diagram</p> <p> policy Class</p> <hr/> <p> Assessment Package</p> <p> Assessment Diagram</p> <p> has assessment Property</p> <p> Assessment Activity Class</p> <p> Assessment Report Class</p> <p> assessment of Property</p> <p> assessment score Property</p> <hr/> <p> Incident Package</p> <p> Incident Diagram</p> <p> Incident Class</p> <hr/> <p> processes Package</p> <p> process and plans Diagram</p> <p> Process and plans Process and plansElement Value</p> <p> Process and plans Process and plansElement Value</p> <p> Invoke Process Class</p>	
<p>Identification and Authentication (IA)</p> <p>IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: <p>1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p>	<p> Control Authority Diagram</p> <p> Subject to Authority Association Class</p> <p> Authority Class</p> <p> has authority over Property</p> <hr/> <p> provides access to Property Association[made available]</p>	<p>Identification and Authentication (IA) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning, and Contact Information of the Threat and Risk Conceptual ModelConceptual reference model. The Contact Information, Control Authority, Asserting Policy Package of classes and properties addresses the responsibility, information and coordination among organizational entities for the IDENTIFICATION AND</p>

<p>2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and</p> <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Identification and authentication policy [Assignment: organization-defined frequency]; and 2. Identification and authentication procedures [Assignment: organization-defined frequency]. 	<p>by:Alter Ability - provides access to:Entity Association</p>  <p>Access IdentifierClass</p> <p>Access PointClass</p> <hr/> <p>/ Association[has opening:Access Point - enters through:Boundary] Association</p>  <p>Association[has portal:Access Point - enters into:System] Association</p>  <p>Access Complexity Enumeration</p>  <p>Access Vector Enumeration</p>  <p>Access Control FailureClass</p> <hr/> <p>/ Association[traversed using:Entry Action - enters through:Access Point] Association</p>  <p>Association[Exit Action - exit through:Access Point] Association</p> <hr/> <p> security level Property</p>  <p>Communications Security Level Class</p> <p> security level Property</p>  <p>Security Danger Class</p> <hr/> <p>Asserting Policy Association</p>  <p>Policy Diagram</p>  <p>Policy Class</p> <hr/> <p> processes Package</p>  <p>process and plans Diagram</p> <p> process and plans Process and plansElement Value</p> <p> process and plans Process and plansElement Value</p>  <p>Invoke Process Class</p> <hr/> <p> Contact Information Package</p>	<p>AUTHENTICATION POLICY AND PROCEDURES.</p>
--	--	---

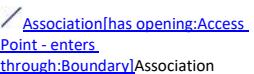
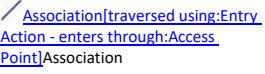
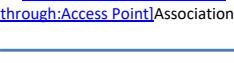
	 Contact Information Diagram  Contact Information Association Class  Contact Means Class  contact for Property  Contactable Class  contact via Property	
Incident Response (IR) Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined frequency].	 Control Authority Diagram  Subject to Authority Association Class  Authority Class  has authority over Property <hr/>  provides access to Property  Association[made available by:Alter Ability - provides access to Entity]Association  Access Identifier Class  Access Point Class  Association[has opening:Access Point - enters through:Boundary]Association  Association[has portal:Access Point - enters into:System]Association  Access Complexity Enumeration  Access Vector Enumeration  Access Control Failure Class  Association[traversed using:Entry Action - enters through:Access Point]Association  Association[Exit Action - exit through:Access Point]Association <hr/>  security level Property	Incident Response (IR) of the 800.53 controls maps to the packages, Control Authority , Provides Access , Security Level , Asserting Policy , Process and Planning , and Incident, Situation areas of the Threat and Risk Conceptual Model . The Contact Information , Control Authority , Asserting Policy Package of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the

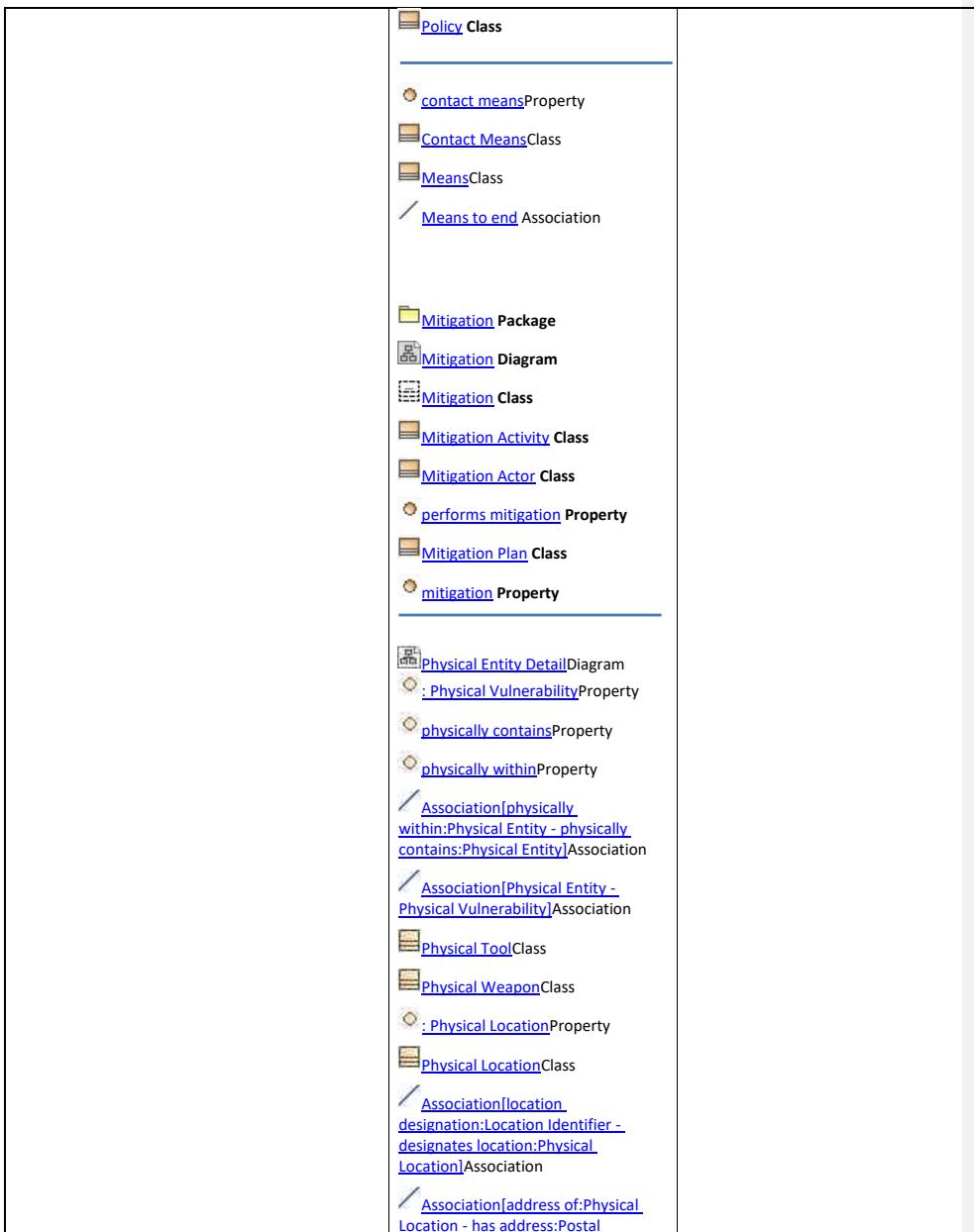
	<p> Communications Security Level Class</p> <p> security level Property</p> <p> Security Danger Class</p> <hr/> <p> Asserting Policy Association</p> <p> Policy Diagram</p> <p> policy Class</p> <hr/> <p> Incident Package</p> <p> Incident Diagram</p> <p> Incident Class</p> <hr/> <p> Situation Package</p> <p> Situation Diagram</p> <p> Situation Classification Generalization Set</p> <p> Situation Class</p> <p> Actual Situation Class</p> <p> Current Situation Class</p> <p> Past Situation Class</p> <p> Potential Situation Class</p> <p> Risky Situation Class</p>	
<p>Maintenance (MA)</p> <p>SYSTEM MAINTENANCE POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and <p>b. Reviews and updates the current:</p>	<p> Control Authority Diagram</p> <p> Subject to Authority Association Class</p> <p> Authority Class</p> <p> has authority over Property</p> <hr/> <p> provides access to Property</p> <p> Association[made available by:Alter Ability - provides access to:Entity] Association</p> <p> Access Identifier Class</p>	<p>This control area (Maintenance (MA)) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and Mitigation Package of the Threat and Risk Conceptual ModelConceptual reference model. The Mitigation, Situation, Process plan and Policy Packages of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the SYSTEM MAINTENANCE POLICY AND PROCEDURES.</p>

<p>1. System maintenance policy [<i>Assignment: organization-defined frequency</i>]; and</p> <p>2. System maintenance procedures [<i>Assignment: organization-defined frequency</i>].</p>	<p> Access PointClass</p> <p> Association[has opening:Access Point - enters through:Boundary]Association</p> <p> Association[has portal:Access Point - enters into:System]Association</p> <p> Access ComplexityEnumeration</p> <p> Access VectorEnumeration</p> <p> Access Control FailureClass</p> <p> Association[traversed using:Entry Action - enters through:Access Point]Association</p> <p> Association[Exit Action - exit through:Access Point]Association</p> <hr/> <p> security levelProperty</p> <p> Communications Security LevelClass</p> <p> security levelProperty</p> <p> Security DangerClass</p> <hr/> <p>Asserting Policy Association</p> <p> Policy Diagram</p> <p> Policy Class</p> <hr/> <p> Mitigation ActorClass</p> <p> performs mitigationProperty</p> <p> Association[mitigated by:Mitigation Actor - performs mitigation:Safeguard Activity]Association</p> <p> Association[countermeasure for:Risk Mitigation Strategy - leverages countermeasure:Countermeasure]Association</p> <p> Risk Mitigation StrategyClass</p>
---	---

	<p>Situation Package</p> <pre> graph TD SP[Situation Package] --> SD[Situation Diagram] SD --> G[Situation Classification Generalization Set] G --> SC[Situation Class] SC --> ASC[Actual Situation Class] SC --> CSC[Current Situation Class] SC --> PSC[Past Situation Class] SC --> PSCC[Potential Situation Class] SC --> RSC[Risky Situation Class] SC -.-> PPD[Process and plans Diagram] PPD --> PC[Plan Class] PPD --> MPC[Mitigation Plan Class] PPD -.-> PP[plan Property] </pre>	
Media Protection (MP) MEDIA PROTECTION POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy [Assignment: organization-defined frequency]; and 2. Media protection procedures [Assignment: organization-defined frequency].	<pre> graph TD MP[Media Protection (MP)] --> CAD[Control Authority Diagram] CAD --> SAAC[Subject to Authority Association Class] SAAC --> AC[Authority Class] AC --> HAO[has authority over Property] HAO -.-> PAO[provides access to Property] PAO --> AAAC[Association[made available by Alter Ability - provides access to Entity]] AAAC --> AIAC[Access Identifier Class] AIAC --> APC[Access Point Class] APC -.-> HAAP[Association[has opening:Access Point - enters through:Boundary]] HAAP -.-> HAPS[Association[has portal:Access Point - enters into:System]] HAPS --> ACE[Access Complexity Enumeration] HAPS --> ACEV[Access Vector Enumeration] </pre>	This control area (Media Protection (MP)) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning. The Security, Means, Control Authority, Asserting Policy and Mitigation, Package of classes and properties address the responsibility, information and coordination among organizational entities for the MEDIA PROTECTION POLICY AND PROCEDURES .

	<p> Access Control Failure Class</p> <hr/> <p>/ Association [traversed using:Entry Action - enters through:Access Point] Association</p> <p>/ Association [Exit Action - exit through:Access Point] Association</p> <hr/> <p> security level Property</p> <p> Communications Security Level Class</p> <p> security level Property</p> <p> Security Danger Class</p> <hr/> <p>Asserting Policy Association</p> <p> Policy Diagram</p> <p> Policy Class</p> <hr/> <p> processes Package</p> <p> process and plans Diagram</p> <p><input checked="" type="checkbox"/> process and plans Process and plansElement Value</p> <p><input checked="" type="checkbox"/> Process and plans Process and plansElement Value</p> <p> Invoke Process Class</p> <hr/> <p> contact means Property</p> <p> Contact Means Class</p> <p> Means Class</p> <p>/ Means to end Association</p> <hr/> <p> Mitigation Package</p> <p> Mitigation Diagram</p> <p> Mitigation Class</p> <p> Mitigation Activity Class</p> <p> Mitigation Actor Class</p> <p> performs mitigation Property</p>
--	--

	<p> Mitigation Plan Class  mitigation Property</p>	
<p>Physical and Environmental Protection (PE) PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency]. 	<p> Control Authority Diagram  Subject to Authority Association Class  Authority Class  has authority over Property</p> <hr/> <p> provides access to Property  Association[made available by Alter Ability - provides access to Entity] Association  Access Identifier Class  Access Point Class  Association[has opening:Access Point - enters through:Boundary] Association  Association[has portal:Access Point - enters into:System] Association  Access Complexity Enumeration  Access Vector Enumeration  Access Control Failure Class  Association[traversed using:Entry Action - enters through:Access Point] Association  Association[Exit Action - exit through:Access Point] Association</p> <hr/> <p> security level Property  Communications Security Level Class  security level Property  Security Danger Class</p> <hr/> <p> Asserting Policy Association  Policy Diagram</p>	<p>This control area (Physical and Environmental Protection (PE)) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and Physical Entity. The Physical Entity, Means, and Control Authority package of <i>classes and properties</i> address the responsibility, information and coordination among organizational entities for the PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES.</p>



	<p>AddressAssociation</p> <p>/ Association[Physical Location - has coordinate:Coordinate]Association</p> <p>/ Association[Relative Coordinate - relative to:Physical Location]Association</p> <p>/ Association[bounds region:Bounded Topology - bounded by:Physical Location]Association</p> <p>/ Association[relocated by:Relocation - relocates:Physical Entity]Association</p> <p>/ Association[loses via:Relocation - from location:Physical Location]Association</p> <p>/ Association[moved via:Relocation - to location:Physical Location]Association</p> <p>Association[topology of:Physical Location - has topology:Topology]Association</p> <p> Geophysical DangerClass</p> <p> Physical System FailureClass</p> <p> Physical VulnerabilityClass</p> <p> : Physical EntityProperty</p>	
<p>Planning (PL)</p> <p>SECURITY PLANNING POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Security planning policy [Assignment: organization-defined frequency]; and 2. Security planning procedures [Assignment: organization-defined frequency]. 	<p> Control Authority Diagram</p> <p> Subject to Authority Association Class</p> <p> Authority Class</p> <p> has authority over Property</p> <hr/> <p> provides access to Property</p> <p>/ Association[made available by:Alter Ability - provides access to:Entity]Association</p> <p> Access IdentifierClass</p> <p> Access PointClass</p> <p>/ Association[has opening:Access Point - enters through:Boundary]Association</p>	<p>This control area Planning (PL) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and Mitigation and (Methods of Contact) and Assessment areas of the Threat and Risk Conceptual ModelConceptual reference model. The Security, Mitigation, Means, Control Authority, Asserting Policy and Assessment Package of <i>classes and properties</i> address the responsibility, information and coordination among organizational entities for the SECURITY PLANNING POLICY AND PROCEDURES.</p>

	<p>Association[has portal:Access Point - enters into:System]Association</p> <p>Access ComplexityEnumeration</p> <p>Access VectorEnumeration</p> <p>Access Control FailureClass</p> <p>Association[traversed using:Entry Action - enters through:Access Point]Association</p> <p>Association[Exit Action - exit through:Access Point]Association</p> <hr/> <p>security levelProperty</p> <p>Communications Security LevelClass</p> <p>security levelProperty</p> <p>Security DangerClass</p> <p>Asserting Policy Association</p> <p>Policy Diagram</p> <p>Policy Class</p> <hr/> <p>processesPackage</p> <p>Process and plansDiagram</p> <p>Process and plans Process and plansElement Value</p> <p>Process and plans Process and plansElement Value</p> <p>Invoke ProcessClass</p> <hr/> <p>Mitigation Package</p> <p>Mitigation Diagram</p> <p>Mitigation Class</p> <p>Mitigation Activity Class</p> <p>Mitigation Actor Class</p> <p>performs mitigation Property</p>
--	---

	<p> Mitigation Plan Class  mitigation Property</p> <hr/>	
Personnel Security (PS) PERSONNEL SECURITY POLICY AND PROCEDURES Control: The organization:	<p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Personnel security policy [Assignment: organization-defined frequency]; and 2. Personnel security procedures [Assignment: organization-defined frequency]. <p> Control Authority Diagram  Subject to Authority Association Class  Authority Class  has authority over Property</p> <hr/> <p> provides access to Property  Association[made available by:Alter Ability - provides access to:Entity]Association  Access IdentifierClass  Access PointClass  Association[has opening:Access Point - enters through:Boundary]Association  Association[has portal:Access Point - enters into:System]Association  Access ComplexityEnumeration  Access VectorEnumeration  Access Control FailureClass  Association[traversed using:Entry Action - enters through:Access Point]Association  Association[Exit Action - exit through:Access Point]Association</p> <hr/> <p> security levelProperty  Communications Security LevelClass  security levelProperty  Security DangerClass</p> <hr/> <p>Asserting Policy Association</p>	<p>This control area Personnel Security (PS) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and Security Levels, Person Identifiers Means, Assessment areas of the Threat and Risk Conceptual Model[Conceptual reference model]. The Security, Person Identifiers, Means, Control authority, Mitigation, Situation, Process plan and Policy Packages of classes and properties addresses the responsibility, information and coordination among organizational entities for the PERSONNEL SECURITY POLICY AND PROCEDURES.</p>

	<p> Policy Diagram</p> <p> Policy Class</p> <hr/> <p> processes Package</p> <p> Process and plans Diagram</p> <p><input checked="" type="checkbox"/> Process and plans Process and plansElement Value</p> <p><input checked="" type="checkbox"/> Process and plans Process and plansElement Value</p> <p> Invoke Process Class</p> <hr/> <p> Person Identifiers Diagram</p> <p> Person at location Association Class</p> <p> Managed Person Identifier Class</p> <p> person Class</p> <p> location of person Property</p> <hr/> <p> Mitigation Package</p> <p> Mitigation Diagram</p> <p> Mitigation Class</p> <p> Mitigation Activity Class</p> <p> Mitigation Actor Class</p> <p> performs mitigation Property</p> <p> Mitigation Plan Class</p> <p> mitigation Property</p>	
<p>Risk Assessment (RA)</p> <p>RISK ASSESSMENT POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <p>1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p>	<p> Control Authority Diagram</p> <p> Subject to Authority Association Class</p> <p> Authority Class</p> <p> has authority over Property</p> <hr/>	<p>This control area (Risk Assessment (RA)) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and Risk. The Risk, Security, Means, Control authority, Mitigation, Situation, Process plan and Policy Packages of classes and properties addresses the responsibility, information and coordination among organizational entities for the RISK ASSESSMENT POLICY AND PROCEDURES.</p>

<p>2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and</p> <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. Risk assessment policy [Assignment: organization-defined frequency]; and 2. Risk assessment procedures [Assignment: organization-defined frequency]. 	<ul style="list-style-type: none"> provides access to Property Association[made available by:Alter Ability - provides access to:Entity] Association Access Identifier Class Access Point Class Association[has opening:Access Point - enters through:Boundary] Association Association[has portal:Access Point - enters into:System] Association Access Complexity Enumeration Access Vector Enumeration Access Control Failure Class Association[traversed using:Entry Action - enters through:Access Point] Association Association[Exit Action - exit through:Access Point] Association <hr/> <ul style="list-style-type: none"> security level Property Communications Security Level Class security level Property Security Danger Class <hr/> <p>Asserting Policy Association</p> <ul style="list-style-type: none"> Policy Diagram Policy Class <hr/> <ul style="list-style-type: none"> processes Package process and plans Diagram process and plans Process and plansElement Value process and plans Process and plansElement Value Invoke Process Class
--	--

	<ul style="list-style-type: none"> Risk and Threat Concepts Package Transfer Risk Class Risk Treatment Package Risk Treatment Diagram Risk Treatment Option Class risk level accepted Property Risky Situation Class risk owner Property risk to Property <hr/> <ul style="list-style-type: none"> security level Property Communications Security Level Class security level Property Security Danger Class <hr/> <ul style="list-style-type: none"> Mitigation Package Mitigation Diagram Mitigation Class Mitigation Activity Class Mitigation Actor Class performs mitigation Property Mitigation Plan Class mitigation Property 	
System and Services Acquisition (SA) SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles] : 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Control Authority Diagram Subject to Authority Association Class Authority Class has authority over Property <hr/> provides access to Property	This control area (System and Services Acquisition (SA)) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and System . The Person Identifiers, Means, Control authority, Mitigation, Situation, Process plan and Policy Packages of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the SYSTEM AND SERVICES ACQUISITION POLICY AND

<p>2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and</p> <p>b. Reviews and updates the current:</p> <p>1. System and services acquisition policy [Assignment: organization-defined frequency]; and</p> <p>2. System and services acquisition procedures [Assignment: organization-defined frequency].</p>	<p>/Association[made available by:Alter Ability - provides access to:Entity]Association</p> <p> Access IdentifierClass</p> <p> Access PointClass</p> <p>/Association[has opening:Access Point - enters through:Boundary]Association</p> <p>/Association[has portal:Access Point - enters into:System]Association</p> <p> Access ComplexityEnumeration</p> <p> Access VectorEnumeration</p> <p> Access Control FailureClass</p> <p>/Association[traversed using:Entry Action - enters through:Access Point]Association</p> <p>/Association[Exit Action - exit through:Access Point]Association</p> <hr/> <p> security levelProperty</p> <p> Communications Security LevelClass</p> <p> security levelProperty</p> <p> Security DangerClass</p> <p>Asserting Policy Association</p> <p> Policy Diagram</p> <p> Policy Class</p> <hr/> <p> processesPackage</p> <p> Process and plansDiagram</p> <p> Process and plans Process and plansElement Value</p> <p> Process and plans Process and plansElement Value</p> <p> Invoke ProcessClass</p> <hr/> <p> System Package</p>	<p>PROCEDURES.</p>
---	--	---------------------------

	<p> System Diagram</p> <p> System Class</p> <p> has subsystem Property</p> <p> Subsystem Association</p> <hr/> <p> security level Property</p> <p> Communications Security Level Class</p> <p> security level Property</p> <p> Security Danger Class</p> <hr/> <p> Process and plans Diagram</p> <p> Plan Class</p> <p> Mitigation Plan Class</p> <p> plan Property</p>	
<p>System and Communications Protection (SC)</p> <p>SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> 1. System and communications protection policy [Assignment: organization-defined frequency]; and 2. System and communications protection procedures [Assignment: organization-defined frequency]. 	<p> Control Authority Diagram</p> <p> Subject to Authority Association Class</p> <p> Authority Class</p> <p> has authority over Property</p> <hr/> <p> provides access to Property</p> <p> Association[made available by:Alter Ability - provides access to:Entity] Association</p> <p> Access Identifier Class</p> <p> Access Point Class</p> <p> Association[has opening:Access Point - enters through:Boundary] Association</p> <p> Association[has portal:Access Point - enters into:System] Association</p> <p> Access Complexity Enumeration</p> <p> Access Vector Enumeration</p>	<p>This control area System and maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and I. The Risk, Security, Means, Control authority, Mitigation, Situation, Process plan and Policy Packages of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the RISK ASSESSMENT POLICY AND PROCEDURES.</p>

<p> Access Control Failure Class</p> <hr/> <p> Association [traversed using:Entry Action - enters through:Access Point] Association</p> <hr/> <p> Association [Exit Action - exit through:Access Point] Association</p> <hr/> <p> security level Property</p> <p> Communications Security Level Class</p> <p> security level Property</p> <p> Security Danger Class</p> <hr/> <p>Asserting Policy Association</p> <p> Policy Diagram</p> <p> Policy Class</p> <hr/> <p> processes Package</p> <p> process and plans Diagram</p> <p> process and plans Process and plansElement Value</p> <p> Process and plans Process and plansElement Value</p> <p> Invoke Process Class</p> <hr/> <p> System Package</p> <p> System Diagram</p> <p> System Class</p> <p> has subsystem Property</p> <hr/> <p> Subsystem Association</p> <hr/> <p> Risks Package</p> <p> Risk Diagram</p> <p> Risk Metrics Diagram</p> <p> Accept Risk Class</p> <p> Risk Treatment Risk TreatmentElement Value</p>	
--	--

	<p> Risk Treatment Risk Treatment Element Value risk level accepted Property :Risk Owner Property</p> <hr/> <p> Mitigation Package Mitigation Diagram Mitigation Class Mitigation Activity Class Mitigation Actor Class performs mitigation Property Mitigation Plan Class mitigation Property</p> <hr/> <p> Means Class Means to end Association Process and plans Diagram Plan Class Mitigation Plan Class plan Property</p>	
System and Information Integrity (SI) SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [Assignment: organization-defined frequency]; and 2. System and information integrity procedures	Control Authority Diagram Subject to Authority Association Class Authority Class has authority over Property <hr/> provides access to Property Association[made available by:Alter Ability - provides access to:Entity] Association Access Identifier Class Access Point Class Association[has opening:Access Point - enters through:Boundary] Association	This control area (System and Information Integrity(SI)) of the 800.53 controls maps to the packages, Control Authority , Provides Access , Security Level , Asserting Policy , Process and Planning and System , of the Threat and Risk Conceptual Model . The Risk, Security, Means, Control authority, Mitigation, Situation, Process plan and Policy Packages of classes and properties addresses the responsibility, information and coordination among organizational entities for the SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES .

<p>[Assignment: organization-defined frequency].</p> <hr/> <p> Association[has portal:Access Point - enters into:System]Association</p> <p> Access ComplexityEnumeration</p> <p> Access VectorEnumeration</p> <p> Access Control FailureClass</p> <hr/> <p> Association[traversed using:Entry Action - enters through:Access Point]Association</p> <hr/> <p> Association[Exit Action - exit through:Access Point]Association</p> <hr/> <p> security levelProperty</p> <p> Communications Security LevelClass</p> <p> security levelProperty</p> <p> Security DangerClass</p> <hr/> <p>Asserting Policy Association</p> <p> Policy Diagram</p> <p> Policy Class</p> <hr/> <p> processes Package</p> <p> Process and plans Diagram</p> <p> Process and plans Process and plansElement Value</p> <p> Process and plans Process and plansElement Value</p> <p> Invoke ProcessClass</p> <hr/> <p> System Package</p> <p> System Diagram</p> <p> System Class</p> <p> has subsystem Property</p> <hr/> <p> Subsystem Association</p> <hr/> <p> security level Property</p>	
--	--

	<p> Communications Security Level</p> <p>Class</p> <ul style="list-style-type: none"> security level Property <p> Security Danger Class</p> <hr/> <p> Process and plans Diagram</p> <p> Plan Class</p> <p> Mitigation Plan Class</p> <ul style="list-style-type: none"> plan Property <hr/> <p> Risks Package</p> <p> Risk Diagram</p> <p> Risk Metrics Diagram</p> <p> Accept Risk Class</p> <p> Risk Treatment Risk TreatmentElement Value</p> <p> Risk Treatment Risk TreatmentElement Value</p> <ul style="list-style-type: none"> risk level accepted Property :Risk Owner Property 	
<p>Program Management (PM)</p> <p>INFORMATION SECURITY PROGRAM PLAN</p> <p>Control: The organization:</p> <ol style="list-style-type: none"> Develops and disseminates an organization-wide information security program plan that: <ol style="list-style-type: none"> Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, 	<p> Control Authority Diagram</p> <p> Subject to Authority Association</p> <p>Class</p> <p> Authority Class</p> <ul style="list-style-type: none"> has authority over Property <hr/> <ul style="list-style-type: none"> provides access to Property <p> Association[made available by:Alter Ability - provides access to:Entity] Association</p> <p> Access Identifier Class</p> <p> Access Point Class</p> <p> Association[has opening:Access Point - enters through:Boundary] Association</p> <p> Association[has portal:Access Point - enters into:System] Association</p>	<p>This control area (Program Management (PM)) of the 800.53 controls maps to the packages, Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and Risk of the Threat and Risk Conceptual Model. The Process plan, System, Resources, Security, Means, Control authority, Mitigation, Situation, Risk, and Policy Packages of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the INFORMATION SECURITY PROGRAM PLAN.</p>

<p>functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [Assignment: organization-defined frequency];</p> <p>c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and</p> <p>d. Protects the information security program plan from unauthorized disclosure and modification.</p>	<p> Access Complexity Enumeration Access Vector Enumeration Access Control Failure Class Association[traversed using:Entry Action - enters through:Access Point] Association Association[Exit Action - exit through:Access Point] Association</p> <hr/> <p> security level Property Communications Security Level Class security level Property Security Danger Class</p> <hr/> <p>Asserting Policy Association Policy Diagram Policy Class</p> <hr/> <p> processes Package process and plans Diagram <input checked="" type="checkbox"/> process and plans Process and plansElement Value <input checked="" type="checkbox"/> Process and plans Process and plansElement Value Invoke Process Class Process and plans Diagram Plan Class Mitigation Plan Class plan Property</p> <hr/> <p>w System Package System Diagram System Class has subsystem Property Subsystem Association</p>	
--	--	--

	<ul style="list-style-type: none">  Resources Package  Resource Diagram  Resource Class  harmed resource Property <hr/> <ul style="list-style-type: none"> Risk and Threat Concepts Package  Transfer Risk Class Risk Treatment Package  Risk Treatment Diagram <hr/> <ul style="list-style-type: none">  Mitigation Package  Mitigation Diagram  Mitigation Class  Mitigation Activity Class  Mitigation Actor Class  performs mitigation Property  Mitigation Plan Class  mitigation Property <hr/> <ul style="list-style-type: none"> security level Property  Communications Security Level Class  security level Property  Security Danger Class <hr/> <ul style="list-style-type: none"> Control Authority Diagram  Subject to Authority Association Class  Authority Class  has authority over Property
--	---

13 Concept Index

[Ability](#), 148
[Ability To Execute Software](#), 193
[Absorbed Dose \(Radiation\)](#), 310
[Abuse Resource](#), 319
[Acceleration](#), 311
[Accept Risk](#), 92
[Access Complexity](#), 133
[Access Control Failure](#), 64
[Access Identifier](#), 265
[Access Point](#), 338
[Access Vector](#), 134
[Accident](#), 73
achieves, 240, 241
[Activity](#), 210
[Activity Effecting Entity](#), 299
[Activity Map Rule](#), 391
[Actor](#), 210
[Actor Identifier of Credential](#), 185
[Actual Activity](#), 212
[Actual Event](#), 212
[Actual State](#), 326
[ActualObservableFacade](#), 368
[Add Information](#), 221
[Add To Container Event](#), 172
[Address Map Rule](#), 396
address of, 163, 230
[Address of Location](#), 229
[Adjacent](#), 134
[Affected Available Resource](#), 149
affected by, 328
affected by action, 150, 321
[AffectedAssetFacade](#), 368
affects, 328
affects control of, 150
affords, 152

[Alter Ability](#), 150
altitude, 233
[Amount of Substance](#), 311
[AND Condition](#), 296
[Angle](#), 311
[Animal](#), 271
[Area](#), 311
area code, 167
[Area Map Rule](#), 413
asserted by, 283, 284
[Assertion of Policy](#), 282
asserts policy, 179, 283
assessed by, 155, 157
[Assessed Entity](#), 155
assesses, 156, 157
[Assessment](#), 156
[Assessment Activity](#), 156
[Assessment Map Rule](#), 394
assessment score, 156
associate, 335, 336
[Associated Actor](#), 334
associated with, 335, 336
[Assume Risk](#), 103
assumes risk from, 104, 108
[Atomic Information Object](#), 222
[Attack](#), 58
attack target, 58, 59
attacked by, 59, 320
[Attest to Ability](#), 186
attests to, 186, 187
[Authentication](#), 135
[Authority](#), 179
automated by, 194, 210
[Automated Capability](#), 194
[Automated Control](#), 194

Formatted: Number of columns: 2

[Automated Entity](#), 195
[automates](#), 194, 195, 197, 198
[Automation Type](#), 196
[Automaton](#), 196
[availability](#), 161
[Availability Impact](#), 135
[Avoid Danger](#), 104
[Benefit](#), 237
[Biological Danger](#), 65
[birth date](#), 272
[Blacklist Indicator](#), 84
[Boundary](#), 338
[Boundary of System](#), 338
[bounded by](#), 231, 234
[bounds](#), 338, 339
[bounds topology](#), 231, 232
[call sign](#), 165
[Campaign](#), 55
[can be utilized by](#), 149, 321
[can execute](#), 193, 199
[Capability](#), 151
[Capture Resource](#), 319
[Catastrophic](#), 100
[Cause and Effect](#), 326
[caused by](#), 79, 80, 327
[causes](#), 327
[causes harm](#), 120, 121
[CBRN Danger](#), 65
[channel](#), 165
[Chemical Danger](#), 65
[city ID](#), 164
[Civil Unrest Danger](#), 65
[Client](#), 358
[Close Information](#), 222
[Collateral Damage Potential](#), 136
[Color](#), 311
[communicates via](#), 196, 200
[Communicating Device](#), 196
[Communications Link](#), 196
[Communications Network](#), 197
[Communications Security Level](#), 160
[Communications Vulnerability](#), 128
[Complete](#), 136, 137, 139
[Compliance Impact](#), 65
[Composite Condition](#), 296
[Computer Control System](#), 197
[Computer System](#), 197
[Concentration](#), 312
[Concentration \(amount of substance\)](#), 312
[Concentration \(Mass\)](#), 312
[Concentration \(Volume\)](#), 312
[condition for](#), 125, 126
[confidence](#), 89
[Confidence](#), 222
[confidence about](#), 222, 223
[Confidence in Assertion](#), 222
[confidence metric](#), 222
[Confidence Metric](#), 304
[Confidentiality Impact](#), 137
[Confirmed](#), 140
[Consequence](#), 237
[Consequence of Situation](#), 239
[Contact Availability](#), 168
[contact for](#), 160, 161
[Contact Information Mapping Rule](#), 397
[Contact Means](#), 160
[Contact Purpose](#), 168
[contact via](#), 161, 162
[Contact Via](#), 160
[Contactable](#), 161
[Contained Information](#), 223
[Container](#), 172
[Containment](#), 173
[Containment Event](#), 174

contains, 172, 173	Custodian, 181
contains information, 223, 227	Custody, 181
context of observation, 247	CVE Identifier, 129
Context of Observation, 247	CVSS Score, 133
contributes to, 74	Cyber Danger, 66
Contribution to Danger, 74	Cyber Resource, 198
contributor, 74, 122	Cyber System Failure, 66
Control, 179	Cyber Vulnerability, 129
Control Failure, 65	Cyber Weapon, 198
Controlled Entity, 180	Damage, 299
Controlling Actor, 181	Damage Resource, 319
Conveyance, 272	Danger Category, 66
Coordinate, 217	Danger Leads to Incident, 78
Coordinate Map Rule, 413	Danger Source, 74
Coordinate of location, 230, 234	Dangerous Condition, 74
Coordinate System, 218	Dangerous Event, 75
coordinate within system, 218	Date and Time, 345
Count, 304	Date Coordinate, 345
Countermeasure, 104	Date Time Coordinate (ISO 8601), 355
countermeasure for, 104, 105	day, 168
Countermeasure for Strategy, 105	death date, 272
Countermeasure Mitigates, 105	Decision-making Impact, 66
Country, 258	degree of affect, 238
country code, 167	degree of mitigation, 109
country ID, 164	Delete Information, 224
Country ID, 259	DeliveryPoint, 386
county ID, 164	depends on, 321, 322
Create, 299	designates location, 230, 231
Create Information, 224	Designation of a Location, 230
creates process instance, 290, 293	desirability, 238
Credential, 187	Desirability Assessment, 240
credential identifier, 185, 187	desirability for, 245
Criminal Danger, 66	desirability of, 244, 245
Critical, 101	Destroy, 300
Currency, 312	Device, 273
Currency Benefit Metric, 304	device address, 276
Current Situation, 327	direction, 233

Disinformation Impact, 66
Disrupt Process, 300
Disrupt Stakeholder's Objective, 75
Disruptive Action, 113
distance, 233
Document, 224
document capable, 162
Dose Equivalent (Radiation), 313
Duration, 313
duration of, 313, 345
Duration of Entity, 345
Effect, 328
Electric Current, 313
Electric Potential, 314
Electromagnetic Spectrum Impact, 66
electronic address, 163, 168
Electronic Contact, 162
elevation, 235
Email Address, 162
emergency, 168
enactement of, 213, 290
Energy, 314
Enterprise, 202
enters into, 338, 341
enters through, 300
Entity Assessment, 156
Entity Exists for Interval, 346
Entiy Map Rule, 401
Entry Action, 300
Environmental Impact, 67
evening, 168
Event, 213
Exceed Resource Capacity, 320
executed by, 193, 200
Execution Platform, 198
exists for, 346
Exit Action, 300
exit through, 300
Exit via, 338
Exploit of Vulnerability, 75
Exploitability, 137
exploited by, 76, 126
exploits, 74, 76
ExploitTargetFacade, 368
Facilitator, 151
Facility, 278
Facility Map Rule, 414
Failure, 79
Failure Category, 67
failure of, 79, 80
Failure of Resource, 80
fax capable, 162
Female, 276
filled by, 173, 175
Financial Identifier, 265
Financial Impact, 67
finish of, 347
Finish Time, 346
finishes at, 347
Fire Danger, 67
Force, 314
Frequency, 314
Frequent, 100
Functional, 138
Geophysical Danger, 67
Geopolitical Entity, 259
Geopolitical ID, 259
Geopolitical Region, 260
given name, 268
Governing Authority, 260
governs region, 259, 260
granularity of, 313, 353
happens during, 350
Harm, 117

harm from, 118, 120
Harm-Benefit Metric, 304
harmed by, 119, 320
harms, 119, 121
Harms Resource, 118
harms victim, 120, 121
Harms Victim, 119
has ability to execute, 151, 211
has ability to utilize, 149, 211
has address, 229, 232
has authority over, 179, 184
has boundary, 339, 342
has capable performer, 151, 210
has child organization, 254
has condition, 121, 125
has confidence, 223
has consequence, 239
has control over, 180, 181
has control system, 195
has coordinate, 230, 232
has credential, 149, 186
has custody of, 181, 182
has duration, 345
has failure, 80, 320
has granularity, 352
has indicator, 332
has leader, 182, 253
has location designation, 230, 232
has member, 252, 253
has member time Point, 352, 353
has nodes, 197, 200
has objective, 243, 244
has opening, 338, 340
has parent organization, 253, 254
has part, 207
has permission to perform, 212, 262
has portal, 341, 342
has product Line, 361, 363
has relative location, 232, 233
has resident, 269, 281
has risk of harm, 96, 321
has risk to objectives, 95, 98
has scope, 85, 332
has sighting, 85, 89
has state, 332
has subprocess, 292, 293
has temporal part, 350
has topology, 232, 234
has vulnerability, 127, 320
Health Impact, 67
height, 273
High, 133, 137, 138, 141, 142, 306, 308
Identification Map Rule, 404
Identity Provider, 187
Identity Theft, 68
Image Impact, 68
Impact, 205
Impact Category, 68
impact measure, 238
impacted by, 206
impacts, 206
importance, 243
Impose Strategy, 92
imposed by, 93, 110
imposes, 93, 95
Improbable, 100
in the custody of, 182, 183
Inability to Communicate Impact, 68
Incident, 80
Incident Map Rule, 405
incorporated by, 256, 257
Incorporated Organization, 256
incorporates, 257, 259
Incorporation, 257

indicated by, 88
indicates, 87, 88
indicates situation, 84, 85
Indicator, 84
Indicator Indicates Situation, 85
Indicator Pattern, 86
Indicator Watchlist, 86
Indirect Threat, 58
Individual Product, 359
Industrial Control Failure, 68
Information Action, 224
Information Impact, 68
Information In Computer, 199
Information Loss Impact, 69
Information Object, 225
Information Repository, 225
Information Resource, 225
Information System Vulnerability, 129
Information Type, 226
Information Vulnerability, 129
Infrastructure Impact, 69
initiates, 293, 295
Injury Map Rule, 408
Integrity Impact, 138
Intellectual Property Impact, 69
Internet Contact, 163
Internet Contact Map Rule, 398
interval of, 346, 351
Invoke Process, 290
involved in, 212, 329
Involvement, 328
involves, 329
is after, 349
is before, 349
is controlled by, 180
is governed by, 260
is in, 173
is in information structure, 223, 225
is part of, 207
is possessed by, 180, 184
is stored in, 199, 225
is subject to authority, 180, 184
Issue Credential, 188
issued by, 187, 188
issues credential, 187, 188
Item, 273
Item Map Rule, 410
latitude, 235
Leader, 182
Leadership, 182
leads, 182
leads to, 75, 79
Legal Impact, 69
length, 273
Length, 315
leveraged by, 126, 144
leverages, 144
leverages countermeasure, 94, 105
License Identifier, 335
likelihood, 74, 86, 88, 119, 286, 293, 331
Likelihood Categories, 99
line, 167
Local, 134
Local Identifier, 335
located person, 232, 267
Location ID, 230
Location Identifier, 230
Location Map Rule, 415
location of, 279, 280
location of person, 266, 267
longitude, 235
loses control, 152, 154
Lose Ability, 152
Loss of Control Danger, 69

[lost by](#), 154, 211
[lost via](#), 180
[Low](#), 133, 136, 141, 306, 308
[Low-Medium](#), 136
[Luminosity](#), 315
[Male](#), 276
[Managed Actor Identifier](#), 188
[Managed Entity](#), 182
[Managed Item Identifier](#), 273
[Managed Person Identifier](#), 266
[Managed Social Agent Identifier](#), 335
[Manufactured Thing](#), 359
[Marginal](#), 101
[Mass](#), 315
[Mass Density](#), 315
[matches indicator](#), 87, 89
[may be performed by](#), 210, 262
[may entail risk](#), 97, 122
[Means](#), 240
[Means To End](#), 241
[Measurement](#), 247
[measures risk of](#), 94, 97
[measures risk to](#), 94, 96
[Medium](#), 133, 141, 308
[Medium High](#), 136
[Medium](#), 142
[member of](#), 252, 336
[Membership](#), 251
[Meteorological Danger](#), 69
[Metric](#), 304
[middle name](#), 268
[Mission Impact](#), 70
[Mission Objective](#), 252
[mitigated by](#), 110, 111
[mitigates](#), 104, 106
[Mitigation Actor](#), 106
[mobile](#), 162
[Moderate](#), 306
[modified by](#), 94, 109
[modifies risk](#), 109
[Modify Information](#), 226
[Modify Resource](#), 320
[Modus Operandi](#), 290
[Monitor](#), 106
[monitored by](#), 85, 107
[Monitoring Safeguard](#), 107
[Multiple](#), 135
[name part](#), 268
[name suffix](#), 268
[Natural Threat](#), 58
[negate](#), 297
[negated by](#), 330
[negates](#), 330
[negation](#), 86
[Negation Effect](#), 329
[Negligible](#), 101
[net benefit](#), 240
[net desirability](#), 240
[net likelihood](#), 240
[net risk](#), 240
[net severity](#), 240
[network address](#), 198
[Network Identifier](#), 163
[night](#), 168
[Node of a Network](#), 199
[None](#), 135, 136, 137, 138, 141
[Non-Technical Impact](#), 70
[Nuclear Danger](#), 70
[number observed](#), 249
[Object Management Group, Inc. \(OMG\)](#), 21
[Objective](#), 241
[Objective for Safety and Security](#), 93
[objective of](#), 242, 243
[Objective of Stakeholder](#), 243

Objective to Disrupt, 76
Objective to Protect Assets, 93
Observability, 248
ObservablePatternFacade, 368
Observation, 248
Observation Tool, 249
observed by, 249
observed in context, 247, 249
Observer, 249
observes, 249, 250
Obtain Ability, 152
obtained by, 153, 212
obtained via, 180
obtains control, 152, 153
Occasional, 100
Offical Fix, 139
official given name, 268
OMG specifications, 21
Open Information, 226
Opening in a Boundary, 339
Operating Location, 278
Opportunity, 243
OR Condition, 297
Organization, 253
Organization Map Rule, 417
Organizational Unit, 253
OSVDB Identifier, 130
other, 169
Output, 213
overlaps from, 348
Overlaps in Time, 347
overlaps to, 348
owned by, 183, 184
Owner, 183
Ownership, 183
owns, 183
Parent Organization, 253
Part of Organization, 254
Parthood, 206
Partial, 136, 137, 139
Passport Identifier, 266
Past Situation, 330
pattern indicated by, 86, 331
Pause Process, 300
PentaScale, 306
Performance, 214
performed by, 210, 215
Performer, 320
performs, 212, 215
performs at, 212, 279
performs safeguard, 106, 111
Permission, 262
Perpetrate, 113
perpetrates, 114
perpetrator, 113, 114
Person, 266
Person at location, 267
Person Map Rule, 419
Person Name, 267
Person Name Map Rule, 420
Person Structured Name, 268
personal, 169
PersonInjuryFacade, 387
Physical Boundary, 231
Physical Container, 174
Physical Containment, 174
Physical Entity, 274
Physical Feature, 274
Physical Location, 231
Physical Point, 232
Physical Quantity, 315
physical sex, 272
Physical System Failure, 70
Physical Tool, 274

[Physical Vulnerability](#), 124
[Physical Weapon](#), 143
[physically contains](#), 174
[physically within](#), 174, 275
[Place](#), 279
[place ID](#), 164
[Place of Occurrence](#), 280
[Plan](#), 291
[Point Of Entry](#), 340
[Point On Earth](#), 232
[Policy](#), 283
[possesses](#), 181, 184
[Possession](#), 183
[Possible Actions](#), 301
[post box ID](#), 164
[post code](#), 164
[postal address](#), 165
[Postal Address](#), 163
[Postal Address Facade](#), 385
[Postal Address Structured](#), 163
[Postal Address Text](#), 164
[Postal Code](#), 165
[PostCodeBase](#), 386
[PostCodeSuffix](#), 386
[Potential Situation](#), 331
[Power](#), 316
[predicted by](#), 286, 331
[Prediction](#), 285
[Predictor](#), 286
[predicts](#), 286
[Pressure](#), 316
[previously known](#), 126
[primary](#), 168
[Private Network Contact](#), 165
[Probability Metric](#), 305
[Probable](#), 100
[Process Action](#), 291
[Process Decomposition](#), 291
[Process Failure](#), 70
[Process Pattern](#), 292
[produced](#), 360, 361
[produced by](#), 214, 359, 361
[Producer](#), 359
[produces](#), 213, 214
[Product Kind](#), 360
[product line of](#), 360, 361
[Product Line of Supplier](#), 360
[Production](#), 361
[Program](#), 255
[Proof of concept](#), 138
[Property](#), 184
[protected by](#), 108, 321
[Protection](#), 107
[protects](#), 104, 108
[provided by](#), 358, 362
[provides access through](#), 338, 340
[provides product](#), 362
[provides product to](#), 362, 363
[provides security level](#), 197
[Providing](#), 361
[providing action](#), 359
[publicly known](#), 126
[purpose](#), 161
[put into](#), 172, 175
[Radiation Exposure](#), 316
[Radio Contact](#), 165
[Radio Map Rule](#), 399
[Radioactivity](#), 316
[Radiological Danger](#), 70
[rank](#), 98
[Read Information](#), 226
[realized by](#), 241, 242
[Recieving Container](#), 175
[recipient name](#), 164

[reduce harm via](#), 106, 121
[Reference Point](#), 233
[referenced by credential](#), 186, 189
[region ID](#), 164
[Regional Identifier](#), 335
[Related](#), 207
[related from](#), 208
[relates to](#), 208
[Relative Coordinate](#), 233
[relative to](#), 233
[Relocation](#), 175
[Remediation Level](#), 139
[Remote](#), 100, 134
[Removal Event](#), 175
[remove from](#), 176
[Remove Information](#), 227
[removed by](#), 173, 176
[replacement cost](#), 99
[Report Confidence](#), 140
[required](#), 125
[Residence](#), 280
[Residency](#), 269
[resides at](#), 266, 269
[Resource](#), 320
[Resource Actions](#), 321
[Resource Dependency](#), 322
[results from](#), 239
[revision](#), 359
[revokes permission](#), 262
[Risk](#), 93
[Risk Agent](#), 108
[risk for](#), 94, 98
[risk level accepted](#), 92
[Risk Mitigation Strategy](#), 94
[Risk Owner](#), 94
[Risk Reduction Objective](#), 95
[Risk To Resource](#), 96
[Risk Topic](#), 96
[Risk Treatment](#), 109
[Risk Treatment Strategy](#), 109
[Safeguard Activity](#), 110
[Safeguarding](#), 110
[Safety Danger](#), 71
[Safety Impact](#), 71
[salutation](#), 268
[Scenario](#), 293
[Scope of Indicator](#), 331
[score](#), 126
[secondary](#), 168
[Security Danger](#), 71
[security level](#), 160
[Security Requirements](#), 140
[sensitive to objective](#), 99
[sensitivity threshold](#), 99
[Serial Number](#), 362
[severity](#), 121
[Severity Categories](#), 100
[Sex Kind](#), 276
[Sighting](#), 86
[Sighting Indicates Situation](#), 87
[Sighting Matches Indicator](#), 88
[Single](#), 135
[situated at](#), 280
[Social Agent](#), 336
[Social Network Contact](#), 166
[Social Security Number](#), 269
[Software](#), 200
[Software Vulnerability](#), 130
[Source of Danger Category](#), 71
[Source of Harm](#), 120
[Spacial Coordinate](#), 233
[Spacial Entity](#), 274
[Speed](#), 316
[Stakeholder](#), 244

[Stakeholder Desirability](#), 245
[Stakeholder Risk](#), 97
[standing height](#), 272
[start of](#), 349
[Start Time](#), 348
[starts at](#), 349
[State](#), 332
[state of](#), 332
[State of Entity](#), 332
[state_province ID](#), 164
[STIX Campaign Rule](#), 370
[STIX Categories Rule](#), 371
[STIX Course Of Action Rule](#), 372
[STIX Incident Rule](#), 373
[STIX Indicator Rule](#), 374
[STIX Objective Rule](#), 375
[STIX Observable Rule](#), 376
[STIX Sighting Rule](#), 377
[STIX Statement Rule](#), 378
[STIX Threat Actor Rule](#), 379
[STIX TTP Rule](#), 380
[STIX Vocabulary Rule](#), 381
[STIX Vulnerability Rule](#), 382
[Stop Process](#), 301
[stores information](#), 198, 199
[street ID](#), 164
[Strenthened Actor](#), 152
[Structured Information Object](#), 227
[Subject to Authority](#), 184
[Subsystem](#), 341
[Supplier](#), 363
[Supplying Container](#), 176
[supported by](#), 99
[Supporting Condition](#), 124
[supports](#), 321, 322
[surname](#), 268
[surname prefix](#), 268
[System](#), 341
[System Failure](#), 71
[system of coordinate](#), 217, 218
[System of Coordinate](#), 218
[Target Distribution](#), 141
[Target of Attack](#), 58
[Tax Authority Identifier](#), 336
[Telecommunication Device](#), 275
[Telephone Area Code](#), 166
[Telephone Country Code](#), 166
[telephone exchange](#), 167
[telephone extension](#), 167
[Telephone Map Rule](#), 400
[telephone number](#), 167
[Telephone Number](#), 166
[Telephone Number Facade](#), 386
[Telephone Number Structured](#), 167
[Telephone Number Text](#), 167
[Temperature](#), 317
[Temporal Order](#), 349
[Temporal Part](#), 350
[Temporary Fix](#), 139
[Terrorism Danger](#), 71
[text message capable](#), 162
[Threat](#), 59
[Threat Actor](#), 114
[Threat Likelihood](#), 98
[Threat Report](#), 369
[Time Coordinate](#), 305, 351
[Time Interval](#), 351
[Time Point](#), 351
[time point on](#), 352, 353
[Time Scale](#), 352
[Time Scale Granularity](#), 352
[Time Scale of Time Point](#), 353
[timeframe for](#), 189, 351
[title](#), 268

Tool, 322
Topological Region, 234
Topology, 234
topology of, 234
Transfer Ability, 153
Transfer Information, 227
Transfer Risk, 111
transfer risk to, 104, 111
Transport Impact, 72
traversed using, 338
trigger, 293, 295
TriScale, 307
typographical conventions, 22
Unavailable, 139
Unconfirmed, 140
Uncorroborated, 140
Undesirable Condition, 120
Undesirable Event, 121
Undesirable Situation, 121
Unintentional Threat, 60
unit ID, 164
Unproven, 138
Unwitting Participant, 77
Usage, 215
used by, 215, 321
used by process, 292, 293
uses, 213, 215
utilized by, 279, 280
valid for time, 187, 189
Valid for Time Interval, 189
Valuation of Asset, 99
value, 130, 166, 222, 305, 355, 356, 357
Valued Asset, 99
values, 93, 99
vector, 126
Very High, 306
Very Low, 306
Victim, 122
victim of, 120, 122
video capable, 162
voice capable, 162
Volume, 317
Vulnerability, 125
Vulnerability Identifier, 126
Vulnerability Metric, 127
vulnerability of, 126, 127
Vulnerability of Resource, 127
War Danger, 72
Watch, 89
watch based on, 107
watched by, 90
watches, 86, 90
Weakened Actor, 153
Weapon, 143
Weapon Leverages Vulnerability, 144
Website Contact, 167
weight, 274
When, 294
Whitelist Indicator, 90
width, 273
withdraws, 152
Witness, 81
witnessed by, 81, 82
witnesses, 81, 82
Witnessing, 81
work, 169
Workaround, 139
World Geodetic System, 234
XOR Condition, 297
XSD Date, 356
XSD Date Time, 357
XSD Time, 357

Ability, 149
Ability To Execute Software, 195
Absorbed Dose (Radiation), 312
Abuse Resource, 321
Acceleration, 313
Accept Risk, 94
Access Complexity, 134
Access Control Failure, 66
Access Identifier, 267
Access Point, 339
Access Vector, 135
Accident, 75
achieves, 242, 243
Activity, 212
Activity Effecting Entity, 301
Activity Map Rule, 393
Actor, 212
Actor Identifier of Credential, 187
Actual Activity, 214
Actual Event, 214
Actual State, 327
ActualObservableFacade, 369
Add Information, 223
Add To Container Event, 173
Address Map Rule, 398
address of, 164, 232
Address of Location, 231
Adjacent, 135
Affected Available Resource, 150
affected by, 329
affected by action, 151, 323
AffectedAssetFacade, 369
affects, 329
affects control of, 151
affords, 153
Alter Ability, 154
altitude, 235
Amount of Substance, 313
AND Condition, 298
Angle, 313
Animal, 273
Area, 313
area code, 168
Area Map Rule, 415
asserted by, 285, 286
Assertion of Policy, 284
asserts policy, 180, 285
assessed by, 156, 158
Assessed Entity, 156
assesses, 157, 158
Assessment, 157
Assessment Activity, 157
Assessment Map Rule, 396
assessment score, 157
associate, 336, 337
Associated Actor, 335
associated with, 336, 337
Assume Risk, 105
assumes risk from, 106, 110
Atomic Information Object, 224
Attack, 60
attack target, 60, 64
attacked by, 61, 322
Attest to Ability, 188
attests to, 188, 189
Authentication, 136
Authority, 180
automated by, 196, 212
Automated Capability, 196
Automated Control, 196
Automated Entity, 197
automates, 196, 197, 199, 200

Automation Type, 198
Automaton, 198
availability, 162
Availability Impact, 136
Avoid Danger, 106
Benefit, 239
Biological Danger, 67
birth date, 274
Blacklist Indicator, 86
Boundary, 339
Boundary of System, 339
bounded-by, 233, 236
bounds, 339, 340
bounds topology, 233, 234
call sign, 166
Campaign, 57
can be utilized by, 150, 323
can execute, 195, 201
Capability, 152
Capture Resource, 321
Catastrophic, 102
Cause and Effect, 327
caused by, 81, 82, 328
causes, 328
causes harm, 121, 122
CBRN Danger, 67
channel, 166
Chemical Danger, 67
city ID, 165
Civil Unrest Danger, 67
Client, 359
Close Information, 224
Collateral Damage Potential, 137
Color, 313
communicates via, 198, 202
Communicating Device, 198
Communications Link, 198
Communications Network, 199
Communications Security Level, 161
Communications Vulnerability, 129
Complete, 137, 138, 140
Compliance Impact, 67
Composite Condition, 298
Computer Control System, 199
Computer System, 199
Concentration, 314
Concentration (amount of substance), 314
Concentration (Mass), 314
Concentration (Volume), 314
condition for, 126, 127
confidence, 91
Confidence, 224
confidence about, 224, 225
Confidence in Assertion, 224
confidence metric, 224
Confidence Metric, 306
Confidentiality Impact, 138
Confirmed, 141
Consequence, 239
Consequence of Situation, 241
Contact Availability, 169
contact for, 161, 162
Contact Information Mapping Rule, 399
Contact Means, 161
Contact Purpose, 169
contact via, 162, 163
Contact Via, 161
Contactable, 162
Contained Information, 225
Container, 173
Containment, 174
Containment Event, 175
contains, 173, 174
contains information, 225, 229

context of observation, 249
Context of Observation, 249
contributes to, 76
Contribution to Danger, 76
contributor, 76, 123
Control, 180
Control Failure, 67
Controlled Entity, 181
Controlling Actor, 182
Conveyance, 274
Coordinate, 219
Coordinate Map Rule, 415
Coordinate of location, 232, 235
Coordinate System, 220
coordinate within system, 220
Count, 306
Countermeasure, 106
countermeasure for, 106, 107
Countermeasure for Strategy, 106
Countermeasure Mitigates, 107
Country, 260
country code, 167
country ID, 165
Country ID, 261
county ID, 165
Create, 301
Create Information, 226
creates process instance, 292, 295
Credential, 189
credential identifier, 187, 189
Criminal Danger, 68
Critical, 103
Currency, 314
Currency Benefit Metric, 306
Current Situation, 328
Custodian, 182
Custody, 183
CVE Identifier, 130
CVSS Score, 134
Cyber Danger, 68
Cyber Resource, 200
Cyber System Failure, 68
Cyber Vulnerability, 130
Cyber Weapon, 200
Damage, 301
Damage Resource, 321
Danger Category, 68
Danger Leads to Incident, 80
Danger Source, 76
Dangerous Condition, 76
Dangerous Event, 77
Date and Time, 346
Date Coordinate, 346
Date-Time Coordinate (ISO 8601), 356
day, 169
death date, 274
Decision-making Impact, 68
degree of affect, 240
degree of mitigation, 111
Delete Information, 226
DeliveryPoint, 388
depends on, 323, 324
designates location, 232
Designation of a Location, 232
desirability, 240
Desirability Assessment, 242
desirability for, 247
desirability of, 246, 247
Destroy, 302
Device, 275
device address, 278
direction, 235
Disinformation Impact, 68
Disrupt Process, 302

Disrupt Stakeholder's Objective, 77
Disruptive Action, 114
distance, 235
Document, 226
document capable, 163
Dose Equivalent (Radiation), 315
Duration, 315
duration of, 315, 346
Duration of Entity, 346
Effect, 329
Electric Current, 315
Electric Potential, 316
Electromagnetic Spectrum Impact, 68
electronic address, 164, 168
Electronic Contact, 163
elevation, 237
Email Address, 163
emergency, 169
enactement of, 214, 292
Energy, 316
Enterprise, 204
enters into, 339, 342
enters through, 302
Entity Assessment, 157
Entity Exists for Interval, 347
Entiy Map Rule, 403
Entry Action, 302
Environmental Impact, 69
evening, 169
Event, 215
Exceed Resource Capacity, 322
executed by, 195, 202
Execution Platform, 200
exists for, 347
Exit Action, 302
exit through, 302
Exit via, 339
Exploit of Vulnerability, 77
Exploitability, 139
exploited by, 78, 127
exploits, 76, 78
ExploitTargetFacade, 369
Facilitator, 152
Facility, 280
Facility Map Rule, 416
Failure, 81
Failure Category, 69
failure of, 81, 82
Failure of Resource, 82
fax capable, 163
Female, 278
filled by, 174, 176
Financial Identifier, 267
Financial Impact, 69
finish of, 348
Finish Time, 347
finishes at, 348
Fire Danger, 69
Force, 316
Frequency, 316
Frequent, 102
Functional, 139
Geophysical Danger, 69
Geopolitical Entity, 261
Geopolitical ID, 261
Geopolitical Region, 262
given name, 270
Governing Authority, 262
governs region, 261, 262
granularity of, 315, 353
happens during, 351
Harm, 118
harm from, 119, 121
Harm-Benefit Metric, 306

harmed by, 120, 322
harms, 120, 122
Harms Resourcee, 119
harms victim, 121, 122
Harms Victim, 120
has ability to execute, 152, 213
has ability to utilize, 150, 213
has address, 231, 234
has authority over, 180, 186
has boundary, 340, 343
has capable performer, 152, 212
has child organization, 256
has condition, 122, 126
has confidence, 225
has consequence, 241
has control over, 181, 182
has control system, 197
has coordinate, 232, 234
has credential, 150, 188
has custody of, 183
has duration, 346
has failure, 82, 322
has granularity, 353
has indicator, 333
has leader, 184, 255
has location designation, 232, 234
has member, 254, 255
has member time Point, 353, 354
has nodes, 199, 202
has objective, 245, 246
has opening, 339, 341
has parent organization, 255, 256
has part, 209
has permission to perform, 214, 264
has portal, 342, 343
has product Line, 361, 364
has relative location, 234, 235
has resident, 271, 282
has risk of harm, 98, 323
has risk to objectives, 97, 100
has scope, 87, 333
has sighting, 87, 91
has state, 333
has subprocess, 294, 295
has temporal part, 351
has topology, 234, 236
has vulnerability, 128, 322
Health Impact, 69
height, 275
High, 134, 138, 139, 142, 143, 308, 310
Identification Map Rule, 406
Identity Provider, 189
Identity Theft, 70
Image Impact, 70
Impact, 207
Impact Category, 70
impact measure, 240
impacted by, 208
impacts, 208
importance, 245
Impose Strategy, 94
imposed by, 95, 111
imposes, 95, 97
Improbable, 102
in the custody of, 183, 184
Inability to Communicate Impact, 70
Incident, 82
Incident Map Rule, 407
incorporated by, 258, 259
Incorporated Organization, 258
incorporates, 259, 261
Incorporation, 258
indicated by, 90
indicates, 89, 90

indicates situation, 86, 87
Indicator, 86
Indicator Indicates Situation, 87
Indicator Pattern, 88
Indicator Watchlist, 88
Indirect Threat, 60
Individual Product, 360
Industrial Control Failure, 70
Information Action, 226
Information Impact, 70
Information In Computer, 201
Information Loss Impact, 71
Information Object, 227
Information Repository, 227
Information Resource, 227
Information System Vulnerability, 130
Information Type, 228
Information Vulnerability, 130
Infrastructure Impact, 71
initiates, 295, 296
Injury Map Rule, 410
Integrity Impact, 139
Intellectual Property Impact, 71
Internet Contact, 164
Internet Contact Map Rule, 400
interval of, 347, 352
Invoke Process, 292
involved in, 214, 330
Involvement, 329
involves, 330
is after, 350
is before, 350
is controlled by, 181, 182
is governed by, 262
is in, 174
is in information structure, 225, 227
is part of, 209
is possessed by, 182, 185
is stored in, 201, 227
is subject to authority, 182, 186
Issue Credential, 190
issued by, 189, 190
issues credential, 189, 190
Item, 275
Item Map Rule, 412
latitude, 236
Leader, 183
Leadership, 183
leads, 183
leads to, 77, 81
Legal Impact, 71
length, 275
Length, 317
leveraged by, 127, 145
leverages, 145
leverages countermeasure, 96, 107
License Identifier, 336
likelihood, 76, 88, 90, 120, 288, 295, 332
Likelihood Categories, 101
line, 168
Local, 135
Local Identifier, 336
located person, 234, 269
Location ID, 232
Location Identifier, 232
Location Map Rule, 417
location of, 281, 282
location of person, 268, 269
longitude, 237
loses control, 153, 155
Lose Ability, 153
Loss of Control Danger, 71
lost by, 155, 213
lost via, 181

Low, 135, 137, 142, 143, 308, 310
Low-Medium, 138
Luminosity, 317
Male, 278
Managed Actor Identifier, 190
Managed Entity, 184
Managed Item Identifier, 275
Managed Person Identifier, 268
Managed Social Agent Identifier, 336
Manufactured Thing, 360
Marginal, 103
Mass, 317
Mass-Density, 317
matches indicator, 89, 91
may be performed by, 212, 264
may entail risk, 99, 122
Means, 242
Means To End, 243
Measurement, 249
measures risk of, 96, 99
measures risk to, 96, 98
Medium, 134, 142, 310
Medium High, 138
Medium, 143
member of, 254, 337
Membership, 253
Meteorological Danger, 71
Metric, 306
middle name, 270
Mission Impact, 72
Mission Objective, 254
mitigated by, 111, 112
mitigates, 106, 108
Mitigation Actor, 108
mobile, 163
Moderate, 308
modified by, 96, 111
modifies risk, 111
Modify Information, 228
Modify Resource, 322
Modus Operandi, 292
Monitor, 108
monitored by, 87, 109
Monitoring Safeguard, 109
Multiple, 136
name part, 270
name suffix, 270
Natural Threat, 60
negate, 299
negated by, 331
negates, 331
negation, 88
Negation Effect, 330
Negligible, 103
net benefit, 242
net desirability, 242
net likelihood, 242
net risk, 242
net severity, 242
network address, 200
Network Identifier, 164
night, 169
Node of a Network, 201
None, 136, 137, 138, 140, 143
Non-Technical Impact, 72
Nuclear Danger, 72
number observed, 251
Object Management Group, Inc. (OMG), 21
Objective, 243
Objective for Safety and Security, 95
objective of, 244, 245
Objective of Stakeholder, 245
Objective to Disrupt, 78
Objective to Protect Assets, 95

Observability, 250
ObservablePatternFacade, 369
Observation, 250
Observation Tool, 251
observed by, 251
observed in context, 249, 251
Observer, 251
observes, 251, 252
Obtain Ability, 153
obtained by, 154, 214
obtained via, 181
obtains control, 153, 154
Occasional, 102
Official Fix, 140
official-given name, 270
OMG specifications, 21
Open Information, 228
Opening in a Boundary, 340
Operating Location, 280
Opportunity, 245
OR Condition, 299
Organization, 255
Organization Map Rule, 419
Organizational Unit, 255
OSVDB Identifier, 131
other, 169
Output, 215
overlaps from, 349
Overlaps in Time, 348
overlaps to, 349
owned by, 185
Owner, 184
Ownership, 184
owns, 184
Parent Organization, 255
Part of Organization, 256
Parthood, 208
Partial, 137, 138, 140
Passport Identifier, 268
Past Situation, 331
pattern indicated by, 88, 332
Pause Process, 302
PentaScale, 308
Performance, 216
performed by, 212, 217
Performer, 322
performs, 214, 217
performs at, 214, 281
performs safeguard, 108, 112
Permission, 264
Perpetrate, 114
perpetrates, 115
perpetrator, 114, 115
Person, 268
Person at location, 269
Person Map Rule, 421
Person Name, 269
Person Name Map Rule, 422
Person Structured Name, 270
personal, 169
PersonInjuryFacade, 389
Physical Boundary, 233
Physical Container, 175
Physical Containment, 175
Physical Entity, 276
Physical Feature, 276
Physical Location, 233
Physical Point, 234
Physical Quantity, 317
physical sex, 274
Physical System Failure, 72
Physical Tool, 276
Physical Vulnerability, 125
Physical Weapon, 144

physically contains, 175
physically within, 175, 277
Place, 281
place ID, 165
Place of Occurrence, 282
Plan, 293
Point Of Entry, 341
Point On Earth, 234
Policy, 285
possesses, 182, 185
Possession, 185
Possible Actions, 303
post box ID, 165
post code, 165
postal address, 166
Postal Address, 164
Postal Address Facade, 387
Postal Address Structured, 164
Postal Address Text, 165
Postal Code, 166
PostCodeBase, 388
PostCodeSuffix, 388
Potential Situation, 332
Power, 318
predicted by, 288, 332
Prediction, 287
Predictor, 288
predicts, 288
Pressure, 318
previously known, 127
primary, 169
Private Network Contact, 166
Probability Metric, 307
Probable, 102
Process Action, 293
Process Decomposition, 293
Process Failure, 72

Process Pattern, 294
produced, 360, 362
produced by, 216, 360, 362
Producer, 360
produces, 215, 216
Product Kind, 361
product line of, 361, 362
Product Line of Supplier, 361
Production, 362
Program, 257
Proof of concept, 139
Property, 185
protected by, 110, 323
Protection, 109
protects, 106, 110
provided by, 359, 363
provides access through, 339, 341
provides product, 363
provides product to, 363, 364
provides security level, 199
Providing, 362
providing action, 360
publicly known, 127
purpose, 162
put into, 173, 176
Radiation Exposure, 318
Radio Contact, 166
Radio Map Rule, 401
Radioactivity, 318
Radiological Danger, 72
rank, 100
Read Information, 228
realized by, 243, 244
Receiving Container, 176
recipient name, 164
reduce harm via, 108, 122
Reference Point, 235

referenced by credential, 188, 191
region ID, 165
Regional Identifier, 336
Related, 209
related from, 210
relates to, 210
Relative Coordinate, 235
relative to, 235
Relocation, 176
Remediation Level, 140
Remote, 102, 135
Removal Event, 176
remove from, 177
Remove Information, 229
removed by, 174, 177
replacement cost, 101
Report Confidencee, 141
required, 126
Residence, 282
Residency, 271
resides at, 268, 271
Resource, 322
Resource Actions, 323
Resource Dependency, 324
results from, 241
revision, 360
revokes permission, 264
Risk, 95
Risk Agent, 110
risk for, 96, 100
risk level accepted, 94
Risk Mitigation Strategy, 96
Risk Owner, 96
Risk Reduction Objective, 97
Risk To Resource, 98
Risk Topic, 98
Risk Treatment, 110
Risk Treatment Strategy, 111
Safeguard Activity, 111
Safeguarding, 112
Safety Danger, 73
Safety Impact, 73
salutation, 270
Scenario, 295
Scope of Indicator, 332
score, 127
secondary, 169
Security Danger, 73
security level, 161
Security Requirements, 141
sensitive to objective, 101
sensitivity threshhold, 101
Serial Number, 363
severity, 122
Severity Categories, 102
Sex Kind, 278
Sighting, 88
Sighting Indicates Situation, 89
Sighting Matches Indicator, 90
Single, 136
situated at, 282
Soocial Agent, 337
Soocial Network Contact, 166
Social Security Number, 271
Software, 202
Software Vulnerability, 131
Source of Danger Category, 73
Source of Harm, 121
Spacial Coordinate, 235
Spacial Entity, 276
Speed, 318
Stakeholder, 246
Stakeholder Desirability, 247
Stakeholder Risk, 99

standing height, 274
start of, 350
Start Time, 349
starts at, 350
State, 333
state of, 333
State of Entity, 333
state_province ID, 165
STIX Campaign Rule, 374
STIX Categories Rule, 372
STIX Course Of Action Rule, 373
STIX Incident Rule, 374
STIX Indicator Rule, 375
STIX Objective Rule, 376
STIX Observable Rule, 377
STIX Sighting Rule, 378
STIX Statement Rule, 379
STIX Threat Actor Rule, 380
STIX TTP Rule, 381
STIX Vocabulary Rule, 382
STIX Vulnerability Rule, 383
Stop Process, 303
stores information, 200, 204
street ID, 165
Strenthened Actor, 153
Structured Information Object, 229
Subject to Authority, 185
Subsystem, 342
Supplier, 364
Supplying Container, 177
supported by, 101
Supporting Condition, 125
supports, 323, 324
surname, 270
surname prefix, 270
System, 342
System Failure, 73
system of coordinate, 219, 220
System of Coordinate, 220
Target Distribution, 143
Target of Attack, 60
Tax Authority Identifier, 337
Telecommunication Device, 277
Telephone Area Code, 167
Telephone Country Code, 167
telephone exchange, 168
telephone extension, 168
Telephone Map Rule, 402
telephone number, 168
Telephone Number, 167
Telephone Number Facade, 388
Telephone Number Structured, 167
Telephone Number Text, 168
Temperature, 319
Temporal Order, 350
Temporal Part, 351
Temporary Fix, 140
Terrorism Danger, 73
text message capable, 163
Threat, 64
Threat Actor, 115
Threat Likelihood, 100
Threat Report, 369
Time Coordinate, 307, 351
Time Interval, 352
Time Point, 352
time point on, 353, 354
Time Scale, 353
Time Scale Granularity, 353
Time Scale of Time Point, 354
timeframe for, 191, 352
title, 270
Tool, 324
Topological Region, 236

Topology, 236
topology of, 236
Transfer Ability, 154
Transfer Information, 229
Transfer Risk, 112
transfer risk to, 106, 112
Transport Impact, 74
traversed using, 339
trigger, 295, 297
TriScale, 309
typographical conventions, 22
Unavailable, 141
Unconfirmed, 141
Uncorroborated, 141
Undesirable Condition, 121
Undesirable Event, 122
Undesirable Situation, 122
Unintentional Threat, 62
unit ID, 165
Unproven, 139
Unwitting Participant, 79
Usage, 217
used by, 217, 323
used by process, 294, 295
uses, 215, 217
utilized by, 281
valid for time, 189, 191
Valid for Time Interval, 194
Valuation of Asset, 101
value, 131, 167, 224, 307, 356, 357, 358
Valued Asset, 101
values, 95, 101
vector, 127
Very High, 308
Very Low, 308
Victim, 123
victim of, 121, 123
video capable, 163
voice capable, 163
Volume, 319
Vulnerability, 126
Vulnerability Identifier, 127
Vulnerability Metric, 128
vulnerability of, 127, 128
Vulnerability of Resource, 128
War Danger, 74
Watch, 91
watch based on, 109
watched by, 92
watches, 88, 92
Weakened Actor, 154
Weapon, 144
Weapon Leverages Vulnerability, 145
Website Contact, 168
weight, 276
When, 296
Whitelist Indicator, 92
width, 275
withdraws, 153
Witness, 83
witnessed by, 83, 84
witnesses, 83, 84
Witnessing, 83
work, 169
Workaround, 141
World Geodetic System, 236
XOR Condition, 299
XSD Date, 357
XSD Date Time, 358
XSD Time, 358